NOTES DEL SEMINARI

MÒDULS DE DRINFELD

Barcelona *2004*

9

Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)

MÒDULS DE DRINFELD

Edició a cura de

X. Xarles

Amb contribucions de

F. Bars L.V. Dieulefait C. A. Infante

E. Nart V. Rotger N. Vila X. Xarles

X. Xarles
Dep. de Matemàtiques
Edifici C
Univ. Autònoma de Barcelona
08193 Bellaterra
Espanya

Classificació AMS
Primària: 11G09, 11G18, 11G40, 11M38, 11R58, 11S31, 11T55
Secundària: 11G45, 11R37, 11R39, 11T06, 11T71

Barcelona, 2004
Amb suport parcial de DGESIC, BHA2000-0180

ISBN:

Índex

Introducció

Aquestes notes contenen les conferències sobre mòduls de Drinfeld presentades en la setzena edició del Seminari de Teoria de Nombres (UB-UAB-UPC), celebrat del 1 al 8 de Febrer de 2002 a Barcelona, a la Facultat de Nàutica de la Universitat Politècnica de Catalunya.

El programa general va ser elaborat per F. Bars, E. Nart i X. Xarles i les sessions varen ser dutes a terme per diferents persones del seminari, gràcies a les quals tenim les notes que presentem aquí.

Un dels desenvolupaments matemàtics més importants del segle XX és la possibilitat d'interpretar certs fenòmens combinatoris associats a varietats algebraiques sobre cossos finits mitjançant idees topològiques que es concreten a través d'una cohomologia aritmètica. El treball pioner de E. Artin, F.K. Schmidt, H. Hasse i A. Weil sobre aquesta qüestió culminà amb el desenvolupament de la cohomologia étale i la cohomologia ℓ-àdica per part de M. Artin, A. Grothendieck i P. Deligne, entre d'altres.

Com passa sovint en Matemàtiques, el treball pioner es focalitzà en objectes molt concrets, que admetien la utilització de tècniques ad hoc. En aquest cas els objectes concrets eren les corbes sobre cossos finits i els mètodes ad hoc consistiren, essencialment, en la utilització de la jacobiana de la corba.

Al mateix temps que aquesta teoria clàssica de corbes sobre cossos finits anava sent descoberta, a les dècades dels anys 30 i 40, L. Carlitz estudiava els mateixos objectes des d'una òptica diferent. En comptes d'associar a la corba una funció zeta complexa, Carlitz introduí una funció exponencial amb arguments i valors en característica positiva.

Amb aquestes idees de Carlitz naixia una nova aritmètica dels cossos de funcions.

Hi ha una "gran teoria"que conté l'aritmètica de Carlitz com a mètode ad hoc particular per tractar un cas concret? Als anys 70, després dels treballs de V.G. Drinfeld es va fer evident que aquesta qüestió havia de tenir una resposta positiva. Els mòduls de Drinfeld permeten estendre les idees de Carlitz, i tota una sèrie de fenòmens aritmètics clàssics, als cossos de funcions sobre un cos finit. Més enllà d'aquest objectiu inicial, les idees de Drinfeld han estat la base d'un cos teòric enorme que està en camí de configurar aquesta "gran teoriaï que sembla capaç de contenir una enorme varietat de fenòmens geomètric-aritmètics en característica positiva: espais de moduli, shtukas, sèries L, formes modulars, formes automorfes, filosofia de Langlands, etc.

En el quatre primers temes del Seminari es fa una introducció detallada a la teoria bàsica de mòduls de Drinfeld. Els temes 5 i 6 presenten unes aplicacions concretes d'aquestes idees. Finalment, els quatre darrers temes esbossen (només) com es traslladen al context dels cossos de funcions certs fenòmens geomètric-aritmètics lligats a les formes modulars i les corbes modulars.

F. Bars, E. Nart i X. Xarles

Bellaterra, 8 de Gener de 2004.

Capítol 1

Anell de polinomis $\mathbb{F}_q$-lineals

Enric Nart

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

Fixem un cos K de característica $p > 0$. Per fixar idees, podeu pensar que K és el cos de funcions d'una corba algebraica sobre un cos finit.

Un polinomi $P(x) \in K[x]$, diem que és ADDITIU si satisfà una de les dues condicions equivalents:

$$P(a+b) = P(a) + P(b), \quad \forall a, b \in \overline{K},$$
$$P(x+y) = P(x) + P(y).$$

El conjunt dels polinomis additius és un K-subespai vectorial de $K[x]$ i adquireix una estructura d'anell no commutatiu respecte de l'operació de composició:

$$Q(x) \circ P(x) = Q(P(x)),$$

on el polinomi x fa d'unitat. Via una identificació natural, aquest anell és canònicament isomorf a $\mathrm{End}_{K-\mathrm{gr.sch.}}(\mathbb{G}_{a,K})$.

Un polinomi additiu $P(x)$ determina, doncs, un homomorfisme de grups:

$$P\colon \overline{K} \longrightarrow \overline{K},$$

i el conjunt de les seves arrels és un subgrup de $\overline{K}$ com a grup additiu. Pels polinomis separables val el recíproc:

1.1.1 Teorema fonamental dels polinomis additius *Considerem $P(x) \in K[x]$ separable i $W \subseteq K^{\text{sep}}$ el conjunt de les seves arrels. Aleshores:*

$$P(x) \quad \textit{additiu} \iff W \quad \textit{subgrup.}$$

Demostració: Podem suposar $P(x)$ mònic. Cal comprovar que si W és subgrup aleshores $P(x) = \prod_{w\in W}(x-w)$ és additiu.

Per a qualsevol $a \in \overline{K}$, considerem el polinomi

$$H_a(x) = P(x+a) - P(x) - P(a).$$

Tenim, clarament,

$$\left.\begin{array}{c} \deg H_a(x) < \deg P \\ H_a(w) = 0,\ \forall w \in W \end{array}\right\} \Longrightarrow H_a(x) = 0.$$

□

Podem fixar l'atenció en un cos base finit $\mathbb{F}_q \subseteq K$, i repetir tot el que hem fet preservant l'estructura de $\mathbb{F}_q$-àlgebra. Definim polinomis $\mathbb{F}_q$-lineals com aquells $P(x) \in K[x]$ pels quals l'aplicació natural $P\colon \overline{K} \longrightarrow \overline{K}$ és $\mathbb{F}_q$-lineal. Es comprova de manera completament anàloga que, si $P(x)$ és separable, el caràcter $\mathbb{F}_q$-lineal equival a que el conjunt W de les seves arrels sigui un $\mathbb{F}_q$-subespai vectorial de K^{sep}.

En completa generalitat, a un polinomi $\mathbb{F}_q$-lineal $P(x) \neq 0$ li associem el subesquema en $\mathbb{F}_q$-espais vectorials de $\mathbb{G}_a$, finit sobre $\operatorname{Spec}(K)$, definit per:

$$W_P := \operatorname{Spec}(K[x]/P(x)).$$

Per a qualsevol K-àlgebra B, $W_P(B)$ és el $\mathbb{F}_q$-subespai vectorial de B format per les arrels de $P(x)$ a B.

Tot subesquema en $\mathbb{F}_q$-espais vectorials de $\mathbb{G}_a$, finit sobre $\mathrm{Spec}(K)$, és d'aquesta forma. Com que $K[x]$ és principal, tot subesquema tancat de $\mathbb{G}_a$ és de la forma $\mathrm{Spec}(K[x]/P(x))$ per a algun polinomi $P(x)$. El subesquema és finit sobre $\mathrm{Spec}(K)$ sii $P(x) \neq 0$, i és en $\mathbb{F}_q$-espais vectorials sii $P(x)$ és $\mathbb{F}_q$-lineal.

1.2 Anell de polinomis de Frobenius

Fixem un cos finit $\mathbb{F}_q \subseteq K$. Denotem per $K\{\tau\}$ el K-espai vectorial de polinomis per l'esquerra, $a_0 + a_1\tau + \cdots + a_n\tau^n$, amb coeficients a K. Dotem $K\{\tau\}$ de l'operació producte que es dedueix de les regles naturals del producte de polinomis, junt amb l'obligació de respectar la condició:

$$\tau \cdot a = a^q \cdot \tau, \quad \forall a \in K.$$

Obtenim un anell no commutatiu (si $K \neq \mathbb{F}_q$) amb una estructura natural de $\mathbb{F}_q$-àlgebra. Noteu que l'estructura d'anell de $K\{\tau\}$ depèn de l'elecció de q, tot i que no ho indiquem en la notació.

Aquest anell conserva algunes de les propietats usuals de l'anell de polinomis. Per exemple, disposem d'una funció GRAU amb les propietats usuals:

$$\begin{aligned} &\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}, \\ &\deg(PQ) = \deg(P) + \deg(Q). \end{aligned}$$

Per tant, $K\{\tau\}$ és un domini i tot element no nul cancel.la multiplicativament per la dreta i per l'esquerra.

Disposem d'un homomorfisme d'anells, $K \longrightarrow K\{\tau\},\ a \mapsto a$, que permet identificar K amb els polinomis constants. No obstant això, $K\{\tau\}$ no és una K-àlgebra:

$$a\tau = a(\tau \cdot 1) = (a\tau) \cdot 1 \neq \tau \cdot a = a^q\tau.$$

1.2.1 Proposició. *L'aplicació K-lineal determinada per:*

$$K\{\tau\} \longrightarrow K[x], \quad \tau^n \mapsto x^{q^n}, \ \forall n \geq 0,$$

és un isomorfisme de $\mathbb{F}_q$-àlgebres entre $K\{\tau\}$ i l'anell dels polinomis $\mathbb{F}_q$-lineals.

Demostració: Els polinomis x^{q^n} són $\mathbb{F}_q$-lineals, aquesta aplicació és $\mathbb{F}_q$-lineal, envia $1 \mapsto x$ i transforma producte de polinomis en τ en composició de polinomis en x.

Falta només comprovar que abastem tots els polinomis $\mathbb{F}_q$-lineals. Suposem que $P(x) \in K[x]$ és un polinomi $\mathbb{F}_q$-lineal. Tenim:

$$P(\zeta a) = \zeta P(a), \ \forall \zeta \in \mathbb{F}_q, \forall a \in \overline{K}.$$

Això equival a: $P(\zeta x) = \zeta P(x)$ i obliga $P(x)$ a ser combinació lineal dels monomis x^{q^n}. □

1.2.2 Notació. Denotem simplement per $P(\tau)$, $P(x)$ una parella de polinomis que es corresponen a través de l'isomorfisme anterior. Per exemple,

$$P(\tau) = a\tau^0 + b\tau^5 + c\tau^8 \ \leftrightarrow \ P(x) = ax + bx^{q^5} + cx^{q^8}.$$

El terme independent d'un polinomi en τ s'acompanya a vegades del símbol τ^0 per emfasitzar que el polinomi representa un determinat polinomi $\mathbb{F}_q$-lineal.

Noteu que si $P(\tau) = a_0 + a_1\tau + \cdots + a_n\tau^n$, el corresponent polinomi $\mathbb{F}_q$-lineal $P(x)$ és separable si i només si $a_0 \neq 0$.

1.3 Divisibilitat a l'anell $K\{\tau\}$

Diem que $g(\tau)$ divideix $f(\tau)$ per la dreta si $f(\tau) = h(\tau)g(\tau)$, per a algun $h(\tau) \in K\{\tau\}$.

1.3.1 Algorisme de divisió per la dreta.

Donats $f(\tau)$, $g(\tau) \in K\{\tau\}$, amb $g(\tau) \neq 0$, existeix una única parella $Q(\tau)$, $R(\tau) \in K\{\tau\}$ satisfent:

$$f(\tau) = Q(\tau)g(\tau) + R(\tau), \qquad \deg R(\tau) < \deg g(\tau).$$

DEMOSTRACIÓ: Apliquem l'algorisme usual de divisió de polinomis, pensant que el quocient multiplica el divisor per l'esquerra. Tot funciona igual perquè tenim divisió exacta entre monomis:

$$(a\tau^m) : (b\tau^n) = \frac{a}{b^{q^{m-n}}}\tau^{m-n}.$$

□

1.3.2 Corol·lari. *$R(x)$ és el residu de fer la divisió euclidiana de $f(x)$ per $g(x)$.*

DEMOSTRACIÓ: $f(x) = Q(x) \circ g(x) + R(x) = g(x)T(x) + R(x)$. □

1.3.3 Corol·lari. *$K\{\tau\}$ és DIP per l'esquerra.*

Tenim, per tant, màxim comú divisor i mínim comú múltiple, per la dreta, d'un parell de polinomis:

$\mathrm{mcd}_{\mathrm{dr}}(f, g)$:= generador mònic de $K\{\tau\}f + K\{\tau\}g$,

$\mathrm{mcm}_{\mathrm{dr}}(f, g)$:= generador mònic de $K\{\tau\}f \cap K\{\tau\}g$,

que satisfan les usuals propietats universals de divisió per la dreta.

1.3.4 Corol·lari.

$$h(\tau) = \mathrm{mcd}_{\mathrm{dr}}(f(\tau), g(\tau)) \implies h(x) = \mathrm{mcd}(f(x), g(x)).$$

DEMOSTRACIÓ: Tots dos mcd es calculen mitjançant l'algorisme d'Euclides i els residus de les divisions es corresponen pel Corol·lari 1.3.2.□

Hi ha algorisme de divisió per l'esquerra només quan K és perfecte, perquè només en aquest cas hi ha divisió exacta de monomis per l'esquerra:

$$(a\tau^m)\colon (b\tau^n) = \left(\frac{a}{b}\right)^{1/q^n} \tau^{m-n}.$$

Altura d'un polinomi

L'altura d'un polinomi $f(\tau) \in K\{\tau\}$ és el mínim grau d'un monomi no nul. Es denota $\mathrm{ht}(f)$. Tenim, doncs,

$$\mathrm{ht}(f) = h \text{ si } f(\tau) = a\tau^h + \text{ termes de grau superior, amb } a \neq 0.$$

Noteu que els polinomis d'altura zero són precisament els separables. Clarament,

$$\mathrm{ht}(f+g) \geq \min\{\mathrm{ht}(f), \mathrm{ht}(g)\},$$
$$\mathrm{ht}(fg) = \mathrm{ht}(f) + \mathrm{ht}(g).$$

Tot polinomi s'escriu de manera única:

$$f(\tau) = f_0(\tau)\tau^{\mathrm{ht}(f)}, \text{ amb } f_0(\tau) \text{ separable.}$$

De la relació $f(\tau) = f_0(\tau)\tau^h$ es dedueix en general, encara que f_0 no sigui separable:

$$W_f(\overline{K}) = W_{f_0}(\overline{K})^{q^{-h}}. \tag{1.1}$$

Com que els polinomis separables són governats pel subespai de les seves arrels a $\overline{K}$, podem determinar també la facultat de dividir per la dreta en termes de les arrels i l'altura.

1.3.5 Lema. *Per a $f(\tau)$, $g(\tau) \in K\{\tau\}$, amb $g(\tau) \neq 0$, les següents condicions són equivalents:*

1. *$g(\tau)$ divideix $f(\tau)$ per la dreta*
2. *$g(x)$ divideix $f(x)$*
3. *$W_g \subseteq W_f$ com a subesquemes en $\mathbb{F}_q$-e.v. de $\mathbb{G}_a$*

4. $W_g(\overline{K}) \subseteq W_f(\overline{K})$ *i* $\mathrm{ht}(g) \leq \mathrm{ht}(f)$

DEMOSTRACIÓ: 1 $\iff$ 2 és una conseqüència immediata del Corol·lari 1.

2 $\iff$ 3 perquè les dues condicions equivalen a que hi hagi una factorització dels homomorfismes canònics de projecció:

$$\begin{array}{ccc} & \nearrow & K[x]/f(x) \\ K[x] & & \downarrow \\ & \searrow & K[x]/g(x). \end{array}$$

$$1 \implies 4 \quad \begin{cases} f(\tau) = h(\tau)g(\tau) \implies \mathrm{ht}(g) \leq \mathrm{ht}(f), \\ f(x) = g(x)T(x) \implies W_g(\overline{K}) \subseteq W_f(\overline{K}). \end{cases}$$

4 $\implies$ 1: Dividint els dos polinomis per $\tau^{\mathrm{ht}(g)}$ i aplicant (1.1), podem suposar $\mathrm{ht}(g) = 0$, i.e. $g(x)$ separable. Ara, fent la divisió per la dreta: $f(\tau) = Q(\tau)g(\tau) + R(\tau)$, veiem que $R(x)$ s'anul·la en totes les $\deg(g(x))$ arrels de $g(x)$; com que $\deg(R) < \deg(g)$, a la força $R(x) = 0$. $\square$

Això permet explicitar $\mathrm{mcd}_{dr}(f, g)$ i $\mathrm{mcm}_{dr}(f, g)$ en termes dels subespais d'arrels. Denotem:

$$\begin{aligned} &W_f = W_f(\overline{K}), \quad W_g = W_g(\overline{K}), \\ &h_m = \min\{\mathrm{ht}(f), \mathrm{ht}(g)\}, \quad h_M = \max\{\mathrm{ht}(f), \mathrm{ht}(g)\}, \\ &P_W(x) = \textstyle\prod_{w \in W}(x - w), \quad \text{per a qualsevol } W \subseteq \overline{K}. \end{aligned}$$

Pel lema anterior,

$$\mathrm{mcd}_{dr}(f, g) = \tau^{h_m} P_{W_f \cap W_g}(\tau), \quad \mathrm{mcm}_{dr}(f, g) = \tau^{h_M} P_{W_f + W_g}(\tau),$$

ja que satisfan les propietats universals respectives de divisibilitat per la dreta.

En particular, considerant els graus com a polinomis en τ:

$$\deg(f) + \deg(g) = \deg(\mathrm{mcd}_{dr}(f, g)) + \deg(\mathrm{mcm}_{dr}(f, g)).$$

Fem observar que el polinomi $P_{W_f \cap W_g}(\tau)$ té coeficients a $K^{-q^{h_m}}$ i només en multiplicar-lo per l'esquerra per τ^{h_m} s'obté un polinomi amb coeficients a K. Anàlogament per a $P_{W_f+W_g}(\tau)$.

A qualsevol polinomi $f(x) \in K[x]$, encara que no sigui $\mathbb{F}_q$-lineal, li podem associar un polinomi $F(\tau) \in K\{\tau\}$ satisfent una propietat universal respecte de la divisibilitat. Considerem l'ideal esquerra

$$I_f := \{P(\tau) \in K\{\tau\} \mid f(x)|P(x)\},$$

i prenem $F(\tau)$ com el seu generador mònic: $I_f = K\{\tau\}F(\tau)$.

Amb les idees anteriors, és fàcil veure que $F(\tau) = \tau^e P_W(\tau)$, on W és el $\mathbb{F}_q$-subespai vectorial de $\overline{K}$ generat per les arrels de $f(x)$ i e és el mínim enter tal, que totes les multiplicitats de les arrels de $f(x)$ són menors o iguals que q^e. Com abans, el polinomi $P_W(\tau)$ pot no tenir coeficients a K.

La teoria de la divisibilitat de $K\{\tau\}$ la culminà Ore amb el concepte adequat de polinomi irreductible i un teorema de factorització única en producte d'irreductibles a menys de *similaritat*. Vegeu [Goss, 1.10,1.11] i [Ore1], [Ore2].

1.4 Immersions de $K\{\tau\}$ en d'altres anells

Podem submergir $K\{\tau\}$ en un anell $K\{\{\tau\}\}$ de sèries formals de Frobenius. La definició d'aquest darrer anell és la natural i es conserven moltes de propietats usuals dels anells de sèries formals commutatius. Per exemple, una sèrie és invertible per la dreta sii és invertible per l'esquerra sii el terme independent és no nul.

De tota manera, la construcció que utilitzarem d'una manera més significativa és la d'un anell de fraccions per l'esquerra. Submergirem $K\{\tau\} \hookrightarrow K(\tau)$, on $K(\tau)$ és un anell de divisió satisfent una propietat universal. La construcció, deguda a Ore, és molt general.

Anell de fraccions per l'esquerra

1.4.1 Definició Un domini R diem que satisfà les *condicions d'Ore per l'esquerra* si per a tot parell d'elements no nuls $a, b \in R$, existeix

una altre parell d'elements no nuls $u, v \in R$, que satisfan $ua = vb$.

1.4.2 Teorema. *Aquestes condicions són necessàries i suficients perquè existeixi una solució mínima al problema universal:*

$$R \hookrightarrow D,$$

D anell de divisió amb la propietat de que tot element es pot expressar com $u^{-1}v$, amb $u, v \in R$.

Demostració: Si existeix D, per a qualsevol parell $a, b \in R$ d'elements no nuls podrem expressar, a D:

$$ab^{-1} = u^{-1}v,$$

amb $u, v \in R - \{0\}$. D'on $ua = vb$ a D, i per tant també a R.

Recíprocament, si es donen les condicions d'Ore es pot construir una solució mínima. Si en una hipotètica fracció per l'esquerra multipliquem numerador i denominador per l'esquerra pel mateix element no nul, obtenim una fracció equivalent:

$$b^{-1}a = b^{-1}u^{-1}ua = (ub)^{-1}ua, \ \forall u \in R, u \neq 0.$$

Definim formalment fraccions $b^{-1}a$, identificant dues fraccions quan multiplicant numerador i denominador de cada fracció per un mateix element de R, puguem fer coincidir els dos numeradors i, també, els dos denominadors:

$$D := (R \times (R - \{0\})) \,/\sim$$

$$(a, b) \sim (c, d) \ \text{ si } \ \exists\, u, v \in R, uv \neq 0, \ \text{tq} \ \begin{cases} ua = vc \\ ub = vd \end{cases}$$

Aquesta relació és d'equivalència. Comprovem, per exemple, la propietat transitiva:

$$\left.\begin{matrix} ua = vc \\ ub = vd \end{matrix}\right\}, \quad \left.\begin{matrix} Uc = Ve \\ Ud = Vf \end{matrix}\right\} \implies \left.\begin{matrix} \lambda ua = \lambda vc = \mu Uc = \mu Ve \\ \lambda ub = \lambda vd = \mu Ud = \mu Vf \end{matrix}\right\},$$

essent $\lambda, \mu \in R$ tals, que $\lambda v = \mu U$.

Podem definir operacions de suma i producte en el conjunt quocient:

$$b^{-1}a + d^{-1}c := (ub)^{-1}ua + (vd)^{-1}vc = (ub)^{-1}(ua + vc),$$

si $ub = vd$ (reduir a comú denominador).

$$b^{-1}a \cdot d^{-1}c = (ub)^{-1}ua \cdot (vd)^{-1}vc = (ub)^{-1}vc,$$

si $ua = vd$.

Es comprova fàcilment que són operacions ben definides i que doten D d'estructura d'anell de divisió. L'homomorfisme: $R \hookrightarrow D, \quad a \mapsto 1^{-1}a$, acaba de resoldre la qüestió. □

L'existència de mcm_{dr} ens fa veure que el domini $K\{\tau\}$ satisfà les condicions d'Ore per l'esquerra.

Bibliografia

[Goss] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin-Heidelberg, 1998.

[Ore1] O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35**(1933), 559-584.

[Ore2] O. Ore, *Theory of non-commutative polynomials*, Ann. of Math. **34**(1933), 480-508.

E. Nart
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
nart@mat.uab.es

Capítol 2

El mòdul de Carlitz

Núria Vila

El primer mòdul de Drinfeld de la història fou introduït per Carlitz (1907-1999). L'objectiu d'aquest capítol és presentar i estudiar amb detall el mòdul de Carlitz. Aquest és el més simple dels mòduls de Drinfeld, on hi apareixen les idees claus que cal tenir present per comprendre la teoria general abstracta. Construirem i estudiarem la funció exponencial de Carlitz que ens defineix l'acció que ens determina una estructura de mòdul de Drinfeld explícita. Estudiarem els punts de torsió per aquesta acció, donats pels valors de divisió de l'exponencial de Carlitz, que defineixen extensions abelianes al adjuntar-los; de fet el seu comportament és anàleg al ciclotòmic. La referència bàsica per aquest capítol és el text de Goss [Go 96].

2.1 La funció exponencial de Carlitz

En primer lloc fixarem algunes notacions que seran utilitzades al llarg de tot el capítol.

Sigui $K = \mathbb{F}_q(T) = K(\mathbb{P}^1)$, el cos de funcions sobre $\mathbb{P}^1_{\mathbb{F}_q}$, on $\mathbb{F}_q$ és el cos finit amb $q = p^r$ elements.

Amb el suport parcial de MCYT BFM 2000-0794-C02-01.

Sigui $\mathbb{A} = \mathbb{F}_q[T] = \mathcal{O}_{\mathbb{P}^1}(\mathbb{P}^1 \backslash \{\infty\})$, l'anell de funcions sobre $\mathbb{P}^1_{\mathbb{F}_q}$ regulars fora de ∞.

Considerem la valoració discreta d'uniformitzant $1/T$:

$$v_\infty : K \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

Sigui $K_\infty = \mathbb{F}_q((T))$ la completació de K respecte de v_∞. Denotem per $\mathbb{C}_\infty = \widehat{\overline{K}_\infty}$ la completació d'una clausura algebraica $\overline{K}_\infty$ de K_∞, fixada, amb l'extensió canònica de v_∞. El cos $\mathbb{C}_\infty$ és complet i algebraicament tancat.

La **funció exponencial de Carlitz** serà una funció entera

$$e_C : \mathbb{C}_\infty \longrightarrow \mathbb{C}_\infty,$$

que definiren imitant la funció exponencial clàssica. En primer lloc ens cal construir un anàleg al factorial.

2.1.1 Definicions. Denotem:

1. $[i] := T^{q^i} - T$, $i > 0$.
2. $L_i := [i].[i-1].\cdots.[1] = \prod_{j=1}^{i}(T^{q^j} - T)$, $i > 0$; $L_0 = 1$.
3. $D_i := [i].[i-1]^q.\cdots.[1]^{q^{i-1}} = \prod_{j=0}^{i-1}(T^{q^i} - T^{q^j})$, $i > 0$; $D_0 = 1$.
4. $\begin{bmatrix} d \\ i \end{bmatrix} := \frac{D_d}{D_i L_{d-i}^{q^i}}$, $d \geq i \geq 0$.

2.1.2 Observació. Els elements $[i]$, L_i, D_i són polinomis mònics de $\mathbb{A}$. Aquests elements són fonamentals en la aritmètica de $\mathbb{A}$. Veurem que també $\begin{bmatrix} d \\ i \end{bmatrix}$ són polinomis de $\mathbb{A}$, això serà conseqüència del Teorema de Carlitz (2.1.6). D'altra banda, és clar que:

$$\deg[i] = q^i, \qquad \deg D_i = iq^i, \qquad \deg L_i = q\frac{q^i - 1}{q - 1}.$$

2.1.3 Proposició. *Es compleixen les propietats següents:*

1. $[i] = \prod$ *pol. mònics irr. de grau divisor de* i.
2. $D_i = [i]D_{i-1}^q$.

3. $D_i = \prod$ *polinomis mònics de grau* i.

4. $L_i = m.c.m.\{$*polinomis mònics de grau* $i\}$.

DEMOSTRACIÓ: L'apartat 1) és un exercici elemental de cossos finits prou conegut. 2) és clar. Per veure 3) i 4) cal comparar el nombre de vegades que un polinomi irreductible i mònic divideix els dos membres de la igualtat i comprovar que coincideix. □

La **funció exponencial de Carlitz** és defineix com

$$e_C(x) := \sum_{i=0}^{\infty} \frac{x^{q^i}}{D_i}.$$

Aquesta suma convergeix a un element de $\mathbb{C}_\infty$ i defineix una funció entera i F_q-lineal

$$e_C : \mathbb{C}_\infty \longrightarrow \mathbb{C}_\infty.$$

En efecte, és clar que

$$v_\infty(\frac{x^{q^i}}{D_i}) = q^i v_\infty(x) + deg D_i = q^i(v_\infty(x) + i)$$

tendeix a ∞, per $i \to \infty$. Per tant la sèrie $e_C(x)$ convergeix a $\mathbb{C}_\infty$ i defineix una funció entera. D'altra banda, $e_C(x)$ és F_q-lineal doncs $e_C(x)$ és lmit de polinomis F_q-lineals

$$e_C(x) = \lim_{m\to\infty} \sum_{i=1}^{m} \frac{x^{q^i}}{D_i}.$$

En anàlisis no-arquimedià una funció entera no constant és exhaustiva i queda determinada a menys d'una constant multiplicativa pel conjunt dels seus zeros, comparant multiplicitats (cf. [Go 96], 2.13, 2.14).

Veurem a continuació que tots els zeros de e_C són simples i que

$$\Lambda := \mathrm{Ker}(e_C)$$

és un sub-$\mathbb{A}$-mòdul de $\mathbb{C}_\infty$.

En una primera aproximació podem pensar que el *mòdul de Carlitz* és $\mathbb{C}_\infty$ dotat amb l'estructura de $\mathbb{A}$-mòdul copiada de $\mathbb{C}_\infty/\Lambda$ via e_C, és a dir, per l'isomorfisme

$$\mathbb{C}_\infty/\Lambda \simeq^{e_C} \mathbb{C}_\infty.$$

La recerca dels zeros de e_C la fem simultàniament amb la recerca d'una expressió de e_C com a producte infinit.

2.1.4 Definició Per $d \geq 0$, sigui $\mathbb{A}(d) := \{\alpha \in \mathbb{A} : \deg \alpha < d\}$.

Posem $e_0(X) = X$ i per $d \geq 0$, considerem els polinomis

$$e_d(X) := \prod_{\alpha \in \mathbb{A}(d)} (X - \alpha) = \prod_{\alpha \in \mathbb{A}(d)} (X + \alpha).$$

2.1.5 Observació. 1. $\mathbb{A}(d)$ és un $\mathbb{F}_q$-espai vectorial de dimensió d, a més $\mathbb{A}(0) = \{0\}$ i $\mathbb{A} = \bigcup_{d \geq 0} \mathbb{A}(d)$.

2. Els polinomis $e_d(X)$ són $\mathbb{F}_q$-lineals.

3. La funció exponencial de Carlitz e_C l'obtindrem com un pas al límit de e_d, quan $d \to \infty$.

2.1.6 Teorema. (Carlitz) *Tenim*

$$e_d(X) = \sum_{i=0}^{d} (-1)^{d-i} \begin{bmatrix} d \\ i \end{bmatrix} X^{q^i}.$$

Com a conseqüència del teorema de Carlitz obtenim que $\begin{bmatrix} d \\ i \end{bmatrix} \in \mathbb{A}$.

El lema següent ens dona una expressió recurrent de $e_d(X)$, que és clau en la demostració per inducció del teorema de Carlitz.

2.1.7 Lema.

$$e_d(X) = e_{d-1}(X)^q - D_{d-1}^{q-1} e_{d-1}(X)$$

DEMOSTRACIÓ: Els dos membres de la igualtat són polinomis mònics en X de grau q^d. N'hi ha prou en veure que el polinomi de la dreta s'anul.la per a tots els elements de $\mathbb{A}(d)$. Sobre tots els de $\mathbb{A}(d-1)$ s'hi anul.la, ja que tots són arrels de $e_{d-1}(X)$. Considerem $\alpha = \zeta h$, amb $\zeta \in \mathbb{F}_q$ i $h = h(T) \in \mathbb{A}$ mònic de grau $d-1$. Tenim que $e_{d-1}(h) = D_{d-1}$, doncs

$$e_{d-1}(h) = \prod_{\alpha \in \mathbb{A}(d-1)} (h+\alpha) = \prod \text{pol. mònics de grau } d-1 = D_{d-1},$$

cf. 2.1.3. Per tant

$$e_{d-1}(\zeta h)^q - D_{d-1}^{q-1} e_{d-1}(\zeta h) = \zeta^q D_{d-1}^q - D_{d-1}^{q-1} \zeta D_{d-1} = 0,$$

doncs $\zeta^q = \zeta$. □

DEMOSTRACIÓ:(del Teorema de Carlitz) Per hipòtesi d'inducció tenim que

$$e_{d-1}(X) = \sum_{i=0}^{d-1} (-1)^{d-1-i} \begin{bmatrix} d-1 \\ i \end{bmatrix} X^{q^i}.$$

El resultat s'obté substituint aquesta expressió en el lema anterior i tenint en compte que:

$\begin{bmatrix} d-1 \\ i \end{bmatrix} = \frac{D_{d-1}}{D_i L_{d-1-i}^{q^i}}$, $\begin{bmatrix} d \\ 0 \end{bmatrix} = \frac{D_d}{D_0 L_d} = \frac{D_{d-1}^q}{D_0 L_{d-1}}$, $D_0 = 1$, $D_i = [i] D_{i-1}^q$. □

Ara, volem passar al límit, per $d \to \infty$ els dos membres de la igualtat del teorema de Carlitz. A fi d'obtenir un producte infinit convergent cal normalitzar, dividint pel coeficient de X en $e_d(X)$:

$$\prod_{0 \neq \alpha \in \mathbb{A}(d)} \alpha = (-1)^d \frac{D_d}{L_d}.$$

Al dividir en el T. Carlitz, obtenim:

$$X \prod_{0 \neq \alpha \in \mathbb{A}(d)} (1 + \frac{X}{\alpha}) = \sum_{i=0}^{d} (-1)^i \frac{L_d}{L_{d-i}^{q^i}} \frac{X^{q^i}}{D_i}.$$

Denotem

$$\beta_i := [1]^{\frac{q^i-1}{q-1}}, \qquad \xi_i := \beta_i/L_i,$$

podem reescriure l'expressió anterior:

$$X \prod_{0\neq\alpha\in\mathbb{A}(d)} (1+\frac{X}{\alpha}) == \frac{1}{\xi_d}\sum_{i=0}^{d}(-1)^i\beta_i\ \xi_{d-i}^{q^i}\ \frac{X^{q^i}}{D_i}.$$

2.1.8 Lema. *Es compleix:*

1. $\xi_d = \prod_{j=1}^{d-1}(1-\frac{[j]}{[j+1]})$.
2. $\xi_* := \lim_{d\to\infty}\xi_d = \prod_{j=1}^{\infty}(1-\frac{[j]}{[j+1]})$, *convergeix a* K_∞.
3. *Per a tot* $x\in\mathbb{C}_\infty$, $\sum_{i=0}^{\infty}(-1)^i\beta_i\ \xi_*^{q^i}\ \frac{x^{q^i}}{D_i}$, *convergeix a* $\mathbb{C}_\infty$.
4. $x\prod_{0\neq\alpha\in\mathbb{A}}(1+\frac{x}{\alpha}) = \frac{1}{\xi_*}\sum_{i=0}^{\infty}(-1)^i\beta_i\ \xi_*^{q^i}\ \frac{x^{q^i}}{D_i}$.

Demostració: Les convergències són clares tenint en compte que les valoracions:
$v_\infty(\frac{[j]}{[j+1]}) = q^{j+1}-q^j\to\infty$, si $j\to\infty$;
$v_\infty(\xi_d) = 0$ i per tant $v_\infty(\xi_*) = 0$;
$v_\infty((-1)^i\beta_i\xi_*^{q^i}\frac{X^{q^i}}{D_i}) = -q\frac{q^i-1}{q-1}+q^i+iq^i = \frac{q}{q-1}+q^i(i+v_\infty(X)-\frac{q}{q-1})\to\infty$, si $i\to\infty$.

Finalment, tenim

$$\prod_{j=1}^{d-1}(1-\frac{[j]}{[j+1]}) = \prod_{j=1}^{d-1}\frac{[j+1]-[j]}{[j+1]} = \prod_{j=1}^{d-1}\frac{[1]^{q^j}}{[j+1]},$$

que ens dóna

$$\frac{\prod_{j=1}^{d-1}[1]^{q^j}}{L_d} = \frac{[1]^{q^{(d-1)/(q-1)}}}{L_d} = \frac{\beta_d}{L_d} = \xi_d.$$

□

2.1.9 Teorema. *Sigui* $\xi := \lambda\xi_* \in \overline{K_\infty}$, *amb* $\lambda^{q-1} = -[1]$. *Per a tot* $x \in \mathbb{C}_\infty$, *es té*

$$x \prod_{0\neq\alpha\in\mathbb{A}} (1 - \frac{x}{\alpha}) = \frac{1}{\xi} e_C(\xi x).$$

2.1.10 Corol·lari. *Posem* $\Lambda := \xi\ \mathbb{A} \subset \overline{K_\infty}$. *Per a tot* $x \in \mathbb{C}_\infty$, *tenim*

$$x \prod_{0\neq\alpha\in\Lambda} (1 - \frac{x}{\alpha}) = e_C(x).$$

Demostració: Recordem que per definició

$$e_C(x) = \sum_{i=0}^{\infty} \frac{x^{q^i}}{D_i},$$

i que per (4) del lema anterior

$$x \prod_{0\neq\alpha\in\mathbb{A}} (1 + \frac{x}{\alpha}) = \frac{1}{\xi_*} \sum_{i=0}^{\infty} (-1)^i \beta_i\ \xi_*^{q^i}\ \frac{x^{q^i}}{D_i}.$$

Ara,

$$\beta_i = ((-\lambda)^{q-1})^{\frac{q^i-1}{q-1}} = (-1)^i \lambda^{q^i-1},$$

$$(-1)^i\ \beta_i\ \xi_*^{q^i-1} = \lambda^{q^i-1} \xi_*^{q^i-1} = \xi^{q^i-1}.$$

Així,

$$x \prod_{0\neq\alpha\in\mathbb{A}} (1 + \frac{x}{\alpha}) = \sum_{i=0}^{\infty} \xi^{q^i-1}\ \frac{x^{q^i}}{D_i} = \frac{1}{\xi} e_C(\xi x).$$

□

Renormalitzant, obtenim el corol.lari.

2.1.11 Observació. 1. El corol.lari ens dóna la factorització de e_C que volíem.

2. Hem normalitzat $e_C(x)$ de manera diferent als treballs originals de Carlitz, seguint [Go 96].

3. ξ és un periode i $\Lambda = \xi\mathbb{A}$ la xarxa dels zeros de $e_C(x)$. Com que aquí una funció entera no constant és exhaustiva, tenim que e_C ens dóna l'isomorfisme

$$\mathbb{C}_\infty/\Lambda \backsimeq^{e_C} \mathbb{C}_\infty.$$

2.2 El mòdul de Carlitz

L'exponencial de Carlitz $e_C(x)$ defineix una nova acció de $\mathbb{A}$-mòdul a $\mathbb{C}_\infty$ que és el que anomenarem mòdul de Carlitz.

Com en el Capítol 1, sigui $\tau : \mathbb{C}_\infty \to \mathbb{C}_\infty$ l'aplicació potència q-èssima $\tau(x) = x^q$. Per cada subcos M de $\mathbb{C}_\infty$, sigui $M\{\tau\}$ l'anell composició de polinomis $\mathbb{F}_q$-lineals.

2.2.1 Proposició. *Es compleix:*

1. *Per a tot $a \in \mathbb{A}$, existeix un polinomi $C_a(X) \in \mathbb{A}[X]$ tal que*

$$e_C(ax) = C_a(e_C(x)),$$

per a tot $x \in \mathbb{C}_\infty$.

2. *El polinomi $C_a(X)$ és £nic i és $\mathbb{F}_q$-lineal. A més, l'aplicació:*

$$C : \mathbb{A} \to \mathbb{A}\{\tau\}$$

que assigna $a \mapsto C_a(\tau)$, és un morfisme injectiu de $\mathbb{F}_q$-àlgebres.

3. *Explícitament el polinomi de Carlitz és:*

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{d} a_j \tau^j,$$

amb $d = \deg a$, a_d el coeficient principal de a i els coeficients a_j, $1 \leq j < d$, estan determinats per:

$$a_1 = \frac{a^q - a}{T^q - T}, \qquad a_2 = \frac{a_1^q - a_1}{T^{q^2} - T}, ..., a_j = \frac{a_{j-1}^q - a_{j-1}}{T^{q^j} - T}, ...$$

DEMOSTRACIÓ: Com a aplicació de $\mathbb{C}_\infty$ en $\mathbb{C}_\infty$, C_a està unívocament determinada i és $\mathbb{F}_q$-lineal. Com que hereta les propietats de "multiplicar perïï, és suficient provar que C_T és un polinomi amb coeficients a $\mathbb{A}$. Ara,

$$e_C(Tx) - Te_C(x) = \sum_{i=0}^{\infty}(T^{q^r} - T)\frac{x^{q^i}}{D_{i-1}} = \sum_{i=1}^{\infty}\frac{x^{q^i}}{D_{i-1}} = (e_C(x)^q).$$

Posem $C_1 = x = \tau^0$. Per tant

$$C_T(x) = Tx + x^q = T\tau^0 + \tau.$$

L'aplicació $a \mapsto C_a$ és $\mathbb{F}_q$-lineal i injectiva. Tenim

$$C_{ab}(e_C(X)) = e_C(abx) = e_c(a(bx)) = C_a(e_C(bx)) = C_a(C_b(e_C(x))),$$

per tant $C_{ab} = C_a.C_b$. Finalment obtenim (3),comparant coeficients i tenint en compte que

$$C_TC_a = C_aC_T$$

a $\mathbb{A}\{\tau\}$. □

Notem que en particular, els polinomis $C_a(X)$ són separables, si $a \neq 0$. D'altra banda, l'apartat (1) de la proposició ens diu el següent diagrama és commutatiu:

$$\begin{array}{ccc} \mathbb{C}_\infty/\Lambda & \stackrel{a}{\to} & \mathbb{C}_\infty/\Lambda \\ \downarrow e_c & & \downarrow e_c \\ \mathbb{C}_\infty & \stackrel{C_a}{\to} & \mathbb{C}_\infty. \end{array}$$

Ara, per tenir el mòdul de Carlitz copiem a $\mathbb{C}_\infty$ l'estructura de $\mathbb{A}$-mòdul de $\mathbb{C}_\infty/\Lambda$, via l'isomorfisme e_C i mitjançant el diagrama anterior. És a dir, si $x \in \mathbb{C}_\infty$ i $x = e_C(y)$, definim:

$$(a, x) = (a, e_C(y)) := e_C(ay) = C_a(e_C(y)) = C_a(x).$$

2.2.2 Definició El **Mòdul de Carlitz** és el morfisme de $\mathbb{F}_q$-àlgebres

$$C : \mathbb{A} \to \mathbb{A}\{\tau\}$$

que assigna $a \mapsto C_a(\tau)$.

Podem pensar C com un functor de la categoria de $\mathbb{A}$-àlgebres a la de $\mathbb{A}$-mòduls,

$$\underline{\mathrm{Alg}}_{\mathbb{A}} \to^{C} \underline{\mathrm{Mod}}_{\mathbb{A}},$$

que assigna a cada $\mathbb{A}$-àlgebra B l'$\mathbb{A}$-mòdul $C(B)$que s'obté prenent B amb l'estructura de $\mathbb{A}$-mòdul

$$(a, b) := C_a(b),$$

on $b \in B$, $a \in \mathbb{A}$. Aquesta acció functorial és el mòdul de Carlitz.

2.3 Punts de divisió del mòdul de Carlitz

2.3.1 Definició Els punts de divisió del mòdul de Carlitz és el conjunt de valors:

$$\{e_C(a\xi), a \in K\} \subset \mathbb{C}_\infty.$$

Si $a = b/f \in K$, $b, f \in \mathbb{A}$ i $f \neq 0$, aleshores $e_C(a\xi)$ és un zero de del polinomi $C_f(x)$, doncs

$$C_f(e_C(a\xi)) = e_C(fa\xi) = e_C(b\xi) = 0.$$

En particular, els elements $e_C(a\xi)$ estan en una clausura algebraica de K i per tant a $\mathbb{C}_\infty$. Notem que de fet $e_C(a\xi)$ és un element de f torsió, doncs:

$$(f, e_C(a\xi)) = C_f(e_C(a\xi)) = 0.$$

2.3.2 Teorema. *Sigui $L \subset \mathbb{C}_\infty$ un cos extensió de K. Sigui $a \in K$ i $L_1 = L(e_C(a\xi))$. Aleshores L_1 és una extensió abeliana de L.*

Demostració: Si $a = b/f$ és irreductible, $b, f \in \mathbb{A}$, tenim

$$e_C(\frac{b}{f}\xi) = C_b(e_C(\frac{\xi}{f})),$$

per tant $L_1 \subset L(e_C(\frac{\xi}{f}))$. D'altra banda, com que els coeficients dels polinomis $C_g(\tau)$ són a $\mathbb{A}$, tenim que tots els valors $e_C(\frac{g}{f}\xi)$ pertanyen a $L(e_C(\frac{\xi}{f}))$. És a dir,

$$L_1 = L(e_C(\frac{\xi}{f}))$$

conté tots els punts de f-divisió. A més, la funció exponencial de Carlitz ens diu que el $\mathbb{A}$-mòdul dels punts de f-divisió és isomorf a $\mathbb{A}/(f)$ com $\mathbb{A}$-mòdul. Així, la extensió L_1/L és Galois, sigui G el seu grup de Galois. Com que $C_g(\tau) \in \mathbb{A}\{\tau\}$, per a tot g, tenim que l'acció de G sobre els punts de f-divisió commuta amb la acció de $\mathbb{A}$. Per tant, si $\rho = e_C(\frac{\xi}{f})$ i $\sigma \in G$, $\sigma(\rho)$ és un generador del $\mathbb{A}$-mòdul dels punts de f-divisió. En conseqüència tenim una injecció $G \hookrightarrow \mathbb{A}/(f)^*$, que ens diu que el grup G és abelià. □

2.3.3 Definició Sigui $g \in \mathbb{A}$, posem

$$C[g] := \{e_C(\frac{b}{g}\xi), b \in \mathbb{A}\} \subset \mathbb{C}_\infty,$$

que anomenem el mòdul dels punts de g-divisió.

$C[g]$ és isomorf com $\mathbb{A}$-mòdul a $\mathbb{A}/(g)$. Un generador de $C[g]$ com $\mathbb{A}$-mòdul s'anomena un punt de g-divisió primitiu. Notem que $C[g]$ depend només de l'ideal que genera g a $\mathbb{A}$. En altres paraules:

$$C[g] = C[g\zeta],$$

si $\zeta \in \mathbb{F}_q^*$.

2.4 Mòdul de Carlitz sobre $\mathbb{A}$-cossos

Volem estudiar mòduls de Carlitz sobre cossos arbitraris contenint $\mathbb{F}_q$.

2.4.1 Definició Un $\mathbb{A}$-*cos és un parell* (L, ι), on L és un cos, $L \supset \mathbb{F}_q$, i

$$\iota : \mathbb{A} \to L$$

és un homomorfisme d'anells.

S'anomena *característica de* (L, ι) a l'ideal primer

$$\mathfrak{p} = \ker(\iota).$$

(L, ι) té característica genèrica si $\mathfrak{p} = (0)$.

Tenim que (L, ι) és un *mòdul de Carlitz*. El morfisme de $\mathbb{F}_q$-àlgebres

$$C : \mathbb{A} \to L\{\tau\}$$
$$a \mapsto C_a(\tau).$$

De fet, apliquem ι al polinomi $C_a(\tau) \in \mathbb{A}\{\tau\}$, per $a \in \mathbb{A}$ i obtenim un element de $L\{\tau\}$.

2.4.2 Observació. 1. Si $M \supset L$ cos, hereta l'estructura de $\mathbb{A}$-cos i de $\mathbb{A}$-mòdul.

2. $C_a(X)' = \iota(a)$, $a \in \mathbb{A}$.

3. El polinomi $C_a(X)$ és separable si i només si $a \notin \mathfrak{p}$.

4. Si (L, ι) té característica genèrica aleshores $L \supset K$.

Sigui (L, ι) un $\mathbb{A}$-cos i $\overline{L}$ una clausura algebraica fixada.

Via C, el cos $\overline{L}$ és un $\mathbb{A}$-mòdul:

$$a.\alpha = (a, \alpha) \longmapsto C_a(\alpha),$$

on $a \in \mathbb{A}$ i $\alpha \in \overline{L}$.

Diem que α és un punt de a-torsió si i només si $C_a(\alpha) = 0$.

El conjunt de punts punts de a-torsió del mòdul de Carlitz és:

$$C[a] := \{x \in C(\overline{L}) |\ a.x = 0\} = \{\text{arrels de } C_a(x) \text{ a } \overline{L}\},$$

sub-$\mathbb{A}$-mòdul finit de $C(\overline{L})$. En el cas $L = \mathbb{C}_\infty$, hem vist que els punts de a-torsió venen parametritzats per l'exponencial de Carlitz.

Per a la torsió en $\mathbb{A}$-cossos tenim:

2.4.3 Teorema. *Sigui* (L, ι) *un* $\mathbb{A}$*-cos de característica* $\mathfrak{p} \in$ *Spec*$(\mathbb{A})$.

1. *Sigui $a \notin \mathfrak{p}$ aleshores $C[a] \cong \mathbb{A}/(a)$ com a $\mathbb{A}$-mòdul.*
2. *Si $(f) = \mathfrak{p}$ aleshores $C[f^i] = \{0\} \subset \overline{L}$.*

Bibliografia

[Ca 35] Carlitz, L.: On certain functions connected with polynomials in a Galois field. *Duke Math. J.* **1** (1935), 137-168.

[Go 96] Goss, D.: Basic Structures of Function Field Arithmetic. Springer, 1996.

N. Vila
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les corts Catalanes 585, E-08007 Barcelona,
vila@mat.ub.es

Capítol 3

Uniformització analítica rígida de mòduls de Drinfeld

Victor Rotger

3.1 Preliminars

Sigui X una corba projectiva, llisa i geomètricament connexa sobre el cos finit $\mathbb{F}_q$ de $q = p^a$ elements. Sigui $\infty \in X(\overline{\mathbb{F}_q})$ un punt tancat de grau d_∞ sobre $\mathbb{F}_q$ i sigui $[\infty] \in \mathrm{Pic}^{d_\infty}(X)(\mathbb{F}_q)$ el divisor format per l'òrbita galoisiana del punt ∞.

Considerem $K = \mathbb{F}_q(X)$ el cos de funcions racionals de X i

$$\mathbb{A} = \bigcap_{P \notin \mathrm{Sup}[\infty]} \mathcal{O}_{X,P}$$

l'anell de funcions de X regulars fora de ∞.

Sigui K_∞ la completació de K respecte la valoració discreta d_∞ associada a ∞ i $\mathbb{C}_\infty$ la completació d'una clausura algebraica fixada de K_∞.

Partially supported by a grant FPI from Ministerio de Educación y Ciencia and by Ministerio de Ciencia y Tecnología BFM2000-0627

L'anell $\mathbb{A}$ és un domini de Dedekind amb cos de fraccions K i tenim una bijecció

$$\mathrm{Max}(A) = (\, X(\overline{\mathbb{F}_q}) \setminus \mathrm{Sup}[\infty] \,) \setminus \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$$

Cada element $a \in \mathbb{A}$, $a \neq 0$, descompon en l'anell $\mathbb{A}$ com $(a) = \prod_{\wp \in \mathrm{Max}(\mathbb{A})} \wp^{n_\wp}$ i per tant té un divisor associat

$$\mathrm{div}(a) = \sum_{\wp \in \mathrm{Max}(\mathbb{A})} n_\wp \mathrm{div}(\wp) - n_\infty [\infty],$$

on $\mathrm{div}(\wp)$ denota l'òrbita galoisiana sencera associada a l'ideal primer $\wp$ per la bijecció anterior.

Respecte la valoració discreta associada al punt ∞, tenim que

$$\mathrm{ord}_\infty(a) = -n_\infty.$$

Com $\deg(\mathrm{div}(a)) = 0$ i $\deg(\infty) = d_\infty$, es compleix que

$$\sum n_\wp \deg(\wp) = n_\infty d_\infty.$$

Anomenarem $\deg(a)$ al valor de qualsevol d'aquestes dues quantitats i estenem aquest concepte a tots els elements de K^*:

$$\deg(x) := -d_\infty \,\mathrm{ord}_\infty(x).$$

Observem que si $a \in \mathbb{A} \setminus \{0\}$, es satisfà que $\sharp \mathbb{A}/(a) = q^{\deg(a)}$.

Agraïments. Aquestes notes són la versió escrita i reduïda d'unes xerrades que va fer el Dr. Enric Nart a la Universitat Autònoma de Barcelona. Qualsevol mèrit d'aquestes notes se li ha d'atribuir a ell. Els errors, en qualsevol cas, són meus.

3.2 Mòduls de Drinfeld

Sigui $\mathbb{A} \overset{i}{\hookrightarrow} \mathcal{F}$ un $\mathbb{A}$-cos de característica $\wp = \ker(i)$.

3.2.1 Definició Un mòdul de Drinfeld sobre l'$\mathbb{A}$-cos $\mathbb{A} \overset{i}{\hookrightarrow} \mathcal{F}$ és un homomorfisme d'anells

$$\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$$

satisfent:

1. $\phi_a(\tau) = i(a)\tau^0 + ...$, per tot $a \in \mathbb{A}$
2. $\exists a \in \mathbb{A} : \phi_a(\tau) = i(a)\tau^0$.

De la mateixa definició se'n segueix la següent

3.2.2 Proposició. *Sigui $\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$ un mòdul de Drinfeld. Aleshores,*

1. *Si $\lambda \in \mathbb{F}_q$, $\phi_\lambda(\tau) = i(\lambda)\tau^0$*
2. *ϕ és un monomorfisme de $\mathbb{F}_q$-àlgebres*
3. *$\phi_a(\tau)$ és separable si i només si $a \notin \wp$.*

3.2.3 Definició Un morfisme $\phi \overset{P}{\to} \psi$ entre mòduls de Drinfels sobre un $\mathbb{A}$-cos $\mathbb{A} \overset{i}{\hookrightarrow} \mathcal{F}$ és un polinomi $P(\tau) \in \mathcal{F}\{\tau\}$ tal que

$$P\phi_a = \phi_a P,$$

per tot $a \in \mathbb{A}$.

Si interpretem $\mathcal{F}\{\tau\} = \mathrm{End}(\mathcal{G}_{a,\mathcal{F}})$ com l'anell d'endomorfismes de l'esquema en grups additiu sobre $\mathcal{F}$, l'homomorfisme $\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$ es pot entendre com una estructura functorial d'$\mathbb{A}$-mòduls sobre qualsevol $\mathcal{F}$-àlgebra en la qual, multiplicar per a consisteix a avaluar el polinomi $\phi_a(x)$ obtingut en substituir $\tau = x^q$:

$$\begin{array}{rccc} \phi : & \underline{Alg}_{\mathcal{F}} & \to & \underline{Mod}_{\mathbb{A}} \\ & R & \mapsto & \phi(R) \end{array}$$

on $\phi(R)$ és l'àlgebra R amb l'estructura d'$\mathbb{A}$-mòdul:

$$a \cdot r = \phi_a(r), \quad a \in \mathbb{A}, \quad r \in R.$$

Anàlogament, un morfisme $\phi \xrightarrow{P} \psi$ de mòduls de Drinfeld es tradueix en un homomorfisme functorial d'$\mathbb{A}$-mòduls que consisteix a avaluar el polinomi $P(x)$:

$$\begin{array}{ccc} \phi(R) & \xrightarrow{P} & \psi(R) \\ r & \mapsto & P(r). \end{array}$$

3.2.4 Definició Sigui $\overline{\mathcal{F}}$ una clausura algebraica fixada de $\mathcal{F}$. Per a qualsevol $a \in \mathbb{A}$ definim l'espai vectorial sobre $\mathbb{F}_q$ dels punts d'a-divisió del mòdul de Drinfeld $\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$ com:

$$\phi[a] := \{x \in \phi(\overline{\mathcal{F}} : a \cdot x = 0)\} = \{\text{Arrels de}\, \phi_a(x)\, \text{en}\, \overline{\mathcal{F}}\}.$$

Els punts d'a-divisió és un sub-$\mathbb{A}$-mòdul finit de $\phi(\overline{\mathcal{F}})$. Per abús de llenguatge també denotarem per $\phi[a]$ el subesquema en grups finit sobre $\mathcal{F}$ de $\mathbb{G}_{a,\mathcal{F}}$ determinat per

$$\phi[a] := \mathrm{Spec}(\mathcal{F}[x]/(\phi_a(x))),$$

de manera que els punts de a-divisió són els punts $\overline{\mathcal{F}}$-valorats d'aquest esquema en grups.

Més generalment, si $\mathfrak{a}$ és un ideal no nul de $\mathbb{A}$, definim

$$\phi[\mathfrak{a}] := \{x \in \phi(\overline{\mathcal{F}}) : \phi_a(x) = 0, \forall a \in \mathfrak{a}\}.$$

3.3 Rang i altura

Considerem les aplicacions

$$\mathcal{F}\{\tau\} \xrightarrow{-\deg} \mathbb{Z} \cup \{\infty\}$$

i

$$\mathcal{F}\{\tau\} \xrightarrow{-\mathrm{ht}} \mathbb{Z} \cup \{\infty\}$$

on $\mathrm{ht}(P)$ i $\deg(P)$ són els graus mínim i màxim entre els monomis no nuls de $P(\tau)$:

$$P(\tau) = a_h\tau^h + \ldots a_n\tau^n, \quad a_h, a_n \neq 0.$$

Les funcions ht i $-\deg$ comparteixen les següents propietats:

- $\mathrm{ht}(PQ) = \mathrm{ht}(P) + \mathrm{ht}(Q)$
- $\mathrm{ht}(P+Q) \geq \min\{\mathrm{ht}(P), \mathrm{ht}(Q)\}$
- $\mathrm{ht}(P) = \infty \Leftrightarrow P = 0$

Per tant, component amb $\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$, obtenim dues valoracions discretes de $\mathbb{A}$. Com a tals, han de ser equivalents a ord_P per a algun punt P de la corba X. De seguida observem que

- $-\deg\cdot\phi$ és equivalent a ord_∞
- $\mathrm{ht}\cdot\phi$ és trivial si $\wp = (0)$ i equivalent a $\mathrm{ord}_\wp$ si $\wp \neq (0)$.

En efecte, $-\deg\cdot\phi$ pren un valor ≤ 0 en tots els elements $a \in \mathbb{A}$; per tant no pot ser equivalent a cap altra que $\mathrm{ord}_\wp$. D'altra banda, $\mathrm{ht}\cdot\phi$ s'anul·la exactament sobre $\mathbb{A} \setminus \wp$.

Per tant existeixen $d, h \in \mathbb{Q}^+$ tals que, per tot $a \in \mathbb{A}$:

$$-\deg(\phi_a(\tau)) = d \cdot d_\infty \,\mathrm{ord}_\infty(a) = -d\deg(a),$$

$$\mathrm{ht}(\phi_a(\tau)) = h\deg(\wp)\,\mathrm{ord}_\wp(a),$$

on els termes $d_\infty = \deg(\infty)$ i $\deg(\wp)$ s'han introduit per normalitzar.

3.3.1 Teorema. (Drinfeld) *1. d és un enter positiu anomenat* rang de ϕ. *Per a qualsevol ideal $\mathfrak{a}$ d'$\mathbb{A}$ coprimer amb $\wp$ es té que*

$$\phi[\mathfrak{a}] \simeq (\mathbb{A}/\mathfrak{a})^d,$$

com a $\mathbb{A}$-mòduls.

2. *Si $\wp \neq 0$, h és un enter positiu anomenat* altura de ϕ. *Per a $\mathfrak{a} = \wp^m$ es té que*
$$\phi[\mathfrak{a}] \simeq (\mathbb{A}/\mathfrak{a})^{d-h},$$
com a $\mathbb{A}$-mòduls.

3.3.2 Corol·lari. *Entre dos mòduls de Drinfeld de diferent rang, l'únic morfisme és el* 0.

3.3.3 Exemple. Sigui $\mathbb{A} = \mathbb{F}_q[T]$ i $\phi = C$ el mòdul de Carlitz. Com $C_T(\tau) = T\tau^0 + \tau$, el rang de C és 1 sobre qualsevol $\mathbb{A}$-cos.

Si $\mathbb{A} \overset{i}{\hookrightarrow} \mathcal{F}$ és un $\mathbb{A}$-cos de característica $\wp \neq 0$, aleshores l'altura de C és 1 i $C[\wp^n] = \{0\}$.

3.4 Mòdul de Drinfeld associat a una xarxa

Fixem un subcos complet de $\mathbb{C}_\infty$, $K_\infty \subseteq M \subseteq \mathbb{C}_\infty$ i el considerem com a $\mathbb{A}$-cos amb l'estructura natural donada per la inclusió $\mathbb{A} \subset M$, de manera que la característica és $\wp = (0)$.

Com en el cas de les corbes el·líptiques sobre $\mathbb{C}$, els mòduls de Drinfeld sobre M estan classificats per xarxes. Definirem el concepte de M-xarxa i establirem un functor

$$\begin{array}{ccc} \underline{\text{Xarxes}}_M & \longrightarrow & \underline{\text{Drin}}_M \\ L & \mapsto & \phi_L, \end{array}$$

que serà una equivalència de categories.

3.4.1 Definició Una M-xarxa és un sub-$\mathbb{A}$-mòdul $L \subseteq \mathbb{C}_\infty$ que satisfà

1. L és finitament generat com a $\mathbb{A}$-mòdul
2. L és discret per la topologia de $\mathbb{C}_\infty$
3. L està inclòs en la clausura separable M^{sep} de M i és estable per $\text{Gal}(M^{\text{sep}}/M)$.

Tota M-xarxa dóna lloc a una funció exponencial:

$$\begin{array}{rccc} e_L: & \mathbb{C}_\infty & \longrightarrow & \mathbb{C}_\infty \\ & x & \mapsto & e_L(x) = x \cdot \prod_{\alpha \in L \setminus \{0\}} (1 - \frac{x}{\alpha}), \end{array}$$

determinada per la funció entera que té com a zeros simples els punts de la xarxa L i satisfà $e'_L(0) = 1$ (cf. [Go], 2.14).

3.4.2 Proposició. *La funció e_L és una funció entera i $\mathbb{F}_q$-lineal. La seva expansió de Taylor al voltant del 0 té coeficients a M. En particular, $e_L(M) \subseteq M$.*

Com en el cas de la funció exponencial de Carlitz, tenim ara un isomorfisme $\mathbb{F}_q$-lineal:

$$\mathbb{C}_\infty \xrightarrow{e_L} \mathbb{C}_\infty$$

que permet obtenir una estructura d'$\mathbb{A}$-mòdul sobre $\mathbb{C}_\infty$ copiant l'estructura de $\mathbb{C}_\infty/L$ via e_L. El següent resultat de Drinfeld ens mostra que aquesta estructura prové d'un mòdul de Drinfeld.

3.4.3 Teorema. *Per tot $a \in \mathbb{A} \setminus \{0\}$,*

$$e_L(ax) = a \cdot e_L(x) \cdot \prod_{0 \neq \alpha \in a^{-1}L/L} (1 - \frac{e_L(x)}{e_L(\alpha)}),$$

per tot $x \in \mathbb{C}_\infty$.

Observem que a posteriori, de la igualtat $e_L(ax) = \phi_a(e_L(x))$ i de la proposició anterior, es dedueix que $\phi_a(x)$ té coeficients a M, és a dir:

$$\phi_a \in M\{\tau\}.$$

3.4.4 Proposició. $\mathbb{A} \xrightarrow{\phi} M\{\tau\}$ *és un mòdul de Drinfeld de rang $d = \mathrm{rang}_{\mathbb{A}}(L)$.*

Sigui $\underline{\mathrm{Xarxes}}_M$ la categoria que té per a objectes les M-xarxes i per morfismes:

$$\mathrm{Mor}(L_1, L_2) = \{0\} \text{ si } L_1 \text{ i } L_2 \text{ tenen rang diferent,}$$

$\mathrm{Mor}(L_1, L_2) = \{c \in \mathbb{C}_\infty : cL_1 \subseteq L_2\}$ si L_1 i L_2 tenen el mateix rang.

3.4.5 Proposició. *La construcció anterior determina un functor*

$$\begin{array}{ccc} \underline{Xarxes}_M & \longrightarrow & \underline{Drin}_M \\ L & \mapsto & \phi_L, \end{array}$$

que conserva el rang.

L'objectiu de la resta d'aquest capítol és construir el functor invers del functor anterior, per tal de demostrar que es tracta d'una equivalència de categories.

3.5 K-mòduls formals i el teorema d'uniformització analítica

3.5.1 Definició Un K-mòdul formal sobre M és un homomorfisme d'anells $K \xrightarrow{\psi} M\{\{\tau\}\}$ tal que $\psi_a(\tau) = a\tau^0 + \ldots$, per a tot $a \in K$.

3.5.2 Lema. *Sigui α un element transcendent sobre $\mathbb{F}_q$ i sigui $f(\tau) = \alpha\tau^0 + a_1\tau + \cdots \in M\{\{\tau\}\}$. Aleshores existeix una única*

$$\lambda_f(\tau) = \tau^0 + c_1\tau + ... \in M\{\{\tau\}\}$$

tal que

$$f = \lambda_f(\alpha\tau)\lambda_f^{-1}$$

3.5.3 Corol·lari. *Amb les mateixes hipòtesis, el centralitzador de f a $M\{\{\tau\}\}$ és $\lambda_f(M\tau^0)\lambda_f^{-1}$.*

3.5.4 Proposició. *Per a tot K-mòdul formal $K \xrightarrow{\psi} M\{\{\tau\}\}$ existeix una única sèrie $e_\psi \in M\{\{\tau\}\}$ ambterme idependent 1 que satisfà:*

$$\psi_a = e_\psi(a\tau^0)e_\psi^{-1}$$

per tot $a \in K$.

Observem que si $\psi : \mathbb{A} \to M\{\tau\}$ és un mòdul de Drinfeld sobre M, aleshores $\psi_a(\tau) = a\tau^0 + ...$ és invertible a $M\{\{\tau\}\}$ si $a \neq 0$ i la seva inversa comença $\frac{1}{a}\tau^0 + ...$

Per tant, ψ indueix de manera natural un K-mòdul formal. Fent servir la unicitat, es pot comprovar que si ψ és el mòdul de Drinfeld associat a una xarxa L, aleshores la sèrie e_ψ coincideix amb l'exponencial e_L construïda anteriorment.

La sèrie e_ψ és la clau per a veure que tot mòdul formal prové d'una xarxa. Ho recollim en el següent teorema de Drinfeld, la demostració del qual pot trobar-se a [Go].

3.5.5 Teorema. *Sigui $\mathbb{A} \xrightarrow{\psi} M\{\tau\}$ un mòdul de Drinfeld sobre M de rang d i sigui e_ψ la sèrie associada al K-mòdul formal determinat per ψ. Aleshores*

1. *e_ψ defineix una funció entera $\mathbb{C}_\infty \to \mathbb{C}_\infty$*
2. *$L_\psi = \ker(e_\psi)$ és una M-xarxa de rang d.*
3. *Si $\phi \xrightarrow{P} \psi$ és un morfisme de mòduls de Drinfeld, existeix $c \in M$ tal que $cL_\phi \subseteq L_\psi$ i el diagrama següent commuta:*

$$\begin{array}{ccc} \mathbb{C}_\infty & \xrightarrow{c} & \mathbb{C}_\infty/L_\psi \\ e_\phi \downarrow & & \downarrow e_\psi \\ \mathbb{C}_\infty & \xrightarrow{P} & \mathbb{C}_\infty \end{array}$$

4. *El functor $\psi \mapsto L_\psi$ és invers del functor $L \mapsto L_\phi$.*

Bibliografia

[Goss] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin-Heidelberg, 1998.

Victor Rotger
Universitat Politècnica de Catalunya,
Departament de Matemàtica Aplicada IV (EUPVG),
Av. Victor Balaguer s/n,
08800 Vilanova i la Geltrú,
Spain.
vrotger@mat.upc.es

Capítol 4

Isogenias, Reducción y Módulos de Tate

Luis V. Dieulefait

4.1 Morfismos de Módulos de Drinfeld: Isogenias

Sea $\mathcal{F}$ un $\mathbb{A}$-cuerpo vía el morfismo (que fijamos):

$$\iota : \mathbb{A} \to \mathcal{F}$$

y $\bar{\mathcal{F}}$ su clausura algebraica. Sean ϕ, ψ módulos de Drinfeld de rango $d > 0$.
Un morfismo de ϕ a ψ sobre $\mathcal{F}$ es un elemento $P(\tau) \in \mathcal{F}\{\tau\}$ que verifica:

$$P\phi_a = \psi_a P$$

para todo $a \in \mathbb{A}$. Tales morfismos forman un $\mathbb{A}$-módulo libre de torsión llamado $\mathrm{Hom}_{\mathcal{F}}(\phi, \psi)$ donde la acción de un elemento $b \in \mathbb{A}$ viene dada por:

$$(b, P) := P\phi_b = \psi_b P$$

en homenaje a Luis Santaló (1911-2001), geómetra excelso

y se tiene: $(P\phi_b)\phi_a = P\phi_a\phi_b = \psi_a\psi_b P = \psi_a(P\phi_b)$.
Como caso particular, si $\phi = \psi$ lo denotamos $\mathrm{End}_{\mathcal{F}}(\phi)$. Nótese que es un subanillo de $\mathcal{F}\{\tau\}$ (bajo la composición).

4.1.1 Proposición *$P \in \mathrm{Hom}_{\mathcal{F}}(\phi, \psi)$ es un isomorfismo si y sólo si el grado de P es 0.*

Demostración: P es isomorfismo si y sólo si existe $Q \in \mathcal{F}\{\tau\}$ con $P \cdot Q = \tau^0$, pues τ^0 es la identidad (recordar que la operación es composición).

4.1.2 Proposición *Sea $\alpha \in \bar{\mathcal{F}}$ un punto de a-división de ϕ. Entonces $P(\alpha)$ es un punto de a-división de ψ.*

Demostración: Inmediato de la definición de morfismo.

4.1.3 Proposición *La inclusión natural:*

$$\mathrm{Hom}_{\mathcal{F}^{sep}}(\phi, \psi) \hookrightarrow \mathrm{Hom}_{\mathcal{G}}(\phi, \psi)$$

es una igualdad, para todo cuerpo $\mathcal{G}$ algebraicamente cerrado que contenga a la clausura separable de $\mathcal{F}$.

Demostración: Tenemos que verificar que los coeficientes de cualquier $P \in \mathrm{Hom}_{\mathcal{G}}(\phi, \psi)$ son algebraicos y separables sobre $\mathcal{F}$.
Dado un tal P tomemos $a \in \mathbb{A}$ coprimo (:= relativamente primo) con la característica de $\mathcal{F}$ y de grado elevado:

$$\deg \phi_a(\tau) = \deg \psi_a(\tau) > \deg P(\tau)$$

Como $\phi_a(\tau)$ y $\psi_a(\tau)$ son separables y P manda $\phi[a]$ en $\psi[a]$, el resultado se sigue del teorema de interpolación de Lagrange.

4.1.4 Proposición *Si la característica de $\mathcal{F}$ es cero, entonces $\mathrm{End}_{\mathcal{F}}(\phi)$ es conmutativo.*

Demostración: Se sigue de la uniformización analítica, pues tenemos las inclusiones:

$$\mathrm{End}_{\mathcal{F}}(\phi) \subseteq \mathrm{End}_{\mathcal{F}^{sep}}(\phi) = \mathrm{End}_{\mathbb{C}_\infty}(\phi) = \mathrm{End}_{\mathbb{A}}(L_\phi)$$

donde L_ϕ es el retículo conmutativo que corresponde a ϕ.

4.1.5 Teorema *El $\mathbb{A}$-módulo $M := \mathrm{End}_{\mathcal{F}}(\phi)$es proyectivo y de rango menor o igual a d^2.*

Idea de la demostración: Recordemos que M es un $\mathbb{A}$-módulo pero con una acción de $\mathbb{A}$ altamente no trivial, pues actúa vía ϕ. Por estar contenido en $\mathcal{F}\{\tau\}$ sabemos que M es libre de torsión. Considerando a M como submódulo discreto de $M \otimes_{\mathbb{A}} K_\infty$ puede verse que este espacio tiene dimensión finita sobre K_∞, y por lo tanto concluir que M es finitamente generado. Luego, aplicando el teorema de estructura de módulos finitamente generados sobre un dominio de Dedekind ($\mathbb{A}$ en nuestro caso) tenemos (pues es libre de torsión):

$$M \cong \mathbb{A} \oplus \mathbb{A} \oplus .... \oplus \mathbb{A} \oplus I$$

donde I es un ideal de $\mathbb{A}$ (todo ideal de $\mathbb{A}$ es proyetivo como $\mathbb{A}$-módulo).
Para acotar el rango, probemos que para $a \notin \wp$ ($\wp :=$ característica de $\mathcal{F}$) la aplicación natural:

$$M/aM \mapsto \mathrm{End}_{\mathbb{A}}(\phi[a])$$

es inyectiva. Supongamos que $P \in M$ se anula sobre $\phi[a]$. Como ϕ_a es separable: $P = Q \cdot \phi_a$, con $Q \in \mathcal{F}\{\tau\}$. Ejercicio elemental: ver que debe ser $Q \in \mathrm{End}_{\mathcal{F}}(\phi)$. Luego: $P = Q \cdot \phi_a = \phi_a \cdot Q$, y por lo tanto $P \in aM$. Esto prueba la inyectividad.
Llamemos r al rango de M. Por un lado tenemos:

$$M/aM \cong (\mathbb{A}/a\mathbb{A})^r$$

Y por el otro:

$$\mathrm{End}_{\mathbb{A}}(\phi[a]) \cong \mathcal{M}_d(\mathbb{A}/(a))$$

(álgebra de matrices). De la inyectividad anterior se desprende que

$$r \leq d^2$$

4.1.6 Definición *Llamaremos isogenias a los morfismos (sobre* $\mathbb{F}$*, entre* ϕ *y* ψ*) no nulos.*
P es isogenia separable cuando $P(\tau)$ *es separable.*
P es isogenia puramente inseparable cuando $P(\tau) = \tau^j$ *para algún* $j > 0$.

4.1.7 Proposición *Sea P isogenia inseparable de* ϕ *en* ϕ *sobre* $\mathbb{F}$*. Entonces* $\mathbb{F}$ *debe tener característica finita* $\wp$*. Además si* $\deg \wp = d$*, el exponente j (en la definición anterior) debe ser múltiplo de d.*

4.1.1 Subesquemas en grupo finitos y núcleos de isogenias

Los subesquemas en grupo finitos de $\mathbb{G}_{a,\mathbb{F}}$ ($\mathbb{F}_q$-lineales) son de la forma:

$$H_P = \mathrm{Spec}(\mathbb{F}[X]/P(X)),$$

$P \in \mathbb{F}\{\tau\}$, $P \neq 0$.
Definimos la altura de H_P como la de P: $\mathrm{alto}(H_P) := \mathrm{alto}(P)$.
Observamos que: $\mathrm{alto}(H_P) = 0 \Leftrightarrow P(\tau)$ es separable $\Leftrightarrow H_P$ es étale (o sea, la componente conexa de la identidad es trivial).

Dados $P(\tau), Q(\tau) \in \mathbb{F}\{\tau\}$ son equivalentes (cf. Lema 1.3.5):

- $P(X) \mid Q(X)$
- $P(\tau)$ divide por derecha a $Q(\tau)$
- $\mathbb{F}[X]/Q(X) \twoheadrightarrow \mathbb{F}[X]/P(X)$
- $H_P \subseteq H_Q \subseteq \mathbb{G}_{a,\mathbb{F}}$
- $H_P(\bar{\mathbb{F}}) \subseteq H_Q(\bar{\mathbb{F}})$ y $\mathrm{alto}(H_P) \leq \mathrm{alto}(H_Q)$

Si P es una isogenia de ϕ en ψ definimos como núcleo de P al correspondiente esquema en grupo H_P: $\ker(P) := H_P$.
Observamos que una isogenia P es separable si y sólo si su núcleo H_P es étale y una isogenia P es puramente inseparable si y sólo si su núcleo es conexo.

4.1.8 Proposición *Sea ϕ un módulo de Drinfeld sobre $\mathbb{F}$, $P(\tau) \in \mathbb{F}\{\tau\}$ y $H := H_P$ el esquema en grupo finito correspondiente. Entonces para que exista un módulo de Drinfeld ψ sobre $\mathbb{F}$ tal que P sea una isogenia de ϕ en ψ (y por lo tanto H sea el núcleo de dicha isogenia) son necesarias y suficientes las siguientes 2 condiciones:*
(1) $H(\bar{\mathbb{F}}) \subseteq \phi(\bar{\mathbb{F}})$ es sub-$\mathbb{A}$-módulo
(2) H es étale ó la característica de $\mathbb{F}$ no es genérica y su grado divide a alto(H).

Cuando H cumpla las propiedades de la proposición anterior denotaremos $\psi := \phi/H$. Este módulo de Drinfeld está unívocamente determinado salvo isomorfismo.

4.1.9 Lema *Sean $H_1 \subseteq H_2 \subseteq \mathbb{G}_{a,\mathbb{F}}$ subesquemas en grupo tales que ambos son núcleos de isogenias desde ϕ (llamemos P_1 y P_2 a éstas). Entonces existe una isogenia P de ϕ/H_1 en ϕ/H_2 tal que*

$$P_1 \cdot P = P_2$$

4.1.10 Corolario *Para toda isogenia P de ϕ en ψ existe $a \in \mathbb{A}$ y una isogenia $\hat{P}$ de ψ en ϕ tal que:*

$$\hat{P} \cdot P = \phi_a$$

Demostración: Sea $H = \ker(P)$. $H(\bar{\mathbb{F}})$ es un sub-$\mathbb{A}$-módulo finito contenido en $\phi[a](\bar{\mathbb{F}})$ para algún $a \in \mathbb{A}$. Por otra parte $\phi/H = \psi$. Sea H_1 la imagen de $\phi[a]$ bajo la aplicación $\phi \to \psi$. Tenemos una isogenia $\psi \to \psi_1 := \psi/H_1$. Además la aplicación $\phi \to \psi \to \psi_1$ da un isomorfismo entre $\phi/\phi[a]$ y ψ_1. Luego, hemos construído la isogenia buscada.

4.1.11 Corolario *Con la notación anterior, $P \cdot \hat{P} = \psi_a$ y las isogenias determinan una relación de equivalencia en el conjunto de los módulos de Drinfeld sobre $\mathbb{F}$.*

4.1.12 Corolario $\mathrm{End}_{\mathbb{F}}(\phi) \bigotimes_A K$ *es un álgebra de división de dimensión finita sobre K.*

Más consecuencias: Mencionemos algunos resultados más que se desprenden de los anteriores:

- $\mathrm{Hom}_{\mathbb{F}}(\phi, \psi)$ es un $\mathbb{A}$-módulo proyectivo de rango menor o igual a d^2
- Si existe una isogenia de ϕ a ψ, entonces $\mathrm{End}_{\mathbb{F}}(\phi)$ y $\mathrm{End}_{\mathbb{F}}(\psi)$ tienen igual rango

4.2 Reducción de módulos de Drinfeld - Módulo de Tate

Sea $\mathbb{F}$ un $\mathbb{A}$ cuerpo vía $\iota : \mathbb{A} \to \mathbb{F}$. Sea v una valoración discreta en $\mathbb{F}$ y $\mathcal{O}_v \subseteq \mathbb{F}$ el anillo de ésta valoración. Asumimos que se tiene: $\iota(\mathbb{A}) \subseteq \mathcal{O}_v$. Sea $M_v \subseteq \mathcal{O}_v$ el ideal maximal y $F_v := \mathcal{O}_v/M_v$ el cuerpo residual. Si ϕ es un módulo de Drinfeld sobre $\mathbb{F}$ de rango d nos interesa estudiar su comportamiento residual respecto de v. A continuación definimos los diferentes comportamientos posibles:

- Decimos que ϕ tiene coeficientes enteros cuando ϕ_a tiene coeficientes en $\mathcal{O}_v$ para todo $a \in \mathbb{A}$ y además la reducción módulo M_v de todos estos polinomios (o sea, de sus coeficientes) define un módulo de Drinfeld (de algún rango $0 < d_1 \leq d$) sobre F_v. Denotaremos en este caso ϕ^v al módulo de Drinfeld residual.
- Decimos que ϕ tiene reducción estable en v cuando existe un módulo de Drinfeld ψ sobre $\mathbb{F}$ isomorfo a ϕ tal que ψ tiene coeficientes enteros.
- Decimos que ϕ tiene buena reducción en v cuando tiene reducción estable y además al reducir módulo M_v (el módulo de Drinfeld con coeficientes enteros isomorfo a ϕ) obtenemos un módulo de Drinfeld sobre F_v de igual rango que ϕ.
- Decimos que ϕ tiene reducción potencialmente estable (o potencialmente buena) en v si existe una extensión $(\mathcal{G}, w)$ de $(\mathbb{F}, v)$ tal

que ϕ (visto como módulo de Drinfeld sobre $\mathcal{G}$) tiene reducción estable (respectivamente, buena) en w.

Para caracterizar la reducción estable de un módulo de Drinfeld en una valoración discreta, será útil considerar el siguiente invariante asociado a todo polinomio aditivo $f(\tau) = \sum_{i=0}^{t} c_i \tau^i \in \mathbb{F}\{\tau\}$:

$$v(f(\tau)) := \min_{j>0}\{v(c_j)/(q^j - 1)\}$$

4.2.1 Lema *Sea $u \in \mathbb{F}^*$. El módulo de Drinfeld $u\phi u^{-1}$ tiene coeficientes enteros respecto a v si y sólo si*

$$v(u) = \min_{a \in \mathbb{A} - \mathbb{F}_q} \{v(\phi_a)\}$$

Demostración: Sea $a \in \mathbb{A} - \mathbb{F}_q$ y sea el correspondiente polinomio aditivo:

$$\phi_a = \sum_{j=0}^{t} \phi_j(a)\tau^j, \;\; \phi_0(a) = \iota(a), \; \phi_t(a) \neq 0$$

Entonces se tiene:

$$u\phi_a u^{-1} = \sum_{j=0}^{t} u^{1-q^j} \phi_j(a)\tau^j$$

Para que $u\phi u^{-1}$ tenga coeficientes enteros es preciso que

$$u^{1-q^j} \phi_j(a) \in \mathcal{O}_v$$

para todo índice j y todo $a \in \mathbb{A}$ y además (para que la reducción sea un módulo de Drinfeld de rango positivo) que exista un índice $j_0 > 0$ y un elemento $a_0 \in \mathbb{A}$ tal que:

$$u^{1-q^{j_0}} \phi_{j_0}(a_0) \in \mathcal{O}_v^*$$

(de donde, a fortriori, $a_0 \notin \mathbb{F}_q$). Esto prueba la igualdad deseada.

4.2.2 Proposición *Sea ϕ un módulo de Drinfeld sobre $\mathbb{F}$. Existe un número natural $e_v(\phi)$ coprimo con p tal que para cualquier extensión $(\mathcal{G}, w)$ de $(\mathbb{F}, v)$ son equivalentes:*
1) ϕ tiene reducción estable en w.
2) El índice de ramificación de w sobre v es múltiplo de $e_v(\phi)$.

Demostración: Necesitamos extensiones w de v tales que exista $u \in \mathcal{G}^*$ con $w(u) = \min_{a\in\mathbb{A}-\mathbb{F}_q}\{w(\phi_a)\}$. Por lo tanto, necesitamos que este mínimo sea un entero.
Como $\mathbb{A}$ es finitamente generado sobre $\mathbb{F}_q$ sabemos que

$$\min_{a\in\mathbb{A}-\mathbb{F}_q}\{v(\phi_a)\} = m$$

existe en $\mathbb{Q}^*$. Además, como los polinomios ϕ_a tienen coeficientes en $\mathbb{F}$ y para todo $x \in \mathbb{F}$ se tiene: $w(x) = e_{w|v}v(x)$, basta elegir el índice de ramificación múltiplo del denominador de m para obtener la condición deseada para w.

4.2.3 Corolario *Todo módulo de Drinfeld tiene reducción potencialmente estable.*

Observación: Y por lo tanto, todo módulo de Drinfeld de rango 1 tiene reducción potencialmente buena (pues ambos conceptos son idénticos en este caso).
A continuación explicaremos el teorema principal de este capítulo, el cual relaciona el tipo de reducción de un módulo de Drinfeld en una valoración v con el comportamiento local en v de la acción del grupo de Galois de $\mathbb{F}$ sobre los puntos de división del módulo de Drinfeld.
Antes introduzcamos algo más de notación galoisiana: Fijemos $\mathbb{F}^{sep}$ una clausura separable de $\mathbb{F}$ y $\bar{v}$ una extensión de v a $\mathbb{F}^{sep}$. Sea $G := \mathrm{Gal}(\mathbb{F}^{sep}/\mathbb{F})$ y $I_{\bar{v}}$ el subgrupo de inercia de G en $\bar{v}$ (por abuso de notación y visto que no se presta a confusión alguna, en lo que sigue lo denotaremos simplemente I_v). Dado un G-módulo M diremos que M es no ramificado en v cuando I_v actúa trivialmente en M.
El siguiente resultado de Takahashi es el claro análogo del teorema de Ogg-Néron-Shafarevich versión drinfeldiana:

4.2.4 Teorema *Sea* $\wp \in \mathrm{Spec}(\mathbb{A})$, $\wp \neq \mathrm{caract}(F_v)$. *Sea* ϕ *módulo de Drinfeld sobre* $\mathbb{F}$. *Entonces* ϕ *tiene buena reducción en* v *si y sólo si el* G*-módulo*

$$\phi[\wp^\infty] := \bigcup_{m\geq 1}\phi[\wp^m]$$

es no ramificado en v.

Demostración: Es claro que en un caso de buena reducción la acción de I_v en $\phi[\wp^\infty]$ es trivial. Probemos la recíproca:

Nuestra hipótesis es que $\phi[\wp^\infty]$, como G-módulo, no ramifica en v. Cómo el número h de clases de $\mathbb{A}$ es finito, tenemos que $\wp^h = (b)$ es principal ($b \in \mathbb{A}$).
Lo primero que haremos es probar que ϕ tiene reducción estable en v: Obsérvese que si $\alpha \in \phi[b]$ entonces $\bar{v}(\alpha) \in \mathbb{Z}$, precisamente por estar en un G-módulo que no ramifica en v. Además, utilizando polígonos de Newton puede verse que:

$$\max_{0 \neq \alpha \in \phi[b]} \{\bar{v}(\alpha)\} = -v(\phi_b) \quad (*)$$

(aquí se usa el hecho de que b es coprimo con la característica residual de v, de donde $v(b_0) = 0$).
Luego, como $\phi[\wp^\infty]$ es no ramificado, concluimos de (*) que

$$v(\phi_b) \in \mathbb{Z}$$

Sea $(\mathcal{G}, w)$ extensión finita de $(\mathbb{F}, v)$ donde ϕ tiene reducción estable. De acuerdo con la proposición 4.2.2 una tal extensión existe y la podemos elegir con índice de ramificación minimal $e_{w|v} = e_v(\phi)$. Sea $u \in \mathcal{G}^*$ tal que $u\phi u^{-1}$ tiene coeficientes enteros respecto de w. A continuación, explicaremos por que en nuestro caso debe ser $e_v(\phi) = 1$: Sea F_w cuerpo residual de $(\mathcal{G}, w)$ respecto de w. Sabemos que $u\phi u^{-1}$ es un módulo de Drinfeld sobre F_w de rango positivo. Luego, si $a \in \mathbb{A} - \mathbb{F}_q$, la reducción de $u\phi_a u^{-1}$ debe tener grado positivo en τ. Razonando como en la demostración del lema 4.2.1 concluimos que $w(u) = w(\phi_a)$. Por lo tanto, $v(\phi_a)$ es independiente de a por lo que para todo $a \in \mathbb{A} - \mathbb{F}_q$:

$$v(\phi_a) = v(\phi_b) \in \mathbb{Z}$$

Esto implica que no hay denominadores que eliminar (ver la demostración de la proposición 4.2.2), es decir que $e_v(\phi) = 1$, o lo que es lo mismo, que ϕ tiene reducción estable en v.
Luego, podemos asumir que ϕ tiene coeficientes enteros en v. Falta demostrar que la reducción es buena. Para esto, basta ver que el coeficiente principal de ϕ_b es una unidad en v. Supongamos que no fuera así. Por hipótesis b es una v-unidad. Luego, existe $\alpha_1 \in \phi[b]$ con $\bar{v}(\alpha_1) < 0$.
Utilizando esta desigualdad y la condición sobre el coeficiente principal de ϕ_b (que conlleva la igualdad $v(\phi_b) = 0$) puede verse fácilmente

razonando por el absurdo que necesariamente debe existir una raíz α_2 de la ecuación

$$\phi_b(x) = \alpha_1$$

que verifique:

$$\bar{v}(\alpha_1) < \bar{v}(\alpha_2) < 0$$

Tenemos entonces: $\phi_b(\alpha_2) = \alpha_1, \quad \bar{v}(\alpha_2) < 0$. Aplicando en forma recursiva el mismo argumento vemos que podemos construir una sucesión infinita $\{\alpha_n\} \subseteq \mathbb{F}^{sep}$ tal que para todo $n \geq 1$:

$$\phi_b(\alpha_{n+1}) = \alpha_n, \quad \bar{v}(\alpha_n) < \bar{v}(\alpha_{n+1}) < 0$$

Como $\alpha_n \in \phi[b^n]$ y este G-módulo es no ramificado en v, sabemos que $\bar{v}(\alpha_n) \in \mathbb{Z}$ para todo $n \geq 1$. Esto nos lleva a una contradicción (por descenso infinito à la Fermat) de donde concluimos que ϕ tiene buena reducción en v.

4.2.5 Definición *Sea $\wp$ un ideal primo de $\mathbb{A}$, $K_\wp$, $\mathbb{A}_\wp$ las completaciones de K y $\mathbb{A}$ respecto de $\wp$. Llamaremos módulo de Tate $\wp$-ádico de ϕ al G-módulo continuo:*

$$T_\wp(\phi) = \mathrm{Hom}_{\mathbb{A}}(K_\wp/\mathbb{A}_\wp, \phi[\wp^\infty])$$

El módulo de Tate $T_\wp(\phi)$ es isomorfo al límite proyectivo de los $\phi[\wp^n]$. De aquí hereda la acción continua de G.
Observación: El fácil ver que es válido el resultado análogo al teorema 4.2.4 en términos del módulo de Tate.
Sea $\mathbb{F}_v$ la completación de $\mathbb{F}$ respecto de v y $\mathbb{F}_v^{nr}$ su máxima extensión noramificada. El siguiente corolario se desprende fácilmente del teorema 4.2.4:

4.2.6 Corolario *ϕ tiene reducción potencialmente buena en v si y sólo si la imagen de I_v en $\mathrm{Aut}_{\mathbb{A}_\wp}(T_\wp(\phi))$ es finita. Cuando esto es así, la extensión $\mathbb{F}_v^{nr}(\phi[\wp^\infty])/\mathbb{F}_v^{nr}$ es independiente de $\wp$ y cíclica de grado $e_v(\phi)$.*

Dado un morfismo f de ϕ en ψ llamemos f_* al $\mathbb{A}_\wp$-morfismo que induce en forma natural de $T_\wp(\phi)$ en $T_\wp(\psi)$.

4.2.7 Proposición *Sean ϕ, ψ módulos de Drinfeld de rango d positivo sobre un $\mathbb{A}$-cuerpo $\mathbb{F}$. La aplicación natural:*

$$\mathrm{Hom}_{\mathbb{F}}(\phi,\psi)\bigotimes \mathbb{A}_{\wp} \to \mathrm{Hom}_{\mathbb{A}_{\wp}}(T_{\wp}(\phi),T_{\wp}(\psi))$$

es inyectiva y tiene conucleo libre de torsión.

Observación: $T_{\wp}(\phi)$ y $T_{\wp}(\psi)$ son libres de rango d sobre $A_{\wp}$. La demostración de la inyectividad es análoga a la prueba del teorema 4.1.5.

4.3 Referencias

Las referencias para la preparación de este capítulo fueron sólo 2: Las notas del Seminario Bars de otoño del 2001 que me facilitara Francesc Bars (a quien aprovecho para agradecer por facilitarme el material y aclararme algunas dudas) y el libro:
D. Goss: "Basic structures of Function Field Arithmetic", Springer Verlag 1996

Luis V. Dieulefait
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les corts Catalanes 585, E-08007 Barcelona,
dieulefait@mat.ub.es

Capítol 5

Mòduls de Drinfeld sobre cossos finits

Enric Nart

Mantenim les notacions $\mathbb{F}_q$, X, K, ∞, d_∞, $\mathbb{A}$, del capítol 3.

En aquest capítol estudiarem les classes, a menys d'isogènia, de mòduls de Drinfeld ϕ sobre un cos finit $\mathbb{F} \supseteq \mathbb{F}_q$, respecte d'una estructura fixada de $\mathbb{F}$ com a $\mathbb{A}$-cos.

A la secció 3 introduirem un anàleg del *polinomi característic de Frobenius* que determina la classe d'isogènia. A la secció 4 veurem un anàleg de la correspondència de Honda-Tate que parametritza les classes d'isogènia per nombres de Weil.

A les seccions 1,2 determinem l'estructura de les àlgebres de divisió $\mathbb{F}(\tau)$ i $\mathrm{End}^0_{\mathbb{F}}(\phi)$. En el primer càlcul no intervé l'estructura de $\mathbb{A}$-cos de $\mathbb{F}$.

5.1 Estructura de $\mathbb{F}(\tau)$ com a àlgebra de divisió

Fixem una extensió finita $\mathbb{F}_q \subseteq \mathbb{F}$ del cos base $\mathbb{F}_q$ i denotem $s = [\mathbb{F}\colon \mathbb{F}_q]$.

Considerem l'anell de polinomis de Frobenius $\mathbb{F}\{\tau\}$, respecte de q, isomorf a l'anell de polinomis $\mathbb{F}_q$-lineals via $\tau = x^q$. Com que $\mathbb{F}$ és perfecte, a $\mathbb{F}\{\tau\}$ tenim algorismes de divisió per la dreta i per l'esquerra i $\mathbb{F}\{\tau\}$ és DIP per l'esquerra i per la dreta.

En aquesta secció volem estudiar l'estructura de la $\mathbb{F}_q$-àlgebra de divisió $\mathbb{F}(\tau)$, de les seves fraccions per l'esquerra (vegeu el capítol 1).

Considerem el polinomi de Frobenius (i mai millor dit):

$$F(\tau) = \tau^s \in \mathbb{F}_q[\tau] \subseteq \mathbb{F}\{\tau\}.$$

Clarament, $\mathbb{F}_q[F]$ és el centre de $\mathbb{F}\{\tau\}$. Per la propietat universal de l'anell de fraccions per l'esquerra, tenim una cadena d'inclusions:

$$\begin{array}{ccc} \mathbb{F}[F] & \subset & \mathbb{F}\{\tau\} \\ \cup & & \cup \\ \mathbb{F}_q[F] & \subset & \mathbb{F}_q[\tau] \end{array} \quad \rightsquigarrow \quad \begin{array}{ccc} \mathbb{F}(F) & \subset & \mathbb{F}(\tau) \\ \cup & & \cup \\ \mathbb{F}_q(F) & \subset & \mathbb{F}_q(\tau) \end{array}$$

Com que $\mathbb{F}(F) = Z_{\mathbb{F}(\tau)}(\mathbb{F}\tau^0)$ i $\mathbb{F}_q(\tau) = Z_{\mathbb{F}(\tau)}(\tau)$, la seva intersecció, $\mathbb{F}_q(F) = \mathbb{F}(F) \cap \mathbb{F}_q(\tau)$, és el centre de $\mathbb{F}(\tau)$.

5.1.1 Lema 1. *Tot element de $\mathbb{F}(\tau)$ es pot escriure de la forma $b^{-1}a$, amb $a \in \mathbb{F}\{\tau\}$ i $b \in \mathbb{F}_q[F]$. En altres paraules, sempre podem suposar que el denominador d'una fracció per l'esquerra pertany al centre de $\mathbb{F}\{\tau\}$.*

Demostració: $\mathbb{F}\{\tau\}$ és un $\mathbb{F}_q[F]$-mòdul per l'esquerra, lliure de rang s^2, amb base:

$$\{\lambda_i \tau^j\}_{0 \le i,j < s}, \quad \text{essent } \lambda_0, \ldots, \lambda_{s-1} \text{ una } \mathbb{F}_q\text{-base de } \mathbb{F}. \tag{5.1}$$

Per tant, tot element de $\mathbb{F}\{\tau\}$ és enter sobre $\mathbb{F}_q[F]$. En particular, per a tot $b \in \mathbb{F}\{\tau\}$ podem trobar un altre element $u \in \mathbb{F}\{\tau\}$ tal,

que $ub \in \mathbb{F}_q[F]$, i la fracció $b^{-1}a = (ub)^{-1}(ua)$ té una expressió amb denominador a $\mathbb{F}_q[F]$. □

En particular, $\dim_{\mathbb{F}_q(F)} \mathbb{F}(\tau) = s^2$, i (5.1) és també una base de $\mathbb{F}(\tau)$ com a $\mathbb{F}_q(F)$-espai vectorial.

Recordem que un $\mathbb{F}_q[F]$-ordre de $\mathbb{F}(\tau)$ és un subanell:

$$\mathbb{F}_q[F] \subseteq \mathcal{O} \subseteq \mathbb{F}(\tau),$$

finitament generat com a $\mathbb{F}_q[F]$-mòdul per l'esquerra i de rang màxim, és a dir, $\mathcal{O}$ conté una $\mathbb{F}_q(F)$-base de $\mathbb{F}(\tau)$.

Pel Lema 1, doncs, $\mathbb{F}\{\tau\}$ és un $\mathbb{F}_q[F]$-ordre de $\mathbb{F}(\tau)$. Encara més:

5.1.2 Lema 2. *$R := \mathbb{F}\{\tau\}$ és un $\mathbb{F}_q[F]$-ordre maximal de $\mathbb{F}(\tau)$.* A més a més, tot $\mathbb{F}_q[F]$-ordre maximal de $\mathbb{F}(\tau)$ és un conjugat de R.

Demostració: Suposem $R \subseteq \mathcal{O}$, amb $\mathcal{O}$ un $\mathbb{F}_q[F]$-ordre de $\mathbb{F}(\tau)$. Tot element de $\mathcal{O}$ és de la forma $b^{-1}a$, amb $a, b \in R$. Com que $\mathcal{O}$ és f.g. com a R-mòdul, existeix $u \in R$ tal que $u\mathcal{O} \subseteq R$. Per tant, $u\mathcal{O}$ és un ideal per la dreta de R i, com que R és DIP, serà principal: $u\mathcal{O} = vR$, per a algun $v \in R$. En altres paraules, $\mathcal{O} = xR$, amb $x = u^{-1}v \in \mathbb{F}(\tau)$. Ara bé, com que $\mathcal{O}$ és subanell, tenim $x^2 \in xR$; d'on $x \in R$ i $\mathcal{O} \subseteq R$.

En tenir R nombre de classes 1, tots els ordres maximals de $\mathbb{F}(\tau)$ són conjugats (vegeu [Reiner, Th.21.6]). □

Les extensions de cossos commutatius,

$$\mathbb{F}_q(F) \subseteq \mathbb{F}(F), \qquad \mathbb{F}_q(F) \subseteq \mathbb{F}_q(\tau),$$

tenen una estructura clara. La primera, $\mathbb{F}_q(F) \subseteq \mathbb{F}(F)$, és una extensió de les constants, cíclica de grau s, generada per l'automorfisme σ que deixa F invariant i aplica l'automorfisme de Frobenius ($x \mapsto x^q$) als coeficients. La segona, $\mathbb{F}_q(F) \subseteq \mathbb{F}_q(\tau)$, és l'extensió determinada pel polinomi $X^s - F$, clarament irreductible. De fet, ja es veu que podem identificar $\mathbb{F}(\tau)$ amb l'àlgebra cíclica:

$$\mathbb{F}(\tau) = (\mathbb{F}(F)/\mathbb{F}_q(F), \sigma, F) = \mathbb{F}(F)\tau^0 \oplus \cdots \oplus \mathbb{F}(F)\tau^{s-1},$$

amb l'estructura natural d'anell determinada per les relacions:

$$\tau^s = F, \qquad \tau x = x^\sigma \tau, \ \forall x \in \mathbb{F}(F).$$

Com a àlgebra central simple sobre el cos global $\mathbb{F}_q(F)$, l'àlgebra de divisió $\mathbb{F}(\tau)$ està determinada pels invariants locals. Tractant-se d'una extensió no-ramificada (extensió de les constants), és comprova fàcilment (vegeu [Goss, 4.11.29(3)]):

$$\mathrm{inv}_{F=\lambda}(\mathbb{F}(\tau)) = \begin{cases} 1/s, & \text{si } \lambda = 0, \\ -1/s, & \text{si } \lambda = \infty, \\ 0, & \text{en tota altra plaça.} \end{cases}$$

5.2 Estructura de l'àlgebra de divisió $\mathrm{End}^0_{\mathbb{F}}(\phi)$

Considerem un mòdul de Drinfeld ϕ sobre $\mathbb{F}$, de rang $d > 0$, respecte d'alguna estructura de $\mathbb{A}$-cos sobre $\mathbb{F}$, $\iota\colon \mathbb{A} \longrightarrow \mathbb{F}$. Denotem per $\mathfrak{p} \in \mathrm{Spec}(\mathbb{A})$ l'ideal $\ker(\iota) = \mathrm{char}(\mathbb{F})$, i per $v_\mathfrak{p}$ la plaça corresponent de K.

Disposem, doncs, d'un monomorfisme d'anells, $\phi\colon \mathbb{A} \longrightarrow \mathbb{F}\{\tau\}$, satisfent:

$$\phi_a(\tau) = \iota(a)\tau^0 + \cdots, \quad \deg(\phi_a(\tau)) = -d\, d_\infty \,\mathrm{ord}_\infty(a), \quad \forall a \in \mathbb{A}.$$

Via ϕ, identifiquem $\mathbb{A}$ amb una subàlgebra de $R := \mathbb{F}\{\tau\}$. Automàticament, K s'identifica amb un subcos de $\mathbb{F}(\tau)$. Per la definició de morfisme de mòduls de Drinfeld tenim:

$$\mathrm{End}_{\mathbb{F}}(\phi) = Z_R(\mathbb{A}).$$

En particular, $\mathrm{End}_{\mathbb{F}}(\phi) \supseteq \mathbb{F}_q[F]$, que és el centre de R.

Hem comentat al capítol anterior que $\mathrm{End}^0_{\mathbb{F}}(\phi) := \mathrm{End}_{\mathbb{F}}(\phi) \otimes_{\mathbb{A}} K$ és una àlgebra de divisió de dimensió finita sobre K. Per procedir a la seva classificació, la identifiquem a una subàlgebra de $\mathbb{F}(\tau)$:

5.2.1 Observació. *L'homomorfisme natural d'anells,*

$$\mathrm{End}_{\mathbb{F}}^0(\phi) \longrightarrow \mathbb{F}(\tau),$$

determina un isomorfisme entre $\mathrm{End}_{\mathbb{F}}^0(\phi)$ *i la subàlgebra*

$$D := Z_{\mathbb{F}(\tau)}(K)$$

de $\mathbb{F}(\tau)$.

En efecte, la imatge d'aquest monomorfisme és la subàlgebra de $\mathbb{F}(\tau)$ generada per $Z_R(\mathbb{A})$ i K. Clarament D conté aquestes subàlgebres. Recíprocament, si $d \in D$, l'expressem com $d = b^{-1}a$, amb $b \in \mathbb{F}_q[F]$, $a \in R$ (Lema 1); considerem la relació:

$$(b^{-1}a)\phi_a = \phi_a(b^{-1}a), \quad \forall a \in \mathbb{A}.$$

En commutar b amb tothom, el podem cancel·lar i deduïm que $a \in Z_R(\mathbb{A})$.

El següent diagrama resumeix la situació:

$$\begin{array}{rccc} & R & \hookrightarrow & \mathbb{F}(\tau) & \\ & \cup & & \cup & \\ \mathrm{End}_{\mathbb{F}}(\phi) = & Z_R(\mathbb{A}) & \hookrightarrow & D & = \mathrm{End}_{\mathbb{F}}^0(\phi) \\ & \cup & & \cup & \\ & \mathbb{A} & \hookrightarrow & K & \end{array}$$

5.2.2 Notació. Denotem $E := K(F)$. Recordem que, de fet, E és el subcos de $\mathbb{F}(\tau)$ generat per $\phi(\mathbb{A})$ i per F. La notació més precisa per a E seria, doncs, E_ϕ, i aquesta és la notació que emprarem més endavant quan considerem aquest cos per a diferents mòduls de Drinfeld.

A continuació analitzem l'estructura de D en una sèrie de proposicions.

5.2.3 Proposició 1. *El centre de* D *és* $E = K(F)$.

DEMOSTRACIÓ: Com que $K \subseteq K(F)$, tenim $D = Z_{\mathbb{F}(\tau)}(K) \supseteq Z_{\mathbb{F}(\tau)}(K(F))$; com que F pertany al centre, $D \subseteq Z_{\mathbb{F}(\tau)}(K(F))$. Per tant, $D = Z_{\mathbb{F}(\tau)}(K(F))$.

Pel teorema del doble centralitzador, $K(F) = Z_{\mathbb{F}(\tau)}(D)$ i el centre de D és $D \cap Z_{\mathbb{F}(\tau)}(D) = K(F)$.□

5.2.4 Proposició 2. *Hi ha una única plaça de E, v_E, damunt la plaça $(F = 0)$ de $\mathbb{F}_q(F)$; aquesta plaça v_E divideix la plaça $v_\mathfrak{p}$ de K.*

Hi ha una única plaça de E, ∞_E, damunt la plaça $(F = \infty)$ de $\mathbb{F}_q(F)$; aquesta plaça ∞_E és l'única plaça de E que divideix la plaça ∞ de K.

$$\begin{array}{ccccccccc} & & \mathbb{F}(\tau) & & & & & & \\ & & \cup & & & & & & \\ K & \overset{\phi}{\hookrightarrow} & E = K(F) & & v_\mathfrak{p} & — & v_E & \infty & — & \infty_E \\ & & \cup & & & & | & & & | \\ & & \mathbb{F}_q(F) & & & & (F=0) & & & (F=\infty) \end{array}$$

DEMOSTRACIÓ: Denotem per w indistintament la plaça $(F = 0)$ o $(F = \infty)$ de $\mathbb{F}_q(F)$ i denotem per $i_w = \text{ind}(\mathbb{F}(\tau)_w)$ l'índex de Schur de l'àlgebra local $\mathbb{F}(\tau)_w$. Com hem vist al final de la darrera secció, $\mathbb{F}(\tau)_w$ és una àlgebra de divisió; per tant, el seu índex de Schur coincideix amb el grau: $i_w = s$.

Considerem un subcos maximal E' de $\mathbb{F}(\tau)$. Com que E' descompon $\mathbb{F}(\tau)$, tenim, per [Goss, 4.11.33]:

$$[E' : \mathbb{F}_q(F)] = s = i_w \mid [E'_W : \mathbb{F}_q(F)_w], \quad \forall W | w.$$

Per tant, només hi pot haver una plaça de E' damunt w. Com que E és subcos d'algun d'aquests E', té la mateixa propietat.

Denotem per v_E, ∞_E, aquestes places. Vénen caracteritzades per:

$$v_E(F) > 0, \qquad \infty_E(F) < 0,$$

respectivament. Pel mateix motiu d'abans, del fet que $\text{End}_\mathbb{F}(\phi) \otimes_\mathbb{A} K_\infty$ és també un anell de divisió (vegeu el capítol anterior), deduïm

que hi ha una única plaça de E dividint la plaça ∞ de K. Aquesta plaça satisfà $W(\phi_a) < 0$, $\forall a \in \mathbb{A}$ no constant (i.e. no invertible). D'altra banda, F és enter sobre $\mathbb{A}$, en ser $\mathrm{End}_{\mathbb{F}}(\phi)$ finitament generat com a $\mathbb{A}$-mòdul; per tant, tenim també $W(F) < 0$ i aquesta plaça és $W = \infty_E$.

Finalment, per a qualsevol $a \in \mathfrak{p} = \mathrm{char}(\mathbb{F})$, tenim $\mathrm{ht}(\phi_a) > 0$ i, per tant,

$$(\phi_a)^s = bF, \text{ per a algun } b \in \mathbb{F}\{\tau\}. \tag{5.2}$$

A més a més,

$$\phi_a,\, F \in \mathrm{End}_{\mathbb{F}}(\phi) \cap E \implies b \in \mathrm{End}_{\mathbb{F}}(\phi) \cap E.$$

D'altra banda, com que $v_E(F) > 0$, tenim $v_E(b) \geq 0$, ja que b és enter sobre $\mathbb{F}_q[F]$, en ser $\mathbb{F}\{\tau\}$ finitament generat com a $\mathbb{F}_q[F]$-mòdul. Això ja ens permet deduir de (5.2) que $v_E(\phi_a) > 0$. Com que això és cert per a tot $a \in \mathfrak{p}$, forçosament v_E divideix $v_{\mathfrak{p}}$.□

5.2.5 Proposició 3. *Sigui r el nombre natural determinat per: $s = r[E\colon \mathbb{F}_q(F)]$. Aleshores, $\dim_E(D) = r^2$, i, com a E-àlgebra central i simple, D està determinada per:*

$$\mathrm{inv}_w(D) = \begin{cases} 1/r, & \text{si } w = v_E, \\ -1/r, & \text{si } w = \infty_E, \\ 0, & \text{en tota altra plaça.} \end{cases}$$

Demostració: Considerem un subcos maximal E' de $\mathbb{F}(\tau)$, que contingui E. Si $r = [E'\colon E]$, tenim:

$$s = [E'\colon \mathbb{F}_q(F)] = r[E\colon \mathbb{F}_q(F)],$$

com pretenia l'enunciat.

Pel teorema del centralitzador (vegeu [Goss, 4.11.14]),

$$\dim_{\mathbb{F}_q(F)}(D) \dim_{\mathbb{F}_q(F)}(E) = \dim_{\mathbb{F}_q(F)}(\mathbb{F}(\tau)) = s^2,$$

d'on traiem:

$$\dim_E(D) = \dim_{\mathbb{F}_q(F)}(D) / \dim_{\mathbb{F}_q(F)}(E) = \left(\frac{s}{[E\colon \mathbb{F}_q(F)]}\right)^2 = r^2.$$

D'altra banda, per [Pierce, 13.3], $D \sim \mathbb{F}(\tau)^E$, com a elements de $\mathrm{Br}(E)$, on $\mathbb{F}(\tau)^E$ denota l'àlgebra $\mathbb{F}(\tau) \otimes_{\mathbb{F}_q(F)} E$, obtinguda per extensió d'escalars a E.

Finalment, els invariants locals de $\mathbb{F}(\tau)^E$ com a E-àlgebra estan determinats pels de $\mathbb{F}(\tau)$ com a $\mathbb{F}_q(F)$-àlgebra (vegeu [Goss, 4.11.29.5]). Més precisament, per a qualsevol plaça W de E, amb restricció w a $\mathbb{F}_q(F)$, es té:

$$\mathrm{inv}_W(\mathbb{F}(\tau)^E \otimes_E E_W) = [E_W \colon \mathbb{F}_q(F)_w] \,\mathrm{inv}_w(\mathbb{F}(\tau)_w).$$

Per tant, aquest invariant val 0 per a qualsevol $W \neq v_E, \infty_E$ (ja que $w \neq 0, \infty$), i val $(s/r)\,\mathrm{inv}_w(\mathbb{F}(\tau)_w)$, per a $W = v_E$ ó $W = \infty_E$, ja que $[E_W \colon \mathbb{F}_q(F)_w] = [E \colon \mathbb{F}_q(F)] = s/r$, en aquest cas.□

5.2.6 Proposició 4. *Denotem per* $|\ |_\infty$ *l'extensió a* E *del valor absolut normalitzat de* K*:*

$$|x|_\infty := q^{\deg(x)} = q^{-d_\infty \,\mathrm{ord}_\infty(x)}, \quad \forall x \in K.$$

Aleshores,

$$d = r\,[E \colon K], \qquad |F|_\infty = q^{s/d} = (\sharp\mathbb{F})^{1/d}.$$

Demostració: Per la Proposició 2, ∞_E és l'única valoració discreta normalitzada de E que estén simultàniament les valoracions discretes normalitzades, ord_∞, de K i $(F = \infty)$, de $\mathbb{F}_q(F)$. Posem:

$$[E \colon K] = e\,f, \qquad [E \colon \mathbb{F}_q(F)] = e'\,f',$$

amb e, e' índexs de ramificació respectius i f, f' graus residuals respectius.

Hem vist al capítol 3 que $-\deg_\tau \circ \phi$ és una valoració discreta de K, equivalent a ord_∞:

$$\deg(\phi_a(\tau)) = -d\,d_\infty\,\mathrm{ord}_\infty(a) = -\frac{d\,d_\infty}{e}\,\infty_E(\phi_a(\tau)), \quad \forall a \in \mathbb{A}.$$

En particular, $-\deg_\tau$ és una valoració discreta de E equivalent a ∞_E, i la relació anterior mostra que la constant que les relaciona és $(d\,d_\infty)/e$. Tenim, doncs,

$$\infty_E(F) = -\frac{e}{d\,d_\infty}\deg_\tau(F) = -\frac{e\,s}{d\,d_\infty}.$$

Per tant,

$$|F|_\infty = q^{-d_\infty \frac{1}{e} \infty_E(F)} = q^{s/d}.$$

D'altra banda, tenim les relacions evidents:

$$e' = \infty_E(\frac{1}{F}) = -\infty_E(F) = \frac{e\,s}{d\,d_\infty}, \qquad f' = f\,d_\infty,$$

la darrera, pel diagrama commutatiu de cossos residuals:

$$\begin{array}{ccc} \kappa(\infty) & \xrightarrow{f} & \mathbb{F}_{E,\infty} \\ & {\scriptstyle d_\infty}\nwarrow \quad \nearrow{\scriptstyle f'} & \\ & \mathbb{F}_q & \end{array}$$

En resum,

$$\frac{[E\colon \mathbb{F}_q(F)]}{[E\colon K]} = \frac{e'\,f'}{e\,f} = \frac{s}{d}, \qquad r = \frac{s}{[E\colon \mathbb{F}_q(F)]} = \frac{d}{[E\colon K]}.$$

□

5.3 Classes d'isogènia de mòduls de Drinfeld sobre cossos finits

Hem vist al capítol 4 que, per a qualsevol $w \in \mathrm{Spec}(\mathbb{A})$, $w \neq \mathfrak{p}$, el mòdul de Tate,

$$T_w(\phi) := \lim_{\leftarrow n} \phi[w^n],$$

és un $\mathbb{A}_w$-mòdul lliure de rang d, on hi opera $G := \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$. L'assignació, $\phi \mapsto T_w(\phi)$ és functorial i l'homomorfisme:

$$\hom_{\mathbb{F}}(\phi,\psi) \otimes_{\mathbb{A}} \mathbb{A}_w \;\longrightarrow\; \hom_{\mathbb{A}_w}(T_w(\phi), T_w(\psi)),$$

és injectiu, amb conucli lliure de torsió. Aquest és un fet completament general, vàlid per a qualsevol $\mathbb{A}$-cos.

Quan treballem sobre un cos finit, podem considerar:

$P_\phi(t) :=$ pol. carac. de $T_w(F)$ com a endo $\mathbb{A}_w$-lineal de $T_w(\phi)$,

$m_\phi(t) :=$ polinomi mònic irreductible de F sobre K.

El polinomi $m_{\phi(t)}$ té coeficients en $\mathbb{A}$, en ser F enter sobre $\mathbb{A}$.

5.3.1 Lema 3. *$P_\phi(t) = m_\phi(t)^r$.*

En particular, $P_\phi(t)$ té coeficients a $\mathbb{A}$ i és independent de w.

DEMOSTRACIÓ: El polinomi $m_\phi(t)$ és irreductible a $K[t]$, de grau $[E\colon K]$ i anul·la $T_w(F)$. La seva factorització a $K_w[t]$ en producte d'irreductibles és de la forma:

$$m_\phi(t) = \prod_{W|w} m_W(t), \quad \text{amb } \deg m_W(t) = [E_W\colon K_w].$$

El polinomi característic $P_\phi(t)$ és producte de potències d'aquests factors irreductibles:

$$P_\phi(t) = \prod_{W|w} m_W(t)^{r_W}.$$

Si veiem que els exponents r_W són independents de W, ja tindrem $P_\phi(t) = m_\phi(t)^r$, per la Proposició 4.

Tenim una descomposició natural:

$$V_w(\phi) \otimes_K E = \oplus_{W|w} V_W, \quad \text{amb } \dim_{E_W}(V_W) = r_W.$$

Doncs bé, es comprova que aquest espais V_W tenen dimensió comuna com a E_W-espais vectorials, interpretant-los com el mòdul de Tate, en les distinites places W, d'un mòdul de Drinfeld ϕ_E sobre E, extensió natural de ϕ (vegeu [Goss, 4.12.8.3]).□

5.3.2 Proposició 5. *Si ϕ, ψ són dos mòduls de Drinfeld sobre $\mathbb{F}$, de rang $d > 0$, les condicions següents són equivalents:*

1. *ϕ i ψ són isògens.*
2. *$\mathrm{End}^0_{\mathbb{F}}(\phi)$ i $\mathrm{End}^0_{\mathbb{F}}(\psi)$ són isomorfs com a K-àlgebres, per un isomorfisme que envia F a F.*
3. *$m_\phi(t) = m_\psi(t)$.*
4. *$P_\phi(t) = P_\psi(t)$.*

DEMOSTRACIÓ: Les condicions 3 i 4 són equivalents pel Lema 3.

$1 \implies 2$. Si ϕ i ψ són isomorfs a la categoria dels mòduls de Drinfeld a menys d'isogènia, les seves àlgebres d'endomorfismes en aquesta categoria són isomorfes.

Més precisament, suposem que $P\colon \phi \longrightarrow \psi$ és una isogènia, $\hat{P}$ és la isogènia dual, i tenim $\hat{P}P = \phi_a$, per a cert $a \in \mathbb{A}$. Podem definir l'isomorfisme:

$$\mathrm{End}^0_{\mathbb{F}}(\phi) \longrightarrow \mathrm{End}^0_{\mathbb{F}}(\psi), \qquad Q \mapsto PQ\hat{P} \otimes a^{-1},$$

d'invers, $R \mapsto \hat{P}RP \otimes a^{-1}$.

Noteu que és isomorfisme de K-àlgebres i envia F a F.

$2 \implies 3$. Si aquestes àlgebres són K-isomorfes, els seus centres E_ϕ, E_ψ, són també isomorfs com a K-àlgebres.

$$\begin{array}{ccc} E_\phi & \xrightarrow{\sim} & E_\psi \\ {\scriptstyle\phi}\nwarrow & & \nearrow{\scriptstyle\psi} \\ & K & \end{array}$$

Com que l'isomorfisme envia F a F, a la força $m_\phi(t) = m_\psi(t)$.

$3 \implies 1$. Si $m_\phi(t) = m_\psi(t)$, podem establir un isomorfisme de K-àlgebres entre E_ϕ i E_ψ, que enviï F a F. Aquest isomorfisme de $\mathbb{F}_q(F)$-àlgebres estén a un isomorfisme, α, entre $\mathrm{End}^0_{\mathbb{F}}(\phi)$ i $\mathrm{End}^0_{\mathbb{F}}(\psi)$, perquè tenen els mateixos invariants locals, respectivament com a E_ϕ-àlgebra i E_ψ-àlgebra centrals simples.

$$\begin{array}{ccccc} & & \mathbb{F}(\tau) & & \\ & \swarrow & & \searrow & \\ Z_{\mathbb{F}(\tau)}(\phi(K)) & & \xrightarrow[\sim]{\alpha} & & Z_{\mathbb{F}(\tau)}(\psi(K)) \\ | & & & & | \\ E_\phi & & \xrightarrow[\sim]{} & & E_\psi \\ & \searrow & & \swarrow & \\ & & \mathbb{F}_q(F) & & \end{array}$$

Pel teorema de Skolem-Noether, existeix $u \in \mathbb{F}(\tau)$ tal, que:

$$\alpha(x) = u\, x\, u^{-1}, \quad \forall x \in \mathbb{F}(\tau).$$

Pel Lema 1, podem expressar $u = Q^{-1}P$, amb $P \in \mathbb{F}\{\tau\}$, $Q \in \mathbb{F}_q[F]$. Com que Q és del centre, tenim:

$$\alpha(x) = P\, x\, P^{-1}, \quad \forall x \in \mathbb{F}(\tau),$$

i ja tenim la isogènia que buscàvem:

$$P\colon \phi \longrightarrow \psi, \qquad \psi_a = \alpha(\phi_a) = P\, \phi_a\, P^{-1}.$$

□

Ja estem en condicions de provar l'anàleg al teorema de Tate.

5.3.3 Teorema. *Per a qualsevol $w \in \mathrm{Spec}(\mathbb{A})$, $w \neq \mathfrak{p} = \mathrm{char}(\mathbb{F})$, el mòdul de Tate $V_w(\phi) := T_w(\phi) \otimes_{\mathbb{A}_w} K_w$ és semisimple com a $K_w[F]$-mòdul. A més a més, l'aplicació natural:*

$$\hom_{\mathbb{F}}(\phi, \psi) \otimes_{\mathbb{A}} \mathbb{A}_w \;\longrightarrow\; \hom_{\mathbb{A}_w}(T_w(\phi), T_w(\psi))^G, \qquad (5.3)$$

és un isomorfisme.

Demostració: La semisimplicitat de l'operador F es prova a [Tag], imitant fil per randa la prova de Tate per a varietats abelianes sobre cossos finits.

Tractant-se d'un monomorfisme amb conucli lliure de torsió, per provar que (5.3) és un isomorfisme, és suficient comprovar que els dos membres tenen el mateix rang com a $\mathbb{A}_w$-mòdul. Equivalentment, volem comprovar:

$$\dim_K \hom^0_{\mathbb{F}}(\phi, \psi) = \dim_{K_w} \hom^0_{\mathbb{F}}(\phi, \psi) \otimes_K K_w \stackrel{?}{=}$$
$$\stackrel{?}{=} \dim_{K_w} \hom_{K_w[G]}(V_w(\phi), V_w(\psi)) = \dim_{K_w} \hom_{K_w[F]}(V_w(\phi), V_w(\psi)).$$

Per la semisimplicitat de F, pel Lema 3 i pel fet que $m_\phi(t)$ és producte de polinomis irreductibles diferents, tenim un isomorfisme de $K_w[F]$-mòduls:

$$V_w(\phi) \simeq S_\phi^r, \quad S_\phi := K_w[t]/m_\phi(t).$$

Si ϕ, ψ no són isògens, tenim $\hom_{\mathbb{F}}(\phi,\psi)=0$. D'altra banda, per la Proposició 5 tindrem $m_\phi(t)\neq m_\psi(t)$ i, en ser coprimers a $K[t]$, aquests polinomis no poden tenir factors comuns a $K_w[t]$ i no hi ha cap homomorfisme de $K_w[F]$-mòduls de S_ϕ a S_ψ. Per tant, també $\hom_{K_w[F]}(V_w(\phi),V_w(\psi))=0$.

Si ϕ, ψ són isògens, tenim $\hom^0_{\mathbb{F}}(\phi,\psi)\simeq \mathrm{End}^0_{\mathbb{F}}(\phi)$ com a K-àlgebres i, també, $V_w(\phi)\simeq V_w(\psi)$ com a $K_w[F]$-mòduls, ja que $S_\phi\simeq S_\psi$, en ser $m_\phi(t)=m_\psi(t)$. A més a més,

$$\mathrm{End}_{K_w[F]}(V_w(\phi))\simeq M_r(\mathrm{End}_{K_w[F]}(S_\phi)),$$

$$\dim_{K_w}\mathrm{End}_{K_w[F]}(S_\phi)=\dim_{K_w}S_\phi=\deg(m_\phi(t)).$$

En efecte, $\mathrm{End}_{K_w[F]}(S_\phi)$ s'identifica amb l'espai de matrius que commuten amb una matriu donada (amb polinomi característic producte de polinomis irreductibles diferents), i aquest espai té per dimensió la grandària de la matriu. En resum,

$$\dim_{K_w}\mathrm{End}_{K_w[F]}(V_w(\phi))=r^2\deg(m_\phi(t))=$$

$$=r^2\,[E_\phi\colon K]=\dim_K\mathrm{End}^0_{\mathbb{F}}(\phi).$$

□

5.4 Correspondència de Honda-Tate

Considerem un $\mathbb{A}$-cos finit $\mathbb{F}$, de característica $\mathfrak{p}$ i denotem $s=[\mathbb{F}\colon\mathbb{F}_q]$.

5.4.1 Definició. Un element $F\in\overline{K}$ diem que és un *nombre de Weil* de rang d, respecte de $\mathbb{F}$, si satisfà les condicions següents:

1. F és enter sobre $\mathbb{A}$.
2. Hi ha una única plaça v_E de $E:=K(F)$, que satisfà $v_E(F)>0$. Aquesta plaça divideix la característica $v_{\mathfrak{p}}$ de $\mathbb{F}$, com a plaça de K.
3. Hi ha una única plaça ∞_E de E dividint la plaça ∞ de K.

4. $|F|_\infty = (\sharp\mathbb{F})^{1/d}$, essent $|\ |_\infty$ l'extensió a E del valor absolut normalitzat de K corresponent a la plaça ∞.

5. $[E\colon K]$ divideix d.

Evidentment, sobre el conjunt de nombres de Weil de rang d hi opera el grup $\mathrm{Aut}_K(\overline{K})$; denotem per W_d el conjunt quocient per a aquesta acció.

Pel que hem vist a les seccions anteriors, disposem d'una aplicació injectiva:

$$\{\text{classes d'isogènia de m.D. sobre } \mathbb{F} \text{ de rang } d\} \ \hookrightarrow\ W_d,$$

que assigna a cada mòdul de Drinfeld ϕ, una arrel de $m_\phi(t)$.

5.4.2 Teorema. *Aquesta aplicació és bijectiva.*

Demostració: Pensem en els subcossos de E:

$$\begin{array}{ccccccc} K & \overset{\phi}{\hookrightarrow} & E = K(F) & \qquad v_{\mathfrak{p}} & — & v_E & \qquad \infty \quad — \quad \infty_E \\ & & \cup & & & | & \qquad\quad | \\ & & \mathbb{F}_q(F) & & & (F=0) & \qquad (F=\infty) \end{array}$$

- v_E, resp. ∞_E, és l'única plaça de E dividint les places $(F=0)$, resp. $(F=\infty)$ de $\mathbb{F}_q(F)$.

En efecte, dividir $(F=0)$ equival a $v(F)>0$ i per hipòtesi v_E és l'única plaça amb aquesta propietat. D'altra banda, qualsevol plaça de E sobre $(F=\infty)$ satisfà $v(F)<0$ i això obliga a $v(a)<0$ per a algun $a\in\mathbb{A}$ (de fet, hauríem d'escriure $v(\phi_a(\tau))<0$), ja que F és enter sobre $\mathbb{A}$. Per tant, totes les places de E sobre $(F=\infty)$ estan també sobre la plaça ∞ de K i, per hipòtesi, ∞_E és l'única amb aquesta propietat.

- $d/[E\colon K] = s/[E\colon \mathbb{F}_q(F)]$ i aquest enter (per(5)) el denotarem r.

En efecte, posem:

$$[E\colon K] = e\,f, \qquad [E\colon \mathbb{F}_q(F)] = e'\,f',$$

amb e, e' índexs de ramificació respectius i f, f' graus residuals respectius. Pensant en les extensions residuals tenim $f' = f\, d_\infty$; d'altra banda, per (4) tenim:

$$e' = -\infty_E(F) = s\, e/d\, d_\infty.$$

Per tant,

$$\frac{d}{[E\colon K]} = \frac{d}{e\, f} = \frac{s}{d_\infty e' f} = \frac{s}{e' f'} = \frac{s}{[E\colon \mathbb{F}_q(F)]}.$$

• Sigui D la E-àlgebra central simple amb invariants locals nuls a tot arreu, excepte per a v_E, ∞_E, on valen $1/r$, $-1/r$. Doncs bé, qualsevol subcos maximal L de D és un cos de descomposició de $\mathbb{F}(\tau)$ (pensant L com a $\mathbb{F}_q(\tau^s)$-àlgebra, via l'isomorfisme evident $\mathbb{F}_q(F) \simeq \mathbb{F}_q(\tau^s)$).

En efecte, per [Goss, 4.11.33],

$$\deg(D) = \operatorname{ind}(D) = \operatorname*{mcm}_w\{\operatorname{ind}(D_w)\} = r,$$

de manera que $\dim_E D = r^2$. Com raonàvem a la secció 2, el fet que D_w és àlgebra de divisió per a $w = v_E, \infty_E$, implica que v_E, ∞_E tenen una única extensió a L. També,

$$[L\colon \mathbb{F}_q(F)] = [L\colon E][E\colon \mathbb{F}_q(F)] = r\,[E\colon \mathbb{F}_q(F)] = s.$$

Per provar que la $\mathbb{F}_q(\tau^s)$-àlgebra $\mathbb{F}(\tau) \otimes_{\mathbb{F}_q(\tau^s)} L$ descompon, comprovem que té tots els invariants locals nuls. Per a tota plaça $(\tau^s = \lambda)$ de $\mathbb{F}_q(\tau^s)$ i qualsevol extensió w a L, la commutativitat del diagrama:

$$\begin{array}{ccc} \operatorname{Br}(\mathbb{F}_q(\tau^s)_\lambda) & \xrightarrow{\operatorname{inv}_\lambda} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle -\otimes_{\mathbb{F}_q(\tau^s)_\lambda} L_w}\downarrow & & \downarrow{\scriptstyle [L_w\colon \mathbb{F}_q(\tau^s)_\lambda]} \\ \operatorname{Br}(L_w) & \xrightarrow{\operatorname{inv}_w} & \mathbb{Q}/\mathbb{Z} \end{array}$$

ens fa veure que per a l'única plaça w damunt de $(\tau^s = 0)$, resp. $(\tau^s = \infty)$, l'invariant local s'anul·la, ja que $\operatorname{inv}_\lambda(\mathbb{F}(\tau)) = \pm 1/s$ i $[L_w\colon \mathbb{F}_q(\tau^s)_\lambda] = [L\colon \mathbb{F}_q(\tau^s)] = s$.

• Disposem d'una $\mathbb{F}_q(\tau^s)$-immersió, $E \overset{\beta}{\hookrightarrow} \mathbb{F}(\tau)$, que envia F a τ^s. La restricció de β a $\mathbb{A}$ és un mòdul de Drinfeld de rang d sobre $\mathbb{F}$, amb nombre de Weil associat (la classe de) F.

En efecte, per [Goss, 4.11.21], el cos L admet una $\mathbb{F}_q(\tau^s)$-immersió dins $\mathbb{F}(\tau)$. Denotem per β la restricció a E d'aquesta immersió.

Considerem $\mathcal{O} := \cap_{w \neq \infty_E} \mathcal{O}_w$ el subanell de E de les funcions regulars arreu excepte potser a ∞_E. Per [Reiner, Sec.8,Ex.1], podem submergir $\beta(\mathcal{O})$ dins d'un $\mathbb{F}_q(\tau^s)$-ordre de $\mathbb{F}(\tau)$ i, pel Lema 2, component β amb un automorfisme intern, podem suposar $\beta(\mathcal{O}) \subseteq \mathbb{F}\{\tau\}$.

Clarament, $\beta\colon \mathbb{A} \longrightarrow \mathbb{F}\{\tau\}$ és un homomorfisme de $\mathbb{F}_q$-àlgebres no trivial (ja que $\beta(F) = \tau^s$). Falta comprovar que $\beta_a(\tau) = \iota(a)\tau^0 + \cdots$. Del diagrama commutatiu,

$$\begin{array}{ccccc} \mathbb{A} & \hookrightarrow & \mathcal{O} & \overset{\beta}{\hookrightarrow} & \mathbb{F}\{\tau\} \\ \downarrow & & \downarrow & & \downarrow \tau = 0 \\ \mathbb{A}/\mathfrak{p} & \longrightarrow & \mathcal{O}/F & \longrightarrow & \mathbb{F}, \end{array}$$

obtenim un homomorfisme $\mathbb{A} \xrightarrow{j} \mathbb{F}$ amb nucli $\mathfrak{p}$ (ja que el nucli conté $\mathfrak{p}$ i aquest ideal és maximal), i $j(a)$ és el terme independent de $\beta_a(\tau)$.

A la força $j = \sigma \circ \iota$, per a algun $\mathbb{F}_q$-automorfisme σ de $\mathbb{F}$; per tant, canviant F per algun conjugat seu, aconseguirem $j = \iota$. De la relació,

$$\deg(\beta_a(\tau)) = -\operatorname{rang}(\beta)\, d_\infty\, \operatorname{ord}_\infty(a), \quad \forall a \in \mathbb{A},$$

deduïm també:

$$\deg(\beta(b)) = -\operatorname{rang}(\beta)\, d_\infty\, \operatorname{ord}_\infty(b), \quad \forall b \in \mathcal{O}.$$

Aplicat a $b = F \in \mathcal{O}$, tenim:

$$s = \deg(\beta(F)) = -\operatorname{rang}(\beta)\, d_\infty\, \frac{(-s)}{d\, d_\infty},$$

d'on $\operatorname{rang}(\beta) = d$.

Finalment, és evident que $m_\beta(t)$ és el polinomi minimal de F sobre K. □

Bibliografia

[Goss] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin-Heidelberg, 1998.

[Gekeler] E.-U. Gekeler, *On Finite Drinfeld Modules*, J. Algebra, **141**(1991), 187-203.

[Pierce] R.S. Pierce, *Associative Algebras*, Graduate Texts in Mathematics 88, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[Reiner] I. Reiner, *Maximal Orders*, Academic Press, 1975.

[Tag] Y. Taguchi, *Semi-simplicity of the Galois representations attached to Drinfeld modules of finite characteristics*, Duke Math. J., **62**(1991), 593-599.

[Yu] J.-K. Yu, *Isogenies of Drinfeld Modules over Finite Fields*, J. Number Theory, **54**(1995), 161-171.

E. Nart
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
nart@mat.uab.es

Capítol 6

Teoria de cossos de classes explícita per a cossos de funcions

Xavier Xarles

6.1 Exemples clàssics de teoria de cossos de classes explícita

Recordem el teorema clàssic de Kronecker-Weber sobre les extensions abelianes de $\mathbb{Q}$.

6.1.1 Teorema. *Tota extensió abeliana de $\mathbb{Q}$ està continguda en una extensió ciclotòmica $\mathbb{Q}(\xi)$.*

El nostre objectiu és de obtenir un teorema anàleg però per al cos de funcions d'una corba sobre un cos finit (o sigui un cos global de característica p). Anem a reinterpretar el resultat anterior de manera que pugui ser generalitzat fàcilment. Observem que tenim una "acció"de $\mathbb{Z}$ en els invertibles del cos $\mathbb{Q}$ i en tots els cossos que el contenen (per exemple a $\mathbb{C}$): per a cada $n \in \mathbb{Z}$ i cada $z \in K$ definim

Amb el suport parcial de MCYT, BHA2000-0180.

$n * z := z^n$. Pensat a $\mathbb{C}$, aquesta acció és l'obtinguda a $\mathbb{C}^*$ de l'acció usual de $\mathbb{Z}$ a $\mathbb{C}$ a traves del morfisme exponencial $e(z) := exp(2*\pi iz)$. Ara, per a cada $n \in \mathbb{N}$, els elements que estan al nucli de $n*$ són les arrels enèsimes de 1, que ens generen totes les extensions abelianes de $\mathbb{Q}$.

Aquesta manera de pensar es anàloga a la teoria de cossos de classes explícita per a extensions quadràtiques purament imaginaries K de $\mathbb{Q}$: aquí tenim l'anell d'enters $\mathcal{O}$ de K, que pensem posat a dins de $\mathbb{C}$ com una xarxa. Aleshores $\mathbb{C}/cO \cong E(\mathbb{C})$, on E és una corba el·líptica (amb multiplicació complexa), i l'isomorfisme bé donat per la $\wp$ de Weierstrass. L'operació de $\mathcal{O}$ a $\mathbb{C}$ es trasllada a una operació a $E(\mathbb{C})$ que de fet esta definida a H (el cos de Hilbert de K). A més, per a cada $\alpha \in \mathcal{O}$, l'operació $\alpha*$ a $E(L)$ per a tota extensió L/H be donada per polinomis. Les arrels d'aquest polinomis, o sigui $E[\alpha]$ en la notació usual, ens donen extensions abelianes de H. Denotem en general $E[\mathfrak{a}]$ per als ideals $\mathfrak{a}$ de $\mathcal{O}$ com els zeros comuns de tots els elements de $\mathfrak{a}$.

6.1.2 Teorema. *Tota extensió abeliana de H està continguda al cos $H(E[\mathfrak{a}])$ per algun ideal $\mathfrak{a} \subset \mathcal{O}$.*

La idea subjacent a aquests dos casos és la de fer actuar l'anell d'enters del cos de manera convenient a totes les extensions d'una certa extensió finita de K (el cos de classes de Hilbert), de manera que l'acció vingui donada per polinomis. Els zeros d'aquests polinomis ens donaran les extensions abelianes del cos. Observem que el fet que les extensions obtingudes són abelianes es dedueix en els dos casos del fet que

$$\mathrm{Gal}(H(E[\mathfrak{a}])/H) \hookrightarrow (\mathcal{O}/\mathfrak{a})^*$$

on el morfisme és el natural (de fet en els dos casos és un isomorfisme).

Per obtenir les extensions abelianes de K hem de construir una funció de Weber: $h : E \to E/\mathrm{Au}(E) \cong \mathbb{P}^1$ (per exemple la funció x si $j_E \neq 0, 1728$).

6.1.3 Teorema. *Tota extensió abeliana de K està continguda al cos $K(j(E), h(E[\mathfrak{a}]))$ per algun ideal $\mathfrak{a} \subset \mathcal{O}$.*

Per a veure demostracions d'aquests resultats podeu consultar l'exposició 3 de [STN2000] o bé el capítol II del llibre del Silverman [14].

6.2 Repàs de teoria de cossos de classes.

Anem a fer un repàs molt breu i ràpid de la teoria de cossos de classes per a cossos de funcions. La teoria és completament anàloga al cas dels cossos de nombres (amb petites diferencies tècniques) i es pot demostrar utilitzant la "teoria de cossos de classes abstracta"(vegeu per exemple el llibre del Neukirch [Ne]).

Sigui K un cos global i sigui K^{ab}/K la maxima extensió abeliana de K. D'altre banda, sigui $\mathbb{I}$ el seu grup d'ideles, o sigui

$$\mathbb{I} = (\mathbb{A})^* = \{(\alpha_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p}^* \ : \ \alpha_\mathfrak{p} \in U_\mathfrak{p} \text{q.p.t. } \mathfrak{p}\}$$

on $U_\mathfrak{p}$ són les unitats del anell d'enters $\mathcal{O}_\mathfrak{p}$ de $K_\mathfrak{p}$, el completat respecte un ideal primer $\mathfrak{p}$ de K. El morfisme de reciprocitat és un epimorfisme continu

$$\psi : \mathbb{I} \longrightarrow \mathrm{Gal}(K^{ab}/K)$$

amb nucli K^* (i per tant un morfisme de $\mathbb{C}l$), de manera que per a cada idele $\mathbf{i} = (i_\mathfrak{p})$,

$$\psi(i) = \prod_\mathfrak{p} (i_\mathfrak{p}, K_\mathfrak{p})$$

on $(-, K_\mathfrak{p})$ és el símbol local de residus nòrmics.

Així, cada subgrup obert de $\mathbb{I}$ ens determina una extensió abeliana de K.

Situem-nos en el cas que K és el cos de funcions d'una corba sobre $\mathbb{F}_q$. Prenem ∞ una plaça fixada de K (i.e. un punt de la corba), i sigui A l'anell dels elements de K amb valoració no negativa a cada plaça finita de K. Donat $\mathfrak{p}$ un ideal primer de A i $n > 0$ un nombre enter, denotarem com és usual per $U_\mathfrak{p}^{(n)} = 1 + \mathfrak{p}^n$. Ara, si prenem

$$\mathfrak{m} := \prod_\mathfrak{p} \mathfrak{p}^{m_\mathfrak{p}}$$

un ideal de A, els subgrups

$$\mathbb{I}(\mathfrak{m}) := K^* \cdot (U_{\mathfrak{m}} \times K_\infty^*) \text{ on } U_{\mathfrak{m}} := \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(m_{\mathfrak{p}})}$$

anomenats grups radials d'ideles mòdul $\mathfrak{m}$, es corresponen als cossos de classes radials mòdul $\mathfrak{m}$, que denotarem $H(\mathfrak{m})$. Tenim a més que

$$\mathrm{Gal}(H(\mathfrak{m})/K) \cong \mathbb{C}l_K(\mathfrak{m}) := \mathbb{I}(\mathfrak{m})/K^*$$

i és la maxima extensió abeliana amb cos de funcions $\mathbb{F}_q$, no ramificada fora dels ideals que divideixen $\mathfrak{m}$ i ∞, tal que ∞ descompon totalment a $H(\mathfrak{m})$, i tal que pel ideals $\mathfrak{p}$ que divideixen $\mathfrak{m}$ el seu conductor en $\mathfrak{p}$ és $m_{\mathfrak{p}}$. Així, per a tota extensió abeliana L/K amb cos de funcions $\mathbb{F}_q$ (o sigui que correspon a un recobriment abelià de la corba) tal que ∞ descompon totalment a L, si $\mathfrak{m}$ és el seu conductor, aleshores $L \subseteq H(\mathfrak{m})$.

Ara, si denotem per $I^{\mathfrak{m}}$ els grup d'ideals fraccionaris primers amb $\mathfrak{m}$, i per $P^{\mathfrak{m}}$ el subgrup d'ideals principals (a) tals que $a \equiv 1 (mod\ \mathfrak{m})$, tenim un isomorfisme natural

$$I^{\mathfrak{m}}/P^{\mathfrak{m}} \cong \mathbb{I}(\mathfrak{m})/K^*.$$

Utilitzant aquest isomorfisme podem expressar el morfisme de reciprocitat

$$\psi^{\mathfrak{m}} : I^{\mathfrak{m}}/P^{\mathfrak{m}} \cong \mathrm{Gal}(H(\mathfrak{m})/K)$$

com

$$\psi^{\mathfrak{m}}(\mathfrak{a}) = (\mathfrak{a}, H(\mathfrak{m})/K) = \prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}^{n_{\mathfrak{p}}}$$

on $\mathfrak{a}$ és un ideal fraccionari coprimer amb $\mathfrak{m}$,

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

i $\varphi_{\mathfrak{p}}$ és el morfisme de Frobenius corresponen al ideal $\mathfrak{p}$, que és no ramificat en $H(\mathfrak{m})$. O sigui,

$$\varphi_{\mathfrak{p}}(a) \equiv a^{q_{\mathfrak{p}}} (mod\ \mathfrak{P}),$$

per a tot element a de A', A' la clausura entera de A en $H(\mathfrak{m})$, on $\mathfrak{P}$ és un ideal primer de A' damunt de $\mathfrak{p}$ i $q_{\mathfrak{p}} := \sharp(A/\mathfrak{p})$. El element $(\mathfrak{a}, H(\mathfrak{m})/K)$ s'anomena el símbol d'Artin.

6.3 El cos de funcions racional

Situem-nos al cas que $k = \mathbb{F}_q(T)$ i $A = \mathbb{F}_q[T]$, i per tant el punt ∞ correspon a la valoració donada per $1/T$. Anem a veure com construir efectivament els cossos H_a introduïts en la secció anterior, on a denota un element qualsevol de a (o si és vol, l'ideal que genera). En aquest cas ens trobarem resultats anàlegs a les extensions ciclotòmiques, i, de fet, les demostracions són gairebé iguals.

Considerem el mòdul de Carlitz, donat per

$$\phi : A \longrightarrow k\{\tau\}$$

$$T \mapsto \tau + T$$

Utilitzarem les següents notacions, ja introduïdes en el tema 2.

6.3.1 Notació. Si $a \in A$ és un polinomi en T, aleshores

$$\phi[a] := \{ \text{ arrels de } \phi_a(X) \text{ a } \overline{k}\},$$

$$\widetilde{H}_a := k(\phi[a])$$

el cos obtingut adjuntant les arrels de ϕ_a, i

$$G_a := \mathrm{Gal}(\widetilde{H}_a/k).$$

Recordem que ja sabem que l'extensió $\widetilde{H}_a/k$ és de Galois i que el morfisme natural

$$G_a \to \mathrm{Aut}_{A-mod}(\phi[a]) \cong \mathrm{Aut}_{A-mod}(A/aA) \cong (A/aA)^*$$

definit via l'isomorfisme com a A-mòduls $\phi[a] \cong A/aA$, és injectiu (doncs els elements de G_a estan determinats un cop sabem la seva acció en les arrels de $\phi_a(x)$).

El primer objectiu que ens proposem es veure que aquest morfisme és isomorfisme, i, a més, estudiar en detall la ramificació de l'extensió.

Fixem λ_a un generador com a A-mòdul de $\phi[a]$; aleshores $\widetilde{H}_a = k(\lambda_a)$. Anem a calcular qui és el polinomi irreductible de λ_a sobre k; obtindrem una mena de polinomis ciclotòmics. Per a fer-ho observem primer el següent lema elemental.

6.3.2 Lema. *Siguin a i b elements de A. Aleshores $\phi_a(x)$ divideix $\phi_{ba}(x)$.*

DEMOSTRACIÓ: Com que $\phi_{ba}(\tau) = \phi_b(\tau)\phi_a(\tau)$, aleshores $\phi_a(\tau)$ divideix per la dreta a $\phi_{ba}(\tau)$. Però això és equivalent a que $\phi_a(x)$ divideixi a $\phi_{ba}(x)$ (vegis per exemple el Corol·lari 1.3.2). □

6.3.3 Definició Sigui $a \in A$ mònic. Definim inductivament $g_1(x) := x$ i

$$g_a(x) := \frac{\phi_a(x)}{\prod_b g_b(x)},$$

on b són els polinomis mònics que divideixen a.

Per exemple, si a és irreductible, aleshores $g_a(x) := \phi_a(x)/x$, i

$$g_{a^r}(x) := \frac{\phi_{a^r}(x)}{\phi_{a^{r-1}}(x)}.$$

6.3.4 Lema. *Suposem que $a \in A$ és irreductible i mònic (com a polinomi en T). Aleshores $g_{a^r}(x)$ és irreductible, de grau $\sharp(A/aA)^*$ i és d'Eisenstein en a.*

DEMOSTRACIÓ: Primer farem el cas $r = 1$. Sigui d el grau de a (com a polinomi en T). Recordem que $\phi_a(\tau) = a\tau^0 + \cdots + \tau^d$, ja que a és mònic. Per tant $g_a(x) = a + \cdots + x^{q^d-1}$. Al reduir mòdul a, obtenim que $g_a(x) = \widetilde{\phi}_a(x)/x$, on $\widetilde{\phi}$ denota el mòdul de Drinfeld sobre $\mathbb{F}_{q^d}$ reducció de ϕ. Ara bé, $\widetilde{\phi}$ és un mòdul de Drinfeld amb altura i rang 1. Així

$$\mathrm{ht}(\widetilde{\phi}_a(\tau)) = \deg(\widetilde{\phi}_a(\tau)) = \deg(a),$$

d'on tenim que

$$g_a(x) \equiv x^{q^d-1} (\mathrm{mod}\ a).$$

Pel criteri d'Eisenstein, $g_a(x)$ és irreductible.

El cas $r > 1$ surt fàcilment observant que $g_{a^r}(x) = g_a(\phi_{a^{r-1}}(x))$.

□

6.3.5 Corol·lari. *Suposem que $a \in A$ és mónic i potència d'un irreductible. Aleshores*

1. *El morfisme $G_a \to (A/aA)^*$ és un isomorfisme.*
2. *L'ideal a descompon totalment a $\widetilde{H}_a$.*
3. *Si b és un element irreductible de A, coprimer amb a, aleshores b és no ramificat a $\widetilde{H}_a$.*

Demostració:

1. És clar donat que
$$\sharp G_a = [\widetilde{H}_a : k] = \deg(g_a(x)) = \sharp(A/aA)^*.$$
2. És una propietat general dels polinomis d'Eisenstein.
3. Surt d'un càlcul amb discriminants. Si denotem per R la clausura entera de A a $\widetilde{H}_a$, aleshores $A[\lambda_a] \subseteq R$ i tenim que
$$\operatorname{disc}(R) \backslash \operatorname{disc}(A[\lambda_a]) \backslash \operatorname{Norm}(\phi'_a(\lambda_a))$$
ja que $\phi_a(\lambda_a) = 0$. Ara, $\phi'_a(x) = a$ i per tant b no divideix $\operatorname{disc}(R)$.

□

Donat que la ramificació de $\widetilde{H}_a$ i $\widetilde{H}_b$ és totalment diferent si a i b són primers entre si, obtenim el resultat buscat per a $\widetilde{H}_a$ si a és qualsevol polinomi mònic.

6.3.6 Corol·lari. *Sigui a un polinomi mònic. Aleshores $g_a(x)$ és mònic i irreductible, $G_a \cong (A/aA)^*$ i per a tot b irreductible i primer amb a és no ramificat a $\widetilde{H}_a/k$.*

Anem a veure que $\widetilde{H}_a$ es pot identificar a un cos de classes radial. Començarem observant que ϕ ens determina el símbol d'Artin $(-, \widetilde{H}_a/k)$ que va de

$$I_a := \{ \text{ ideal fraccionaris de A coprimers amb a}\}$$

a G_a.

6.3.7 Proposició. *Sigui $b \in A$ mònic i irreductible, coprimer amb a. Aleshores, per a tota $\lambda \in A$ tenim que*

$$((b), \widetilde{H}_a/k)(\lambda) = \phi_b(\lambda).$$

DEMOSTRACIÓ: Cal veure que el morfisme $\lambda \mapsto \phi_b(\lambda)$ és el Frobenius. Prenem $\mathcal{B}$ un ideal primer de $\widetilde{H}_a$ a sobre de b. Aleshores

$$\phi_b(x) \equiv x^{q^{\deg(b)}} (\text{mod } \mathcal{B})$$

tal com em vist en el lema anterior. Però això ens diu que és el Frobenius. □

Amb aquesta proposició podem determinar explícitament qui és el nucli del símbol d'Artin: si $x \in A$ és monic i coprimer amb a, aleshores

$$((x), \widetilde{H}_a/k) = id \;\Leftrightarrow\; \phi_x(\lambda) = \lambda \;\Leftrightarrow\; \phi_{x-1}(\lambda) = 0 \;\Leftrightarrow\; x \equiv 1 (\text{mod } a).$$

Si denotem per

$$\widetilde{\mathcal{P}}_a := \{(x) \subseteq A \mid x \equiv 1(\text{mod } a),\ x \text{ mònic } \}$$

aleshores tenim que

$$I_a/\widetilde{\mathcal{P}}_a \cong G_a.$$

El punt clau per a identificar el subgrup de les ideles que correspon a $\widetilde{H}_a$ és saber com ramifica el primer de l'infinit.

6.3.8 Teorema. *Sigui $a \in A$ monic, $a \neq 0$. Aleshores ∞ és moderadament ramificat a $\widetilde{H}_a/k$. A més, si a és una potencia d'un irreductible mònic, aleshores ∞ trenca en $\sharp(A/aA)^*/(q-1)$ primers, i $e_\infty = q-1$, $f_\infty = 1$.*

La demostració d'aquest teorema és un càlcul llarg i laboriós amb polígons de Newton (vegeu el teorema 3.2 de [Ha2]).

Utilitzant aquest resultat podem veure finalment que $\widetilde{H}_a$ és el cos de classes radial corresponent al subgrup

$$k^*(U_a \times (\frac{1}{T}) \times U_\infty^{(1)}).$$

Observeu que

$$K_\infty^* = \mathbb{F}_q \times (\frac{1}{T}) \times U_\infty^{(1)}.$$

Finalment obtenim una descripció explicita del cos H_a.

6.3.9 Teorema. *Sigui $a \in A$, $a \neq 0$, a mònic. Sigui λ_a un generador de $\phi[a]$, arrel del polinomi $g_a(x) \in A[x]$. Aleshores*

$$H_a = k(\lambda_a^{q-1}).$$

6.3.10 Remarca. Aquest resultat és anàleg al cas dels cossos ciclotòmics, extensions abelianes de $\mathbb{Q}$. En efecte, el subgrup de les ideles corresponen a $\mathbb{Q}(\xi_n)$ és $\mathbb{Q}^*(U_n \times \mathbb{R}_{>0}^*)$; i el cos de classes radial corresponent a $\mathbb{Q}^*(U_n \times \mathbb{R}^*)$ és $\mathbb{Q}(\xi_n)^+$, la maxima extensió real dins de $\mathbb{Q}(\xi_n)$ (o sigui, la extensió on ∞ descompon totalment).

Bibliografia

[Ge80] *E.-U.Gekeler*: Drinfeld Modular Curves. LNM 1231 (1980).

[Ge] *E.-U.Gekeler, M.van der Put, M.Reversat, J.Van Geel*: Proceedings of the workshop on: Drinfeld modules, modular schemes and applications. Alden-Biesen, 9-14 September 1996. World Scientific (1997).

[Go] *David Goss*: Basic Structures of Function Field Arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 35, Springer Verlag (1991).

[Ha] *D. Hayes*: Explicit class field theory for rational function fields. Trans. Amer. Math. Soc. 189, 77-91 (1974).

[Ha2] *D. Hayes*:Explicit class field theory in global function fields. Studies in algebra and number theory, pp. 173–217, Adv. in Math. Suppl. Stud. 6, Academic Press, New York-London, 1979.

[Ne] *J. Neukirch*: Class field theory. Grundlehren der Mathematischen Wissenschaften, 280. Springer-Verlag, Berlin, 1986

[Sil2] *J.H. Silverman*: Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[STN2000] *P. Bayer, E. Nart i J.Quer (eds)*: Varietats abelianes amb multiplicació complexa. Notes del Seminari de Teoria de Nombres (UB-UAB-UPC), Collbato (2000).

X. Xarles

Departament de Matemàtiques

Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
xarles@mat.uab.es

Capítol 7

Uniformización de curvas de Mumford y Jacobianas.

Carlos A. Infante

El objetivo de esta charla es recordar algunos conceptos relativos al semi- plano superior no-arquimediano y sus cocientes por subgrupos discretos de GL_2 . Estudiaremos la uniformización analítica rígida de las curvas que surgen de estos cocientes, así como su reducción y la construcción de su Jacobiana como espacio analítico rígido.

Primero fijemos la notación: Denotaremos por K un cuerpo completo respecto a una valoración discreta, $\mathcal{O}$ el anillo de enteros y $C = \widehat{\overline{K}}$ la completación de la clausura algebraica de K. Supondremos que el cuerpo residual $k = \mathbb{F}_q$ es finito, π un elemento uniformizador de K y $|\ |$ el valor absoluto sobre K y sobre su extensión C.

7.1 Árbol de Bruhat-Tits de $\mathrm{GL}_2(K)$.

Una exposición más detallada del contenido de este apartado puede consultarse en [1].

Consideremos los $\mathcal{O}$-submódulos M de rango 2 de K^2 bajo la siguiente relación de equivalencia:

$$M_1 \sim M_2 \Leftrightarrow \exists \lambda \in K \text{ tal que } M_1 = \lambda M_2.$$

Sea $[M]$ la clase de equivalencia de M.

El árbol de Bruhat-Tits, que de aquí en adelante denotaremos por τ, queda definido como el grafo conexo y sin lazos que tiene por vértices el conjunto

$$V(\tau) := \left\{ [M] \mid M \ \mathcal{O}\text{-submódulo de } K^2 \text{ de rango } 2 \right\}$$

y por aristas (orientadas) el conjunto
$A(\tau) := \{ [M_1] , [M_2] \}$ tales que

$$\pi M_1 \subsetneq M_2 \subsetneq M_1.$$

Recordemos que el grupo $\mathrm{PGL}_2(K)$ actúa transitivamente sobre los vértices y las aristas de τ. Sobre la descripción local de τ recordemos que en cada vértice concurren exactamente $q+1$ aristas y que una semi-línea de τ es un sub-árbol de τ de la forma:

Recordemos que dos semi-líneas de τ se identifican si difieren por un número finito de vértices y que el conjunto de semi-líneas de τ se corresponde con los puntos de $\mathbb{P}^1(K)$.

En la siguiente sección veremos como la estructura de espacio rígido del semiplano superior está estrechamente relacionada con este grafo.

7.2 Semiplano superior no-arquimediano.

El semiplano superior no-arquimediano es el espacio analítico rígido sobre K definido por

$$\mathbb{H}_\infty := \mathbb{P}^1_C(C) \backslash \mathbb{P}^1_K K) = C \backslash K.$$

Recordemos que tiene un recubrimiento especial por espacios afinoides tales que si $\overline{\mathbb{H}_\infty}$ es la reducción de $\mathbb{H}_\infty$ respecto a este recubrimiento, entonces el grafo reducción de $\overline{\mathbb{H}_\infty}$ es isomorfo a τ [2].

También $\mathrm{GL}_2(K)$ actúa de manera natural sobre $\mathbb{H}_\infty$ a través de las transformaciones fraccionarias lineales sobre $\mathbb{H}_\infty$ y sobre τ de manera que tenemos una aplicación canónica

$$\mathbb{H}_\infty \longrightarrow \tau(\mathbb{R})$$

que es compatible con la acción de $\mathrm{GL}_2(K)$ en ambos lados, donde $\tau(\mathbb{R})$ es la realización de τ (ver Lecture 9 en [2]).

7.3 Uniformización de Curvas.

Primero observemos que no cualquier subgrupo Γ de $\mathrm{GL}_2(K)$ da una estruc- tura de espacio analítico rígido al cociente $\Gamma\backslash\mathbb{H}_\infty$ en el sentido de tener un recubrimiento admisible para la topología rígida. Sin embargo, si Γ es un subgrupo discreto de $\mathrm{GL}_2(K)$, este actúa con estabilizadores finitos sobre $\mathbb{H}_\infty$ y sobre τ , y por tanto tiene sentido formar el cociente $\Gamma\backslash\mathbb{H}_\infty$ como espacio rígido.

Por otro lado, una condición para que $\Gamma\backslash\tau$ tenga estructura de grafo es que Γ actúe sobre τ sin inversiones (es decir, $\nexists\gamma \in \Gamma$ tal que $\gamma(v_1) = v_2$ y $\gamma(v_2) = v_1$).

La idea es comparar la geometría de $\Gamma\backslash\mathbb{H}_\infty$ con la de $\Gamma\backslash\tau$ sabiendo que el grafo dual de la reducción $\Gamma\backslash\overline{\mathbb{H}_\infty}$ es canónicamente isomorfo a $\Gamma\backslash\tau$.

El siguiente teorema nos da una descripción completa del cociente $\Gamma\backslash\mathbb{H}_\infty$ a través del análisis del grafo cociente.

7.3.1 Teorema *Sea Γ subgrupo discreto de $\mathrm{GL}_2(K)$ como antes. Supongamos que $\Gamma\backslash\tau$ tiene la siguiente estructura*

$$\Gamma\backslash\tau = (\Gamma\backslash\tau)^\circ \cup \bigcup_{i=1}^{m} \ell_i$$

donde $(\Gamma\backslash\tau)^\circ$ es un grafo finito y $\{\ell_1, \ldots, \ell_m\}$ es un número finito de clases de semi-líneas.

Entonces existe una curva $\widehat{M_\Gamma}$ *proyectiva, no-singular, conexa y un con- junto* S *de* m *puntos tales que*

$$\Gamma\backslash\mathbb{H}_\infty = (\widehat{M_\Gamma}\backslash S)^{an}.$$

S *se denomina el conjunto de cúspides de* $M_\Gamma = (\widehat{M_\Gamma}\backslash S)$. *Más aún, se tienen las siguientes igualdades*

$$g(\widehat{M_\Gamma}) = \operatorname{rank}_{\mathbb{Z}} H^1(\Gamma\backslash\tau, \mathbb{Z}) = rank_Z(\Gamma^{ab}),$$

donde $\Gamma^{ab} = \Gamma/[\Gamma,\Gamma]$ *es el abelianizado de* Γ *y* $\operatorname{rank}_{\mathbb{Z}} H^1(\Gamma\backslash\tau, \mathbb{Z})$ *es el número de Betti de* $\Gamma\backslash\tau$.

Las principales diferencias con el caso complejo vienen del hecho de que en el caso rígido no todo recubrimiento étale coincide con uno analítico y que en nuestro caso $\widehat{M_\Gamma}$ es una curva de Mumford, es decir

$$(\widehat{M_\Gamma})^{an} = \widehat{\Gamma}\backslash\mathbb{H}_\infty$$

con $\widehat{\Gamma}$ un cierto grupo de Schottky (finitamente generado, sin torsión y discontinuo, lo cual implica que es libre en g generadores y no-abeliano si $g > 1$) pues sólo estas curvas poseen un recubrimiento universal con grupo recubridor isomorfo a uno de este tipo (ver Lecture 6 en [2]). En [3] se estudia una posible relación entre Γ y $\widehat{\Gamma}$.

7.4 Ejemplo Estándar.

Veamos brevemente el siguiente ejemplo estándar para $A = \mathbb{F}_q[T]$. Sea K el cuerpo de fracciones de A, $K_\infty = \mathbb{F}_q((T))$ la completación de K en ∞ y $\pi = T^{-1}$ un uniformizante.

Hagamos actuar $\Gamma = \mathrm{PGL}_2(A) \subset \mathrm{PGL}_2(K_\infty)$ que es un subgrupo dis- creto y actúa sin inversiones en τ.

7.4.1 Teorema *Sea* $V = \{[M_0], [M_1], [M_2], \dots\}$ *el vértice de* τ *definido por* $M_i = T^i\mathcal{O} + \mathcal{O}$, $i \geq 1$. *Se tiene* $V = \Gamma\backslash\tau$ *y*

$$\Gamma\backslash\mathbb{H}_\infty \cong \mathbb{A}^{1,an}_{K_\infty}.$$

Para la demostración ver Lecture 7 en [2].

7.5 Jacobianas.

Comencemos recordando que un toro split sobre C es un grupo algebraico $T \cong (\mathbb{G}_m)^g$, con $\mathbb{G}_m$ el grupo multiplicativo (ver Lecture 12 en [2]).

El grupo de caracteres de T queda definido por:

$$\chi(T) := \mathrm{Hom}(T, \mathbb{G}_m) \cong \mathbb{Z}^g.$$

Sea $\{\xi_1, \ldots, \xi_g\}$ una $\mathbb{Z}$-base de $\xi(T)$, consideremos la aplicación

$$\underline{\ell}\colon T(C) \longrightarrow \mathbb{R}^g$$

$$t \mapsto (\log_q |\xi_1(t)|, \ldots, log_q|\xi_g(t)|).$$

Una red en T es un subgrupo Λ de $T(C)$ cuya imagen $\underline{\ell}(\Lambda)$ en $\mathbb{R}^g$ es una red en el sentido usual (un $\mathbb{Z}$-módulo libre de rango máximo).

Si Λ en T es una red, siempre podemos formar el cociente T/Λ en la categoría de grupos analíticos rígidos sobre C. Surge de manera natural la siguiente pregunta:

¿Cuándo es T/Λ algebraizable? Es decir, ¿cuándo es el espacio analítico asociado a una variedad abeliana A sobre C (que es única por GAGA)?

Recordemos que en el caso complejo toda variedad abeliana es un toro complejo, pero que el inverso no siempre es verdad. Para ello se deben satisfacer las condiciones de Riemann. La siguiente proposición nos da el equivalente a las condiciones de Riemann en nuestro caso.

7.5.1 Proposición *T/Λ es algebraizable $\Leftrightarrow$ $\exists\sigma\colon \Lambda \to M = \xi(T)$ homomorfismo tal que la aplicación bilineal*

$$\Lambda\times\Lambda \longrightarrow C^*$$

$$(\alpha, \beta) \mapsto \sigma(\alpha)(\beta)$$

es simétrica y definida positiva (esto último significa $\log_q(\alpha)(\alpha) > 0$ para $1 \neq \alpha \in \Lambda$).

7.6 Funciones theta.

En esta parte introduciremos las llamadas funciones theta con el único fin de definir un apareamiento adecuado que nos permita construir la Jacobiana de $\widehat{M_\Gamma}$ como espacio analítico rígido.

Sea Γ subgrupo discreto de $\mathrm{GL}_2(K)$. Definimos

$$\overline{\Gamma} := \Gamma^{ab}/tor$$

que es un grupo abeliano libre en g generadores (g el género de $\widehat{M_\Gamma}$), y

$$\widetilde{\Gamma} := \Gamma/\Gamma \cap \mathcal{Z}(K_\infty)$$

donde $\mathcal{Z}(K_\infty)$ es el grupo de matrices escalares.

Notemos que $\Gamma \cap \mathcal{Z}(K_\infty)$ es el núcleo de las acciones de Γ sobre $\mathbb{H}_\infty$ y sobre τ.

Sean ω y η dos elementos fijos de $\mathbb{H}_\infty$. Definimos

$$\theta(\omega, \eta, z) = \prod_{\gamma \in \widetilde{\Gamma}} \frac{(z - \gamma\omega)}{(z - \gamma\eta)}.$$

7.6.1 Teorema *Sean $\Gamma\omega$ la órbita y $\widetilde{\Gamma}_\omega$ el estabilizador de ω, respectivamente.*

1. *$\theta(\omega, \eta, z)$ converge uniforme y localmente en $\mathbb{H}_\infty$. La resultante función meromorfa $\theta(\omega, \eta, \cdot)$ tiene ceros de orden $\sharp\widetilde{\Gamma}_\omega$ en Γ_ω y polos de orden $\sharp\widetilde{\Gamma}_\eta$ en $\Gamma\eta$ si $\Gamma\omega \neq \Gamma\eta$. Si $\Gamma\omega = \Gamma\eta$ no tiene ceros ni polos sobre $\mathbb{H}_\infty$.*

2. *Para cada $\alpha \in \Gamma$ existe una constante $c(\omega, \eta, \alpha) \in C^*$ tal que*

$$\theta(\omega, \eta, \alpha z) = c(\omega, \eta, \alpha)\theta(\omega, \eta, z)$$

   es independientemente de z.

3. *$c(\omega, \eta, \alpha)$ depende únicamente de la clase de α en $\overline{\Gamma}$, de donde tenemos un homomorfismo de grupos*

$$c(\omega, \eta, \cdot)\colon \Gamma \to \overline{\Gamma} \to C^*$$

$$\alpha \mapsto c(\omega, \eta, \alpha).$$

4. *La función holomorfa*

$$u_\alpha(z) := \theta(\omega, \alpha\omega, z)$$

es independiente de la elección de $\omega \in \mathbb{H}_\infty$ *y sólo depende de* $\alpha \in \overline{\Gamma}$.

5. $c_\alpha = c(\omega, \alpha\omega, \cdot) : \Gamma \to C^*$ *(es más, en* K^**) define una aplicación bilineal y simétrica*

$$\overline{\Gamma}\times\overline{\Gamma} \to C^*$$

$$(\alpha, \beta) \mapsto c_\alpha(\beta).$$

6. *El* $\mathbb{Q}$*-apareamiento bilinear y simétrico*

$$\overline{\Gamma}\times\overline{\Gamma} \to \mathbb{Q}$$

$$(\alpha, \beta) \mapsto -\log_q |c_\alpha(\beta)|$$

es definido positivo.

Como consecuencia se tiene

7.6.2 Corolario *Sea* $\Gamma \subseteq \mathrm{GL}_2(K)$ *como antes. Sea* $T_{\overline{\Gamma}} := Hom(\overline{\Gamma}, \mathbb{G}_m)$ *el toro con grupo de caracteres* $\overline{\Gamma}$.

Consideremos $\overline{\Gamma}$ *como un subgrupo de* $T_{\overline{\Gamma}}(C)$ *vía la inmersión* $\overline{c}\colon \overline{\Gamma} \to \mathrm{Hom}(\overline{\Gamma}, C^*)$ *inducida por la aplicación* $\alpha \mapsto c_\alpha$.

Entonces existe una variedad abeliana A_Γ *sobre* C *caracterizada por la siguiente sucesión exacta de puntos* C*-valuados*

$$1 \to \overline{\Gamma} \xrightarrow{\overline{c}} T_{\overline{\Gamma}}(C) \to A_\Gamma(C) \to 0.$$

7.6.3 Teorema *La variedad abeliana* A_Γ *es canónicamente isomorfa a la Jacobiana* $J(\widehat{M_\Gamma})$ *de* $\widehat{M_\Gamma}$.

Sólo daremos una breve idea de la demostración [2]. Sea $\omega_0 \in \mathbb{H}_\infty$ fijo. La aplicación

$$\psi\colon \mathbb{H}_\infty \to A_\Gamma(C)$$

que a cada ω asigna la clase de $c(\omega_0, \omega, \alpha)$ en $A_\Gamma(C)$ es analítica, Γ-invariante y factoriza a través de $\Gamma\backslash\mathbb{H}_\infty$, lo cual nos lleva a una aplicación analítica

$$\psi_\Gamma\colon M_\Gamma(C) = \Gamma\backslash\mathbb{H}_\infty \to A_\Gamma(C)$$

que se extiende a una aplicación analítica

$$\overline{\psi} : \widehat{M_\Gamma}(C) \to A_\Gamma(C),$$

que, por GAGA, es un morfismo de variedades algebraicas. De la propiedad universal de las Jacobianas, tenemos un morfismo entre variedades abelianas $\varphi : J_\Gamma \to A_\Gamma$ que es inyectivo sobre los puntos C-valuados. Finalmente, como $\dim(J_\Gamma) = g(\Gamma) = \dim(A_\Gamma)$, se tiene que φ es exhaustivo.

Bibliografia

[1] X. Xarles, Uniformització p-àdica de corbes de Shimura, Notes del STNB2001.

[2] E.-U. Gekeler, M. van der Put, M. Reversat, Proceedings of the work- shop on: Drinfeld Modules, modular schemes and applications, 106-109. September 1996. World Scientific (1997).

[3] M. Reversat, Sur les revètemens de Schottky dels courbes modu- lares.Arch. Math (Basel) 66 (1996)n 5, 378-387.

C. A. Infante
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
cinfante@mat.uab.es

Capítol 8

Corbes modulars de Drinfeld

X. Xarles

En aquesta xerrada farem una breu introducció a les corbes modulars de Drinfeld, tant des del punt de vista analític com des del d'espais de moduli. Es convenient tenir presents les construccions de les corbes modulars clàssiques sobre $\mathbb{C}$, doncs molts dels resultats i alguns dels mètodes que utilitzarem són anàlegs als resultats clàssics. Tal com passa en el cas clàssic, la construcció analítica és molt més senzilla però no és suficient per a moltes de les aplicacions aritmètiques que farem després. La construcció via espais de moduli només la esbossarem breument.

Recordem les notacions que em estat utilitzant en les anteriors xerrades.

8.1 Exemple bàsic.

Considerem el cas en que $A = \mathbb{F}_q[T]$, i la plaça del infinit és $\infty = T$. EL nostre objectiu és classificar els mòduls de Drinfeld de rang 2

sobre $\mathbb{C}_\infty$, sobre K_∞ i fins i tot sobre K.

Sabem del capítol 3 [Ro] que tots els mòduls de Drinfeld de rang 2 sobre $\mathbb{C}_\infty$ es poden construir a partir de xarxes de rang 2 sobre $\mathbb{C}_\infty$: A-sub-mòduls discrets de $\mathbb{C}_\infty$ de rang 2, on els morfismes entre xarxes venen donats per homotècies.

Tenim així una equivalència de categories

$$\underline{\text{Drinf}}\,{}^{2}_{\mathbb{C}_\infty} \leftrightsquigarrow \underline{\text{Xarxes}}\,{}^{2}_{\mathbb{C}_\infty}.$$

8.1.1 Exercici. Observem que, com que A és DIP, tota xarxa L és isomorfa com a A-mòdul a A^2, i per tant L és isomorfa com a xarxa a $A \oplus A\alpha$ per un cert $\alpha \in \mathbb{C}_\infty$.

Demostreu aleshores que $A \oplus A\alpha$ és una xarxa (i.e. és un sub-mòdul *discret*) si i només si $\alpha \notin K_\infty$

Tenim així que podem classificar les xarxes de rang 2 a $\mathbb{C}_\infty$ mòdul isomorfismes de xarxes per nombres $\alpha \in \mathbb{C}_\infty \setminus K_\infty$, mòdul una certa relació d'equivalència. Concretament tenim

8.1.2 Proposició. *Tenim una correspondència bijectiva*

$$\underline{\textit{Xarxes}}\,{}^{2}_{\mathbb{C}_\infty}/\simeq \xrightarrow{\sim} (\mathbb{C}_\infty \setminus K_\infty)/\sim$$

on

$$\alpha \sim \beta \;\Leftrightarrow \exists M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \textit{ tal que } M(\alpha) := \frac{a\alpha + b}{c\alpha + d} = \beta.$$

Demostració (Idea): Considerem dues xarxes de la forma $L_\alpha := A \oplus A\alpha$ i $L_\beta := A \oplus A\beta$. Un morfisme de xarxes entre L_β i L_α ve donat per un nombre $\psi \in \mathbb{C}_\infty$ complint que $\psi \cdot 1 = c\alpha + d$ i $\psi \cdot \beta = a\alpha + b$ per a certs elements a, b, c i d de A. Tenim per tant que $\beta = \frac{a\alpha+b}{c\alpha+d}$. No és difícil de comprovar que aquest morfisme és un isomorfisme si i només si

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A).$$

□

Recordem que en el capítol 7 [In] em vist que

$$(\mathbb{C}_\infty \setminus K_\infty)/\sim \cong \ \mathrm{GL}_2(A)\backslash(\mathbb{P}^1(\mathbb{C}_\infty) \setminus \mathbb{P}^1(K_\infty)) \cong$$
$$\cong \mathrm{GL}_2(A)\backslash\mathbb{H}_\infty \xrightarrow{\sim} (\mathbb{A}^1_{\mathbb{C}_\infty})^{an}.$$

8.1.3 Corol·lari. *Tenim una correspondència canònica*

$$j\colon \underline{Drinf}^{\,2}_{\mathbb{C}_\infty}/ \cong \xrightarrow{\sim} (\mathbb{A}^1_{\mathbb{C}_\infty})^{an} \cong \mathbb{C}_\infty$$

De manera anàloga al que fem amb les corbes el·líptiques, anomenarem l'invariant j d'un mòdul de Drinfeld ϕ de rang 2 al nombre $j(\phi)$. Podem explicitar totalment qui és el morfisme j i veure que, de fet, l'invariant j d'un mòdul de Drinfeld és un nombre en el cos on ϕ està definit. Vegem la construcció explícita: Donat ϕ un mòdul de Drinfeld de rang 2 sobre L, sabem que ϕ ve determinat donant $\phi_T = T\tau^0 + c_1\tau^1 + c_2\tau^2$. Un isomorfisme u entre dos mòduls de Drinfeld ϕ i ϕ' és un element $u \in L^* \subset L\{\tau\}$ complint que

$$uT\tau^0 + uc_1\tau^1 + uc_2\tau^2 = u\phi_T = u\phi'_T u = uT\tau^0 + u^q c'_1\tau^1 + u^{q^2}c'_2\tau^2,$$

que es equivalent a

$$uc_1 = u^q c'_1 \ \text{ i } \ uc_2 = u^{q^2}c'_2,$$

per tant que

$$c_1 = u^{q-1}c'_1 \ \text{ i } \ c_2 = u^{q^2-1}c'_2.$$

Aquestes igualtats impliquen que

$$\frac{{c_1}^{q+1}}{c_2} = \frac{{c'_1}^{q+1}}{c'_2},$$

i, de fet, són equivalents a aquesta si el cos L és algebraicament tancat.

8.1.4 Proposició. *Donat ψ un mòdul de Drinfeld sobre L, determinat per $\psi_T = T\tau^0 + c_1\tau^1 + c_2\tau^2$, aleshores l'invariant j de psi ve donat per $j(\psi) = \frac{{c_1}^{q+1}}{c_2}$ i pertany a L.*

Observeu que, de la mateixa manera que per a corbes el·líptiques, dos mòduls de Drinfeld amb el mateix invariant j són isomorfs en la clausura algebraica, però no necessàriament en el cos on estan definits.

8.1.5 Remarca. Si prenem ara A qualsevol (en general no DIP), aleshores tota xarxa és isomorfa com a A-mòdul a $A \oplus I$ per a cert I ideal de A, i que dues xarxes $A \oplus I$ i $A \oplus I'$ són isomorfes com a xarxes si tenen les mateixes classes de I i de I' a $\mathrm{Pic}(A)$. Tenim per tant que

$$\{L - \text{xarxa de rang } 2 \mid L \cong_{A-\mathrm{mod}} A \oplus I\}/\cong \xrightarrow{\sim} \mathrm{GL}(A \oplus I)\backslash \mathbb{H}_\infty,$$

i obtenim una corba modular per a cada element de $\mathrm{Pic}(A)$. Compte per que aquestes corbes no són en general isomorfes a $\mathbb{A}^1$. De fet no ho són ni en el cas de la corba $\mathrm{GL}_2(A)\backslash\mathbb{H}_\infty$ corresponent a la classe trivial.

8.2 Grups aritmètics

8.2.1 Definició Sigui $\Gamma \subseteq \mathrm{GL}_2(K_\infty)$ un subgrup discret. Diem que Γ és aritmètic si és commensurable amb $\Gamma(1) := \mathrm{GL}_2(A)$ (o sigui, si $\Gamma \cap \Gamma(1)$ és d'index finit a Γ i a $\Gamma(1)$).

8.2.2 Exemples. Sigui $\mathfrak{n}$ un ideal de A. Aleshores els següents subgrups de $Gamma(1)$ són d'index finit i per tant són grups aritmètics:

$$\Gamma(\mathfrak{n}) := \mathrm{Ker}\left(\mathrm{GL}_2(A) \to \mathrm{GL}_2(A/\mathfrak{n})\right)$$

$$\Gamma_0(\mathfrak{n}) := \left\{ M \in \mathrm{GL}_2(A) \mid A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod}\ \mathfrak{n}) \right\}.$$

Ara, si Y és una xarxa de rang 2 a $\mathbb{C}_\infty$, $\Gamma(Y) := \mathrm{GL}(Y)$ és també un grup aritmètic.

Recordem que en el Capítol anterior em vist que $\mathrm{GL}_2(K_\infty)$ actua en l'arbre de Bruhat-Tits τ de $\mathrm{GL}_2(K_\infty)$, d'on tenim que els grups aritmètics també ho fan. Per tal de poder donar una estructura geomètrica a $\Gamma\backslash\mathbb{H}_\infty$ cal primer verificar que es compleixen les condicions necessaries.

8.2.3 Proposició. *Si Γ és un grup aritmètic, aleshores verifica que no té inversions (i.e. $\nexists \gamma \in \Gamma$ tal que $\gamma(v_1) = v_2$ i $\gamma(v_2) = v_1$) i*

$$\Gamma\backslash\tau = (\Gamma\backslash\tau)^\circ \cup \bigcup_{i=1}^{m} \ell_i$$

on $(\Gamma\backslash\tau)^\circ$ *és un graf finit i* $\{\ell_1,\ldots,\ell_m\}$ *és un nombre finit de classes de semi-línies.*

No és difícil veure (vegis per exemple el llibre del Serre [Se]) que el grup $\mathrm{GL}_2(A)$ verifica les propietats de la proposició, d'on es dedueix fàcilment el resultat per a qualsevol grup aritmètic.

D'aquesta proposició, junt amb el teorema 7.3.1 del capítol anterior [In] tenim que existeix una corba $X(\Gamma)$ llisa i projectiva de gènere

$$g = \mathrm{rank}_{\mathbb{Z}}\, H^1(\Gamma\backslash\tau,\mathbb{Z}) = \mathrm{rank}_Z\left((\Gamma/\Gamma_f)^{ab}\right),$$

on Γ_f és el subgrup generat pels elements de torsió, i un conjunt $S=\{p_1,\ldots,p_n\}$ de n punts de $X(\Gamma)$ tal que

$$\Gamma\backslash\mathbb{H}_\infty \cong Y(\Gamma)^{an} := (X(\Gamma)\backslash S)^{an}.$$

Els punts de S s'anomenen les puntes $\mathrm{Cusps}(\Gamma)$ de $Y(\Gamma)$, i a $X(\Gamma)$ la compactificació de $Y(\Gamma)$.

Per els grups aritmètics definits abans utilitzarem les següents notacions (standard):

$$Y(\mathfrak{n}) := \Gamma(\mathfrak{n})\backslash\mathbb{H}_\infty$$

$$Y_0(\mathfrak{n}) := \Gamma_0(\mathfrak{n})\backslash\mathbb{H}_\infty$$

amb les corresponents compactificacions $X(\mathfrak{n})$ i $X_0(\mathfrak{n})$.

Estudiem ara amb més detall les puntes.

8.2.4 Proposició. *Si* Γ *és un grup aritmètic, aleshores*

$$\mathit{Cusps}(\Gamma) \cong (\Gamma\backslash\mathbb{P}^1(K)).$$

Demostració (Idea): Recordem que les puntes es corresponen a les semilinees de $\Gamma\backslash\tau$, i que les semilinees de τ es corresponent als punts $s\in\mathbb{P}^1(K_\infty)$. Ara sols cal observar que del fet que Γ es aritmètic, si s ens dóna una semilínia de $\Gamma\backslash\tau$ no trivial, aleshores $s\in\mathbb{P}^1(K)$. □

8.2.5 Exemple. Si Y és una A-xarxa, aleshores $\mathrm{Cusps}(\mathrm{GL}(Y)) \cong \mathrm{Pic}(A)$.

Podem pensar així que

$$X(\Gamma)^{an} = \Gamma \backslash \left(\mathbb{H}_\infty \cup \mathbb{P}^1(K) \right).$$

8.2.6 Remarca. Per a calcular el gènere de $X(\Gamma)$ podem utilitzar que

$$g(X(\Gamma)) = \text{rank}_{\mathbb{Z}}((\Gamma/\Gamma_f)^{ab}) = \text{rank}_{\mathbb{Z}}(\Gamma^{ab}/tor(\Gamma^{ab})),$$

o bé, si sabem el gènere de $X(\Gamma(1))$ i $\Gamma \subset \Gamma(1)$, podem utilitzar la fórmula de Hurwitz via el morfisme

$$X(\Gamma) \longrightarrow X(\Gamma(1)).$$

8.3 Racionalitat

Per a poder demostrar que les corbes definides anteriorment sobre $\mathbb{C}_\infty$ i K_∞ estan de fet definides a K o a una certa extensió finita de K (de fet tenen models enters naturals definits a l'anell d'enters o a certs ordres en l'anell d'enters) necessitem veure que representen certs problemes de moduli i que aquests problemes de moduli són de fet representables al cos que volem. Però per a poder veure que representen certs problemes de moduli ens trobem primer amb el problema de definir que vol dir un mòdul de Drinfeld definit sobre un A-esquema qualsevol, i després definir estructura de nivell en un mòdul de Drinfeld. Per a poder definir estructura de nivell el cas més difícil és quan el "nivell" divideix la "característica": per a fer-ho Drinfeld va introduir una noció d'estructura de nivell que de fet va ser utilitzada posteriorment per Katz i Mazur en el món de les corbes modulars clàssiques (vegis [K-M]).

Comencem primer per a definir que es un mòdul de Drinfeld sobre un A-esquema S qualsevol; intuitivament, un mòdul de Drinfled sobre S és una familia continua de mòduls de Drinfeld sobre els cossos residuals de S.

8.3.1 Definició Sigui S un A-esquema i $\mathcal{L}$ un fibrat de linea sobre S. Un mòdul de Drinfeld $(\mathcal{L}, \phi)$ de rang r sobre S és un morfisme d'anells

$$\phi \colon A \longrightarrow \text{End}_S(\mathcal{L}, +)$$

$$f \mapsto \phi_f$$

en l'anell d'isomorfismes del esquema en grups additiu $(\mathcal{L}, +)$, verificant la següent condició: Existeix una trivialització de $\mathcal{L}$ per oberts afins $\mathrm{Spec}(B)$ de S tal que

$$\phi_f|\,\mathrm{Spec}(B) = \sum_{i=0}^{N(f)} a_i \tau^i$$

amb $a_i \in B$, a_0 igual a la imatge de f sota el morfisme canònic de A a B, $N(f) = r \cdot \deg(f)$ i el coeficient $a_{N(f)}$ una unitat en B.

Escriurem abreujadament ϕ per l'objecte $(\mathcal{L}, \phi)$. Un morfisme entre dos mòduls de Drinfeld és un morfisme entre els esquemes en grup corresponents compatibles amb l'acció de A.

Per a tal de poder estudiar el functor $\mathcal{M}_1^r$ que assigna a cada esquema S el conjunt de mòduls de Drinfeld de rang r sobre S (mòdul isomorfismes), ens cal, com en el cas de les corbes modulars "clàssiques", introduir estructures de nivell.

Donat un mòdul de Drinfeld ϕ sobre S i $0 \neq f \in A$, definim l'esquema ${}_f\phi$ de f-divisió com el subesquema $\mathrm{Ker}(\phi_f)$ de $(\mathcal{L}, +)$. Ara, si $\mathfrak{n}$ és un ideal de A no necessariament principal definim

$${}_{\mathfrak{n}}\phi := \bigcap_{f \in \mathfrak{n}} {}_f\phi.$$

No és difícil veure que ${}_{\mathfrak{n}}\phi$ és un esquema finit i pla de grau $\sharp(A/\mathfrak{n})^r$ sobre A, que és étale fora del suport de $\mathfrak{n}$. A més, si L és un cos algebraicament tancat, ${}_{\mathfrak{n}}\phi$ és isomorf com a A-mòdul a $(A/\mathfrak{n})^r$ si la característica de L (coma A-mòdul) no divideix a $\mathfrak{n}$, i a $(A/\mathfrak{n})^s$ per algun $s < r$ si divideix a $\mathfrak{n}$.

Intuitivament, una estructura de $\mathfrak{n}$-nivell hauria de ser l'elecció de d'un isomorfisme de $(A/\mathfrak{n})^r$ amb ${}_{\mathfrak{n}}\phi$. Això funciona bé fora del support de $\mathfrak{n}$, però és clar que si alguna característica residual de S divideix a $\mathfrak{n}$.

8.3.2 Definició Sigui ϕ un mòdul de Drinfeld de rang r sobre un A-esquema S, i sigui $\mathfrak{n}$ un ideal de A. Una estructura de nivell $\mathfrak{n}$ a ϕ

és un homomorfisme de A-mòduls

$$\varphi\colon (A/\mathfrak{n})^r \longrightarrow \mathcal{L}(S)$$

tal que

$$\sum_{f\in(A/\mathfrak{n})^r} \varphi(f) =_{\mathfrak{n}} \phi$$

vistos com a divisors de Cartier sobre S.

Considerem ara el functor

$$\mathcal{M}^r_{\mathfrak{n}}\colon \underline{\text{Schemes}}_A \rightsquigarrow \underline{\text{Sets}}$$

que assigna a cada S-esquema el conjunt de classes d'isomorfia de mòduls de Drinfeld de rank r sobre S amb una estructura de nivell $\mathfrak{n}$ (l'isomorfisme respectant l'estructura de nivell). Aquest functor no és representable per un esquema en general: per exemple, per estructura de nivell 1, o sigui sense estructura de nivell, si el functor fos representable tindríem que dos mòduls de Drinfeld no isomorfs no poden esdevenir isomorfs al fer un canvi de base. Per tal que pugui ser representable necessitem que els objectes que classifiquen no tinguin automorfismes. Una altre possible solució, que no desenvoluparem aquí podria ser estudiar la representabilitat de $\mathcal{M}^r_{\mathfrak{n}}$ com a stack algebraic: es un exercici fàcil de la teoria de stack veure aquesta representabilitat a partir dels resultat següent (demostrat en l'article seminal de Drinfeld [3])

8.3.1 Teorema *(Drinfeld) Suposem que $\mathfrak{n}$ és un ideal primer de A. Aleshores el functor $\mathcal{M}^r_{\mathfrak{n}}$ restringit als esquemes $S/\operatorname{Spec}(A[1/\mathfrak{n}])$ és representable per un esquema $M^r_{\mathfrak{n}}$ afí, llis i de dimensió relativa $r-1$.*

L'existència de $M^r_{\mathfrak{n}}$ no és molt difícil de provar: de fet és pot descriure com l'espectre de certa A-algebra donada explícitament amb generadors i relacions. El que és realment la part més difícil es demostrar que és llis, resultat que Drinfeld dedueix d'un anàlisis acurat de les propietats de deformació dels mòduls de Drinfeld.

D'aquest resultat podem demostrar ja, utilitzant tècniques ara ja estàndard, la representabilitat en general del functor $M^r_{\mathfrak{n}}$ sobre A quan $\mathfrak{n}$ és divisible per a dos o més ideals diferents.

8.3.3 Corol·lari. *Si* $\mathfrak{n}$ *és divisible per a dos ideals primers diferents, aleshores* $\mathcal{M}^r_{\mathfrak{n}}$ *és representable sobre* A *per un esquema afí i de tipus finit.*

8.3.4 Exemple. Anem a posar un exemple que lliga amb el que hem fet al Capítol 6. Si ens situem en el cas que $r = 1$, tenim que

$$M^1_\eta = \mathrm{Spec}(A(\eta)),$$

on $A(\eta)$ és la clausura entera de A a $H(\eta)$, cos que classes radial de Hilbert corresponent a $\eta \cup \infty$ (i.e. no ramificat fora de η i de ∞).

Un cop demostrada la existència de l'espai de moduli, sota certes condicions, ens podem preguntar ara per l'existència del espai de moduli "groller"per en general. Una possible manera de fer-ho, com en el cas de les corbes modulars "clàssiques", és la següent: donat $\mathfrak{n}$ qualsevol (per exemple, l'ideal (1)), prenem $\mathfrak{m}$ un ideal que el conté i divisible per dos o més ideals primers diferents. Construïm aleshores $M^r(\mathfrak{n})$ com a un quocient de $M^r(\mathfrak{m})$ respecte l'acció d'un cert grup ($\approx GL_r(\mathfrak{n}/\mathfrak{m})$).

Una altre manera, molt millor ja que ens dona la construcció de molts més espais de moduli (com les corbes de moduli $Y_0(\mathfrak{n})$ que utilitzarem en el capítol 10) és utilitzar la torre modular: Considerem

$$M^r := \varprojlim_{\mathfrak{n}} M^r(\mathfrak{n}),$$

que pot ser descrit com l'espai de moduli dels mòduls de Drinfeld de rank r amb un sistema compatible de estructures de nivell $\mathfrak{n}$ per a tot $\mathfrak{n}$ "prou gran".

Considerem ara $\widehat{A} := \varprojlim_{\mathfrak{n}} A/\mathfrak{n}$ i

$$1 \; to \, \mathrm{GL}_r(\widehat{A}, \mathfrak{n}) \to \mathrm{GL}_r(\widehat{A}) \to \mathrm{GL}_r(A/\mathfrak{n}) \to 1$$

el nucli del morfisme reducció. Tenim aleshores una acció natural de $\mathrm{GL}_r(\widehat{A}, \mathfrak{n})$ a M^r (actuen com a matrius en els sistemes compatibles d'estructures de nivell), i un isomorfisme canònic:

$$\mathrm{GL}_r(\widehat{A}, \mathfrak{n}) \backslash M^r \xrightarrow{\sim} M^r(\mathfrak{n})$$

sempre que $M^r(\mathfrak{n})$ està definit. En el casos en que no ho està definim $M^r(\mathfrak{n})$ simplement com aquest quocient.

Finalment, observem que podem fer aquesta construcció per a un subgrup *obert* $\mathcal{K}$ qualsevol de $\mathrm{GL}_r(\widehat{A})$.

8.3.5 Exemple. Donat $\mathfrak{n}$ un ideal qualsevol de A, considerem el subgrup de $\mathrm{GL}_2(\widehat{A})$ donat per

$$\mathcal{K}_0(\mathfrak{n}) := \left\{ \begin{pmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{pmatrix} \in \mathrm{GL}_e(\widehat{A}) \mid \underline{c} \equiv 0 (mod \mathfrak{n}) \right\}.$$

Definim la corba modular $Y_0(\mathfrak{n})$ com el quocient de M^2 per $\mathcal{K}_0(\mathfrak{n})$; no és un esquema de moduli fi mai sobre S, però és especialment important per raons aritmètiques com veurem en el capítol 10.

Bibliografia

[Dr] *V.G. Drinfeld*, Elliptic modules, Math. USSR-Sb. 23 (4), (1976), 561-592.

[In] *C.A. Infante*, Uniformización de curvas de Mumford y Jacobianas, Notes del STNB2002, Capítol 7.

[GPR] *E.-U. Gekeler, M. van der Put, M. Reversat*, Proceedings of the work- shop on: Drinfeld Modules, modular schemes and applications, 106-109. September 1996. World Scientific (1997).

[K-M] *Katz, Mazur*, Aritmetic moduli of elliptic curves. Ann. of Math. Stud. 108, Princeton 1985.

[R] *M. Reversat*, Sur les revètemens de Schottky dels courbes modu- lares.Arch. Math (Basel) 66 (1996)n 5, 378-387.

[Ro] *V. Rotger*, Uniformització analítica dels mòduls de Drinfeld, Notes del STNB2002, Capitol 3.

[Se] *J.-P. Serre*, Arbres, Amalgames, SL_2, Lecture Notes in Mathematics.

[Xa] *X. Xarles*, Uniformització p-àdica de corbes de Shimura, Notes del STNB2001.

X. Xarles
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
xarles@mat.uab.es

Capítol 9

Formes modulars de Drinfeld

Enric Nart

Recordem la situació clàssica. Tota corba el·líptica complexa admet una uniformització analítica:

$$\begin{array}{ccccc} \mathbb{C}/\Lambda & \xrightarrow{\sim} & E_\Lambda(\mathbb{C}) & \subseteq & \mathbb{P}^2(\mathbb{C}), \\ z & \mapsto & (\mathfrak{P}_\Lambda(z), \mathfrak{P}'_\Lambda(z), 1) & & \end{array}$$

on Λ és una xarxa de $\mathbb{C}$. Tenim ben controlada la variació de les classes d'isomorfisme de corbes el·líptiques en funció de la xarxa:

$$\begin{array}{ccccccc} \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} & \leftrightarrow & \{\text{xarxes de } \mathbb{C}\}/_{\text{sem}} & \leftrightarrow & \{\text{c.e.}_{|\mathbb{C}}\}/_{\text{isom}} & \overset{j}{\leftrightarrow} & \mathbb{C} \\ z & \mapsto & \langle\, z, 1 \,\rangle_{\mathbb{Z}} = \Lambda & \mapsto & E_\Lambda & \mapsto & j(E_\Lambda) \end{array}$$

La funció modular j s'expressa en termes d'altres formes modulars, g_2, g_3, Δ, totes elles calculables en funció de sèries d'Eisenstein, que són formes modulars bàsiques que apareixen com els coeficients de la sèrie de Taylor de $\mathfrak{P}_\Lambda$, i es poden calcular directament a partir de la xarxa.

$$\mathfrak{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{k\geq 2}(k+1)E_{k+2}(\Lambda)z^k, \qquad E_k(\Lambda) = \sum_{\alpha\in\Lambda}{}' \frac{1}{\alpha^k}.$$

La corba plana $E_\Lambda(\mathbb{C})$ satisfà l'equació:

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

on

$$g_2(\Lambda) = 60E_4(\Lambda), \quad g_3(\Lambda) = 140E_6(\Lambda),$$

Tenim, finalment,

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0, \qquad j(\Lambda) = 1728g_2(\Lambda)^3/\Delta(\Lambda).$$

Les formes modulars de Drinfeld han de permetre descriure, també, la variació, respecte de la xarxa Λ, de les classes d'isomorfia dels mòduls de Drinfeld ϕ_Λ sobre $\mathbb{C}_\infty$.

Introduïm els primers exemples de formes modulars de Drinfeld, a partir de sèries d'Eisenstein, que es poden definir d'una manera completament anàloga, a partir d'una xarxa de $\mathbb{C}_\infty$.

9.1 Sèries d'Eisenstein

$\mathbb{A}$ anell de Drinfeld, Λ xarxa de $\mathbb{C}_\infty$ de rang r. Definim,

$$E_k(\Lambda) := \sum_{\alpha\in\Lambda}{}' \frac{1}{\alpha^k}, \quad k \geq 1.$$

La sèrie convergeix pel caràcter discret de Λ.

9.1.1 Propietats

- $E_{kp}(\Lambda) = E_k(\Lambda)^p, \quad \forall k \geq 1,$
- $E_k(a\Lambda) = a^{-k}E_k(\Lambda), \quad \forall k \geq 1, \ \forall a \in \mathbb{A}$

- $k \not\equiv 0 \phi : \mathbb{A} \to \mathcal{F}\{\tau\} q - 1 \implies E_k(\Lambda) = 0$
  (surt de $a\Lambda = \Lambda$, per a algun $a \in \mathbb{F}_q^*$ amb $a^k \neq 1$)
- $E_0(\Lambda) = -1$ per conveni.

Comprovem que els coeficients de Taylor de la funció exponencial de la xarxa s'expressen en termes de sèries d'Eisenstein. Considerem,

$$e_\Lambda(\tau) = \sum_{n=0}^{\infty} \alpha_n \tau^n, \qquad \log_\Lambda(\tau) = \sum_{n=0}^{\infty} \beta_n \tau^n,$$

una inversa de l'altra com a elements de $\mathbb{C}_\infty\{\{\tau\}\}$.

Tenim $\alpha_0 = \beta_0 = 1$, i els coeficients β_n estan unívocament determinats pels α_n i per β_0, a través de la relació:

$$\left(\sum_{n=0}^{\infty} \alpha_n \tau^n\right)\left(\sum_{n=0}^{\infty} \beta_n \tau^n\right) = 1 \implies \sum_{n=0}^{k} \alpha_n \beta_{k-n}^{q^n} = 0, \quad \forall k \geq 1.$$

9.1.2 Teorema. $\beta_k = -E_{q^k-1}(\Lambda), \quad \forall k \geq 0.$

Demostració: Treballem a $\mathbb{C}_\infty[[z]]$, després de fer el canvi $\tau = z^q$.

$$e_\Lambda(z) = z \prod_{\alpha \in \Lambda}{}' (1 - \frac{z}{\alpha}) \implies \frac{1}{e_\Lambda(z)} = \frac{e'_\Lambda(z)}{e_\Lambda(z)} = \sum_{\alpha \in \Lambda} \frac{1}{z - \alpha},$$

on l'última igualtat s'obté derivant productes finits i passant al límit. Aquesta sèrie defineix una funció meromorfa sobre $\mathbb{C}_\infty$, amb pols a $\Lambda \setminus \{0\}$; per tant, és holomorfa en un entorn de zero. Dins del domini d'holomorfia tenim,

$$\frac{z}{e_\Lambda(z)} = \sum_{\alpha \in \Lambda} \frac{z}{z - \alpha} = 1 - \sum_{\alpha \in \Lambda}{}' \frac{z/\alpha}{1 - z/\alpha} = 1 - \sum_{\alpha \in \Lambda}{}' (\frac{1}{\alpha} z + \frac{1}{\alpha^2} z^2 + \cdots) =$$
$$= -\sum_{k \geq 0} E_k(\Lambda) z^k.$$

Finalment, imposant l'anul.lació del terme en z^{q^k-1},

$$\left(\sum_{n=0}^{\infty}\alpha_n z^{q^n-1}\right)\left(\sum_{n=0}^{\infty}E_n(\Lambda)z^n\right)=-1 \implies$$

$$\implies 0=\sum_{n=0}^{k}\alpha_n E_{q^k-q^n}=\sum_{n=0}^{k}\alpha_n E_{q^{k-n}-1}^{q^n}.$$

□

9.1.3 Corol.lari. *Sigui $\phi=\phi_\Lambda$ el mòdul de Drinfeld associat a Λ. Per a qualsevol $a\in\mathbb{A}$,*

$$\phi_a(\tau)=a\tau^0+\ell_1\tau+\cdots+\ell_m\tau^m \implies aE_{q^k-1}=\sum_{n=0}^{k}E_{q^n-1}\ell_{k-n}^{q^n},\quad \forall k\geq 1.$$

En particular, els ℓ_n són polinomis isobàrics de pes q^n-1 en les E_k (suposades de pes k).

Demostració:

$$a\log_\Lambda(\tau)=\log_\Lambda(\tau)e_\Lambda(\tau)a\log_\Lambda(\tau)=\log_\Lambda(\tau)\phi_a(\tau)e_\Lambda(\tau)\log_\Lambda(\tau)=$$

$$=\log_\Lambda(\tau)\phi_a(\tau)\implies a\beta_k=\sum_{n=0}^{k}\beta_n\ell_{k-n}^{q^n},\quad\forall k\geq 1.$$

□

Per exemple, si prenem $\mathbb{A}=\mathbb{F}_q[T]$ i $\Lambda=\xi\mathbb{A}$ com a xarxa de rang 1 (vegeu el capítol 2), obtenim el mòdul de Carlitz, $C_T(\tau)=T+\tau$. Pel Corol·lari,

$$TE_{q-1}(\Lambda)=-1+E_{q-1}(\Lambda)T^q \implies E_{q-1}(\Lambda)=\frac{1}{T^q-T}.$$

Si prenem la pròpia $\mathbb{A}=\mathbb{F}_q[T]$ com a xarxa de rang 1, com que és semblant a la xarxa Λ, obtenim un mòdul de Drinfeld, $\phi_T(\tau)=T+c\tau$, isomorf al mòdul de Carlitz. El Corol·lari ens dóna ara $E_{q-1}(\mathbb{A})=c/(T^q-T)$. Com que $E_{q-1}(\mathbb{A})=\xi^{q-1}E_{q-1}(\Lambda)$, tenim la relació:

$$\xi^{q-1}=(T^q-T)E_{q-1}(\mathbb{A}),$$

anàloga a la relació clàssica $(2\pi i)^2=-24\zeta(2)=-12E_2(\mathbb{Z})$.

Noteu que el pes $2=\sharp\mathbb{Z}^*$ en la teoria clàssica, es converteix en $q-1=\sharp\mathbb{A}^*$, quan treballem amb cossos de funcions.

9.2 Anàlisi rígid sobre el semiplà superior de Drinfeld

El semiplà superior de Drinfeld es defineix

$$\mathbb{H}_\infty := \mathbb{C}_\infty - K_\infty = \mathbb{P}^1_K(\mathbb{C}_\infty) - \mathbb{P}^1_K(K_\infty).$$

9.2.1 Definició. La *part imaginària* d'un $z \in \mathbb{C}_\infty$ és:

$$|z|_i := \mathrm{d}(z, K_\infty) = \inf\{|z - x| \mid x \in K_\infty\}.$$

Gaudeix de les següents propietats:

- $\exists\ z \in K_\infty : \quad |z|_i = |z - x| \qquad (K_\infty \text{ loc. compacte})$
- $|\gamma(z)|_i = |\det(\gamma)||z|_i/|cz + d|^2$
- $\mathbb{H}_\infty = \{z \in \mathbb{C}_\infty \mid |z|_i > 0\} = \bigcup_{n\geq 0} U_n$, on $U_n = \{z \in \mathbb{C}_\infty \mid |z| \leq q^n,\ |z|_i \geq q^{-n}\}$.

9.2.2 Definició

- $U_n \xrightarrow{f} \mathbb{C}_\infty$ holomorfa si és límit uniforme d'una successió de funcions racionals sense pols a U_n.
- $U_n \xrightarrow{f} \mathbb{C}_\infty$ meromorfa si existeix una funció racional g sense pols a U_n tal que gf és holomorfa.
- $\mathbb{H}_\infty \xrightarrow{f} \mathbb{C}_\infty$ holomorfa/meromorfa si ho és restringida a cada U_n

Per exemple, podem pensar les sèries d'Eisenstein com a funcions sobre el semiplà superior:

$$E_k(z) = {\sum_{a,b\in\mathbb{A}}}' \frac{1}{(az + b)^k},$$

entenent que cada $z \in \mathbb{H}_\infty$ dóna lloc a la xarxa $\langle\, z, 1 \,\rangle_{\mathbb{A}}$. És clar que $E_k(z)$ és límit de funcions racionals amb pols concentrats a K_∞ i és fàcil comprovar que el límit és uniforme sobre els U_n. Per tant, les sèries d'Eisenstein són funcions holomorfes sobre $\mathbb{H}_\infty$.

9.3 Més exemples de formes modulars

Suposem d'ara endavant:

$$\mathbb{A} = \mathbb{F}_q[T], \qquad \mathfrak{m} = \mathrm{GL}_2(\mathbb{A}).$$

Donats $z_1, z_2 \in \mathbb{C}_\infty$, el $\mathbb{A}$-mòdul $\Lambda = \mathbb{A}\, z_1 + \mathbb{A}\, z_2$ és discret sii z_1, z_2 són K_∞-linealment independents. Recordem que "discret" vol dir que cada $B(0,r)$ conté un nombre finit d'elements. Aquest concepte no coincideix amb el concepte merament topològic de discreció perquè $\mathbb{C}_\infty$ no és localment compacte (el seu cos residual és $\overline{\kappa(\infty)}$).

En el cas en que estem, la uniformització analítica del capítol 3 ens permet reproduir la situació clàssica per als mòduls de Drinfeld de rang 2. Tot mòdul de Drinfeld sobre $\mathbb{C}_\infty$ ve determinat per una xarxa:

$$e_\Lambda \colon \mathbb{C}_\infty/\Lambda \xrightarrow{\sim} \mathbb{C}_\infty, \qquad (\phi_\Lambda)_a\,(e_\Lambda(x)) = e_\Lambda(ax),\ \forall a \in \mathbb{A},\, x \in \mathbb{C}_\infty,$$

i tenim, també, ben controlada la variació de les classes d'isomorfisme de mòduls de Drinfeld de rang 2 en funció de la xarxa:

$$\begin{array}{ccccccc} \mathfrak{m}\backslash\mathbb{H}_\infty & \leftrightarrow & \left\{\begin{array}{c}\text{xarxes de}\\ \text{rang 2 de } \mathbb{C}_\infty\end{array}\right\}\!/\text{sem} & \leftrightarrow & \left\{\begin{array}{c}\text{m.D.}_{|\mathbb{C}_\infty}\\ \text{de rang 2}\end{array}\right\}\!/\text{isom} & \overset{j}{\leftrightarrow} & \mathbb{C}_\infty \\ z & \mapsto & \langle z, 1\rangle_{\mathbb{A}} = \Lambda & \mapsto & \phi_\Lambda & \mapsto & j(\phi_\Lambda) \end{array}$$

Disposem de formes modulars $g(\Lambda)$, $\Delta(\Lambda)$, $j(\Lambda)$, definides per:

$$(\phi)_T\,(\tau) = T + g(\Lambda)\tau + \Delta(\Lambda)\tau^2, \qquad j(\Lambda) := \frac{g(\Lambda)^{q+1}}{\Delta(\Lambda)}.$$

Com a funcions sobre $\mathbb{H}_\infty$, les funcions g i Δ són holomorfes perquè, com hem vist al Corol·lari de la secció anterior, són polinomis en les sèries d'Eisenstein. De fet, aplicant el Corol·lari per a k=1, obtenim:

$$TE_{q-1} = -g + E_{q-1}T^q \implies g = (T^q - T)E_{q-1},$$

relació anàloga a la relació clàssica $g_2 = 60E_4$; mentre que si apliquem el Corol·lari per a $k = 2$, obtenim:

$$\begin{aligned} TE_{q^2-1} = -\Delta + E_{q-1}g^q + E_{q^2-1}T^{q^2} &\implies \\ &\implies \Delta = (T^{q^2} - T)E_{q^2-1} + (T^q - T)^q E_{q-1}^{q+1}, \end{aligned}$$

anàleg a $\Delta = g_2^3 - 27g_3^2 = (60E_4)^3 - 27(140E_6)^2$.

9.4 Holomorfia a l'infinit

Continuem en el cas $\mathbb{A} = \mathbb{F}_q[T]$, $\mathfrak{m} = \mathrm{GL}_2(\mathbb{A})$. Les "puntes" del semiplà superior de Drinfeld estan classificades per Pic$\mathbb{A}$, a través de la bijecció natural:

$$\mathfrak{m}\backslash\mathbb{P}^1(K) \;\leftrightarrow\; \mathrm{Pic}\mathbb{A}, \qquad (\lambda_0, \lambda_1) \mapsto \left\langle\, \lambda_0, \lambda_1 \,\right\rangle_{\mathbb{A}} \subseteq K.$$

En el nostre cas, doncs, hi ha una única punta: ∞.

Fixem $1 < c \in q^{\mathbb{Q}}$ i considerem l'entorn de ∞:

$$U_c = \{z \in \mathbb{H}_\infty \mid |z|_i \geq c\}.$$

9.4.1 Fet. *U_c és un obert admissible, i*

$$\gamma U_c \cap U_c \neq \emptyset \iff \gamma(\infty) = \infty.$$

Per tant, tenim una immersió oberta d'espais analítics:

$$\Gamma_\infty\backslash U_c = \mathfrak{m}\backslash U_c \subseteq \mathfrak{m}\backslash\mathbb{H}_\infty.$$

Volem parametritzar $\Gamma_\infty\backslash U_c$. D'entrada, el subgrup d'isotropia de l'infinit el podem descompondre:

$$\Gamma_\infty \simeq \mathbb{F}_q^* \times \mathbb{A} \rtimes \mathbb{F}_q^*, \qquad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & da^{-1} \end{pmatrix}.$$

Com que $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ actua com la identitat,

$$\Gamma_\infty\backslash U_c = (\mathbb{A} \rtimes \mathbb{F}_q^*)\backslash U_c = \mathbb{F}_q^*\backslash(\mathbb{A}\backslash U_c),$$

on $\mathbb{A}$ opera sobre U_c sumant, i $\mathbb{F}_q^*$ opera multiplicant. Les operacions no commuten, $\lambda(z + b) \neq \lambda z + b$, però els conjunts quocients estan ben definits.

Concentrem-nos de moment en $\Gamma_\infty\backslash U_c$. D'entrada, podem utilitzar la funció exponencial $e_{\mathbb{A}}$ com a paràmetre local:

$$e_{\mathbb{A}} \colon \mathbb{C}_\infty/\mathbb{A} \;\xrightarrow{\sim}\; \mathbb{C}_\infty.$$

Com que $e_{\mathbb{A}}$ no s'anul·la a U_c, podem utilitzar també:

$$\begin{array}{ccc} U_c & \xrightarrow{t} & \mathbb{C}_\infty \\ \downarrow & \nearrow & \\ \mathbb{A}\backslash U_c & & \end{array}, \qquad t(z) := \frac{1}{\xi e_{\mathbb{A}}(z)} = \frac{1}{e_\Lambda(\xi z)},$$

on $\Lambda = \xi\mathbb{A}$. Noteu l'analogia amb $q = \exp(2\pi i z)$, sobre $\mathbb{Z}\backslash U_c$, en el cas clàssic.

9.4.2 Fet. *t indueix un isomorfisme analític,*

$$\mathbb{A}\backslash U_c \xrightarrow[\sim]{t} B(0, r_c) \setminus \{0\},$$

i podem estendre aquesta bijecció a la punta, assignant $\infty \mapsto 0$.

Pareu atenció al fet que t no és invariant per l'acció de $\mathbb{F}_q^*$. Per la $\mathbb{F}_q$-linealitat de $e_{\mathbb{A}}$,

$$t(\lambda z) = \frac{1}{\xi e_{\mathbb{A}}(\lambda z)} = \frac{1}{\xi\lambda e_{\mathbb{A}}(z)} = \frac{1}{\lambda}\, t(z), \quad \forall \lambda \in \mathbb{F}_q^*.$$

Per tant el paràmetre local genuí de $\Gamma_\infty\backslash U_c$ és t^{q-1}:

$$\begin{array}{ccc} \mathbb{A}\backslash U_c & \xrightarrow{t^{q-1}} & B(0, (r_c)^{q-1}) \setminus \{0\} \\ \downarrow & \nearrow_{\sim} & \\ \Gamma_\infty\backslash U_c = \mathbb{F}_q^*\backslash(\mathbb{A}\backslash U_c) & & \end{array}$$

De tota manera, s'acostumen a expressar els desenvolupaments de Fourier a l'infinit, respecte del paràmetre t.

Pensem, per simplificar, que la holomorfia a l'infinit es tradueix en el fet que la funció admeti un desenvolupament de Fourier respecte del paràmetre t.

Vegem a continuació com s'obtenen aquests desenvolupaments per a les sèries d'Eisenstein E_k. Recordem els anàlegs als polinomis ciclotòmics:

$$f_a(x) := x^{q^{\deg a}} C_a(x^{-1}) = a x^{q^{\deg a}-1} + \cdots + a_d \in \mathbb{A}[x],$$

on $a_d \in \mathbb{F}_q^*$ és el coeficient principal de $a \in \mathbb{F}_q[T]$. Noteu que $f_a(x)$ és invertible a $\mathbb{A}[[x]]$.

Es construeix una família unívocament determinada de polinomis $G_{k,\Lambda}(x)$, anomenats *polinomis de Goss*, que satisfan recurrències anàlogues a certes identitats trigonomètriques. L'holomorfia a l'infinit de E_k és conseqüència del següent resultat.

9.4.3 Teorema. *Per a $\Lambda = \xi\mathbb{A}$, es té:*

$$E_k(z) = \xi^k E_k(\Lambda) - \xi^k \sum_{a\in\mathbb{A}'} G_{k,\Lambda}(t_a(z)),$$

on $\mathbb{A}'$ denota el conjunt de polinomis mònics de $\mathbb{A}$, i:

$$t_a(z) := t(az) = \frac{1}{e_\Lambda(\xi az)} = \frac{1}{C_a(e_\Lambda(\xi z))} = \frac{1}{C_a(t^{-1}(z))} = \\ = \frac{t^{q^{\deg a}}}{f_a(t)} \in t^{q^{\deg a}}\mathbb{A}[[t]].$$

El polinomi $G_{k,\Lambda}(x)$ té coeficients a K i no té terme independent. Per tant,

$$G_{k,\Lambda}(t_a(z)) \in t^{q^{\deg a}}\mathbb{A}[[t]] \otimes_{\mathbb{A}} K,$$

és una sèrie formal amb coeficients fraccions de denominador acotat. Per tant, la t-expansió de $\xi^{-k}E_k$ té coeficients a K amb denominadors acotats.

Noteu que $E_k(\infty) = \xi^k E_k(\Lambda) \neq 0$, si $q-1|k$.

Utilitzant càlculs explícits dels polinomis de Goss per a $k = q-1$, q^2-1, obtenim:

$$\xi^{1-q}E_{q-1} = \frac{1}{[1]} - \sum_{a \text{ mònic}} t_a^{q-1}.$$

$$\xi^{1-q^2}E_{q^2-1} = -\frac{1}{[1][2]} - \sum_{a \text{ mònic}} t_a^{q^2-1} - \frac{1}{[1]}t_a^{q^2-q}.$$

D'aquí podem extraure els desenvolupaments de g, Δ. També s'obté una relació anàloga a la fórmula del producte de Jacobi. Per a

$$g_{\text{new}} := \xi^{1-q}g, \qquad \Delta_{\text{new}} := \xi^{1-q^2}\Delta \in \mathbb{A}[[t]],$$

es té:

$$\Delta_{\text{new}} = -t^{q-1} \prod_{a \text{ mònic}} f_a(t)^{(q^2-1)(q-1)}.$$

Heu de pensar que l'exponent q^2-1 fa el paper del 12 i l'exponent $q-1$ fa el paper del 2, de manera que l'exponent total és l'anàleg del 24 clàssic.

9.5 Formes modulars de Drinfeld

Continuem en el cas $\mathbb{A} = \mathbb{F}_q[T]$, $\mathfrak{m} = \mathrm{GL}_2(\mathbb{A})$.

Fixem $k \geq 0$ enter, i $m \in \mathbb{Z}/(q-1)\mathbb{Z}$.

9.5.1 Definició. Una forma modular de pes k i tipus m respecte de $\mathfrak{m}$ és una funció, $f\colon \mathbb{H}_\infty \longrightarrow \mathbb{C}_\infty$ satisfent:

1. f és holomorfa.
2. $f(\gamma(z)) = \det(\gamma)^{-m}(cz+d)^k f(z), \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{m}.$
3. f admet un desenvolupament, en algun entorn de ∞:

$$f(z) = \sum_{n=0}^{\infty} a_n t^n(z), \quad \forall |z|_i \geq c$$

9.5.2 Observacions

- Podem pensar m com el Nebentypus donat per una potència del caràcter $\mathfrak{m} \xrightarrow{\det} \mathbb{F}_q^*$, que té ordre $q-1$.
- $k \not\equiv 2m\phi : \mathbb{A} \to \mathcal{F}\{\tau\} q-1 \implies f = 0.$

$$f(z) = f(\gamma(z)) = \lambda^{-2m}\lambda^k f(z), \quad \forall \gamma = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},\ \lambda \in \mathbb{F}_q^*$$

- $n \not\equiv m\phi : \mathbb{A} \to \mathcal{F}\{\tau\}q - 1 \implies a_n = 0.$

  Per a $\gamma = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$, $\lambda \in \mathbb{F}_q^*$:

  $$\sum_{n=0}^{\infty} a_n \lambda^{-n} t^n(z) = f(\lambda z) = \lambda^{-m} f(z) = \sum_{n=0}^{\infty} a_n \lambda^{-m} t^n(z).$$

- $f(z)dz$ és $\mathfrak{m}$-invariant sii $k = 2$, $m = 1$.

  Només dóna lloc a una forma diferencial holomorfa de la corba $X(\mathfrak{m})$ si $a_0 = a_1 = 0$.

9.5.3 Exemples

- $E_k \in M_{k,0}(\mathfrak{m})$.
- $g \in M_{q-1,0}(\mathfrak{m})$, $\Delta \in M_{q^2-1,0}(\mathfrak{m})$.
- $\forall a \in \mathbb{A}$, tenim formes modulars $\ell_n \in M_{q^n-1,0}(\mathfrak{m})$, que provenen de considerar els coeficients de $\phi_a(\tau)$, variant ϕ entre tots els mòduls de Drinfeld de rang 2 sobre $\mathbb{C}_\infty$.
- sèries de Poincaré, $P_{k,m} \in M_{k,m}(\mathfrak{m})$.
- derivada de Serre, $M_{k,m}(\mathfrak{m}) \xrightarrow{\partial} M_{k+2,m+1}(\mathfrak{m})$

Espais de formes modulars

Denotem per $Z = \{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{F}_q^*\}$. Un punt $z \in \mathbb{H}_\infty$ es diu $\mathfrak{m}$-el·líptic si $Z \subsetneq \mathfrak{m}_z$. En el nostre cas, $\mathbb{A} = \mathbb{F}_q[T]$, $\mathfrak{m} = \mathrm{GL}_2(\mathbb{A})$, es té:

$$z \ \mathfrak{m}\text{-el·líptic} \iff z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \iff j(z) = 0,$$

de manera que hi ha un únic punt $\mathfrak{m}$-el·líptic a $\mathfrak{m}\backslash\mathbb{H}_\infty$.

Per als punts $\mathfrak{m}$-el·líptics tenim,

$$\mathfrak{m}_z \xrightarrow{\sim} \mathbb{F}_{q^2}^*, \qquad \gamma \mapsto \text{ valor propi del vector } (z, 1).$$

Per tant, $\sharp(\mathfrak{m}_z/Z) = q+1$, i $\mathbb{H}_\infty \xrightarrow{j} \mathbb{C}_\infty$ és un revestiment ramificat de $\mathbb{C}_\infty$, amb índex $q + 1$ als punts el·líptics.

Anàlogament al cas clàssic, per a tota $f \in M_{k,m}(\mathfrak{m})$, $f \neq 0$ es té:

$$\sum_{z \in \mathfrak{m} \backslash \mathbb{H}_\infty}{}^{*} \operatorname{ord}_z(f) + \frac{1}{q+1} \operatorname{ord}_e(f) + \frac{1}{q-1} \operatorname{ord}_\infty(f) = \frac{k}{q^2-1},$$

on e denota un punt el·líptic i $\sum^*$ exclou els punts el·líptics.

De manera completament anàloga al cas càssic, d'aquest resultat es deriva un còmput de la dimensió de l'espai de formes modulars:

$$\dim_{\mathbb{C}_\infty} M_{k,m}(\mathfrak{m}) = \left[\frac{k}{q^2-1}\right] \quad \left(+1 \text{ si } k\phi : \mathbb{A} \to \mathcal{F}\{\tau\} q^2 - 1 \geq m(q+1)\right),$$

i l'estructura de $\mathbb{C}_\infty$-àlgebra del conjunt de totes les formes modulars:

$$M_0(\mathfrak{m}) := \oplus_{k \geq 0} M_{k,0}(\mathfrak{m}) = \mathbb{C}_\infty[g, \Delta],$$

$$M(\mathfrak{m}) := \oplus_{k \geq 0,\, m \in \mathbb{Z}/(q-1)\mathbb{Z}} M_{k,m}(\mathfrak{m}) = \mathbb{C}_\infty[g, h],$$

on $h \in M_{q+1,1}(\mathfrak{m})$ és una sèrie de Poincaré satisfent $h^{q-1} = c\Delta$, per a certa constant $c \in \mathbb{C}_\infty^*$.

També tenim formes modulars amb coeficients enters:

$$M_{k,m}(\mathfrak{m})(\mathbb{A}) := M_{k,m}(\mathfrak{m}) \cap \mathbb{A}[[t]],$$

i tenim:

$$M_0(\mathfrak{m})(\mathbb{A}) = \mathbb{A}[g_{\text{new}}, \Delta_{\text{new}}], \qquad M(\mathfrak{m})(\mathbb{A}) = \mathbb{A}[g_{\text{new}}, h].$$

Bibliografia

[1] *E.-U. Gekeler*, Lectures on Drinfeld modules.
http://cicma.mathstat.concordia.ca/faculty/cicma/CP99.html.

E. Nart
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
nart@mat.uab.es

Capítol 10

L'anàleg per a cossos de funcions de la conjectura de Shimura Taniyama Weil

Francesc Bars

Exposició: 8 de Febrer 2002

10.1 Introducció

Quins problemes i conjectures clàssiques en cossos de nombres tenen una analogia en cossos de funcions, i com és aquesta analogia? Aquesta exposició intenta explicar aquesta pregunta referent a la conjectura de Shimura-Taniyama-Weil. Recordem que aquesta conjectura, recentment 1995-99 provada, (Wiles [17] i en generalitat per Breuil-Conrad-Diamond-Taylor [1]), ha estat a la mira de tot amant de la Teoria de nombres després de que Ribet [12] va demostrar que la prova d'aquesta conjectura implicava el teorema de Fermat.

Sota el support econòmic de DGI, BHA2000-0180.

10.1.1 Conjectura (Shimura-Taniyama-Weil) *Sigui E una corba el·líptica definida sobre $\mathbb{Q}$ amb conductor N. Llavors existeix un morfisme π definit sobre $\mathbb{Q}$ de la corba modular $X_0(N)$ en E,*

$$\pi : X_0(N) \to E.$$

En aquesta situació tenim una bijecció entre:

1. *classes d'isogènia sobre $\mathbb{Q}$ de corbes el·líptiques definides sobre $\mathbb{Q}$ amb conductor N.*
2. *Factors 1 dimensionals de la $\mathbb{Q}$-descomposició de la part nova de la Jacobiana de $X_0(N)$, que denotem per $J_0^{new}(N)$.*
3. *formes noves cuspidals normalitzades de $S_2(\Gamma_0(N))$, vector propi dels operadors de Hecke.*

En el cas de cossos de funcions, tenim espais de moduli groller per mòduls de Drinfeld de rang r amb estructura de nivell, [18]. El cas anàleg de les corbes modulars $X_0(N)$ en cossos de funcions correspond als espais de moduli $X_0(\mathfrak{n})$ ([18]) amb un punt ∞ del cos de funcions fixat i $\mathfrak{n}$ un ideal coprimer amb ∞. Aquestes corbes corresponen a certs espais de moduli groller anteriors amb $r = 2$ amb nivell $\infty\mathfrak{n}$. Drinfeld va provar que aquestes corbes tenen en la seva jacobiana les corbes el·líptiques definides sobre el mateix cos de funcions amb conductor igual al nivell de la corba modular $X_0(\mathfrak{n})$ i això ens permet fer una conjectura anàloga pel cas de cossos de funcions; vegeu §2 per a la seva formulació.

En el cas de cossos de funcions, la prova és molt fàcil gràcies que tenim que les funcions L per corbes el·líptiques sobre cossos de funcions tenen les propietats desitjades (Deligne); en el cas de les corbes el·liptiques sobre $\mathbb{Q}$ aquest fet es dedueix després d'haver provat la conjectura de Shimura-Taniyama-Weil, ja que es coneixia el resultat per la funció L associada a una forma cuspidal nova, però en principi no per la funció L per una corba el·líptica definida sobre $\mathbb{Q}$.

Aquest capítol de [16] esbossa els principals elements per la formulació de la conjectura pel cas de cossos de funcions, la prova i questions sobre parametritzacions de Weil en el cas més simple de $\mathbb{P}^1$

sobre un cos finit $\mathbb{F}_q$(que com a cos de funcions correspon a $\mathbb{F}_q(T)$). Per veure el cas general de tota corba C projectiva no singular definida sobre $\mathbb{F}_q$ vegeu l'article original de Gekeler i Reversat [8]. Una altra referència interessant és l'article de Gekeler [7] en que fa un survey de l'article [8].

Notacions

Fixem notacions per tot aquest capítol. C denota una corba projectiva no singular, geomètricament connexa sobre el cos finit $\mathbb{F}_q$ de característica p, $q = p^e$. Fixem ∞ un punt de la corba C, $\mathbb{A}$ denota l'anell de funcions regulars en $C \setminus \{\infty\}$, K és el cos quocient, K_∞ la completació en la plaça ∞ de K. Per simplificar l'exposició prendrem que $C = \mathbb{P}^1_{\mathbb{F}_q}$ i que l'uniformitzant de ∞ sigui $\frac{1}{T}$, i considerarem

$$(K, \infty, \mathbb{A}) = (\mathbb{F}_q(T), \infty, \mathbb{F}_q[T]).$$

Observem que $cl(K) = 1$ cosa que fa menys tècnica la presentació dels resultats. Presentarem també la situació general $(K, \infty, \mathbb{A})$ i algun dels detalls que comporta $cl(K) \neq 1$ en algunes situacions. El cas general el podeu consultar a [8].

$\mathfrak{n}$ denota un ideal de $\mathbb{A}$,
$X_0(\mathfrak{n})$ la corba modular de Drinfeld associada al grup $\Gamma_0(\mathfrak{n})$, (veieu final de l'exposició 8 [18]).
$J_0(\mathfrak{n})$ denota la jacobiana associada a la corba $X_0(\mathfrak{n})$.

10.2 La conjectura

Sigui en aquest capítol $(K, \infty, \mathbb{A})$ una tripleta general. Donat $\mathfrak{n}$ un ideal no zero de A arbitrari, recordem que $J_0(\mathfrak{n})$ està definida sobre K i que la varietat abeliana $J_0(\mathfrak{n})/K_\infty$ té reducció totalment split multiplicativa, fet que es dedueix de la seva descripció analítica [18]. Per tant cadascun dels seus factors K_∞-isògens té reducció split multiplicativa a ∞. Així, per formular la conjectura de Shimura-Taniyama-Weil per a cossos de funcions ens hem de restringir a les

corbes el·líptiques E definides sobre K amb reducció multiplicativa split en el primer fixat ∞ i per tant $cond(E) = \infty\mathfrak{n}$ amb $(\mathfrak{n}, \infty) = 1$. Observem ([Tate] Theorem 5.3 [14]) que E com a corba sobre K_∞ és una corba de Tate.

10.2.1 Teorema. (S-T-W per a cossos de funcions) *Sigui E/K una corba el·líptica sobre K amb reducció totalment multiplicativa a ∞ i $cond(E) = \infty\mathfrak{n}$. Llavors existeix un morfisme dominant K-definit de corbes algebraiques,*

$$\pi : X_0(\mathfrak{n})_{/K} \to E_{/K}.$$

El morfisme π s'anomena la parametrització de Weil.

10.2.2 Observació.

1. La restricció a que la reducció a ∞ sigui multiplicativa split per trobar parametritzacions de Weil de corbes el·líptiques E sobre K no és molt forta. Si $j(E)$ no és constant, sempre podem triar una plaça de K, que la elegim com la plaça ∞, amb $v_\infty(j(E)) < 0$. Llavors hi ha una extensió finita i separable K' de K i una extensió ∞' de ∞ en K' on $E/K'_{\infty'}$ té reducció multiplicativa split. Les corbes el·líptiques E amb $j(E)$ constant, és a dir $j(E) \in \mathbb{F}_q$, són classificades directament.

2. La conjectura de Shimura-Taniyama-Weil 10.1.1, ens dóna una relació entre factors 1 dimensionals de la jacobiana de corbes modulars, amb certes formes cuspidals; sobre K obtindrem aquestes bijecció entre factors 1 dimensionals de la jacobiana per corbes modulars de Drinfeld i certes representacions cuspidals. Observem que les formes modulars de Drinfeld ([11]) viuen en característica p i això no ens permet distingir diferents corbes el·liptiques; no així les representacions cuspidals (que es troben a característica zero). Veieu l'exemple 2 §5 (observació 10.5.4), on fem explícit que les formes cuspidals no ens diferencien corbes el·líptiques sobre K no K-isògenes.

La conjectura ens afirma la existència de parametritzacions de Weil. Suposant la existència ens podem preguntar sobre la de menor grau, que correspondrà al factor isògen de la jacobiana de la corba modular de Drinfeld d'aquesta corba el·líptica. Aquesta parametrització s'anomenarà, seguint la teoria clàssica, parametrització forta de Weil.

Anem a centrar-nos d'ara en endavant al cas que

$$(\mathbb{A}, \infty, K) = (\mathbb{F}_q[T], 1/T, \mathbb{F}_q(T)).$$

Aquesta exposició s'estructura bàsicament en dues parts. En la primera,§3, es fa un overview de la prova de l'anterior teorema: la prova es basa en el fet bàsic que tenim equació funcional per la funció L per aquestes corbes el·liptiques, i utilitzant el treball de Jaquet-Langlands junt amb la relació entre formes cuspidals i jacobianes de corbes modulars de Drinfeld (Drinfeld) s'obté el resultat. La segona part, §4 i §5, tracta de la construcció de parametritzacions fortes de Weil, i explicitar-ne alguns exemples concrets, veient com en l'arbre de Bruhat-Tits hi ha tota la informació de parametritzacions fortes de Weil en el cas de cossos de funcions.

10.3 Una pinzellada de la prova del teorema 10.2.1

Sigui E/K corba el·líptica sobre cos K i imposem que el j-invariant no està a $\mathbb{F}_q$ ($\mathbb{F}_q \subset K$) i que $cond(E) = \infty\mathfrak{n}$. Considerant les realitzacions étales $H^1(E \times_K \overline{K}, \mathbb{Q}_l)$ amb $l \neq p$ primer, obtenim associada una $Gal(K^{sep}/K)$-representació que anomenem π_E que forma un sistema compatible de representacions l-àdiques (veieu §8[2] per la definició, exemple 9.6 [2]). Considerem les representacions que s'obtenen twistant la representació anterior mitjançant χ, caràcters unitaris de I_K/K^*. Sigui $L_E(\chi, s)$ la funció L associada. Llavors tenim els següents resultats de Grothendieck-Deligne (§9[2]):

1. Les funcions $L_E(\chi, s)$ són funcions polinomials en q^{-s} a coeficients a $\mathbb{Q}$;

2. satisfan, via una definició adequada de factors epsilon (veieu [2]), l'equació funcional,

$$L_E(\chi, s) = \epsilon_E(\chi, s) L_E(\overline{\chi}, 2 - s).$$

De 2, la correspondència de Jacquet-Langlands, thm. 11.3 [5], ens afirma l'existència d'una única representació automorfa cuspidal $\rho_E =$

$\rho(\pi_E)$, V_{ρ_E} de

$$\mathfrak{K}(\mathfrak{n}) := \{\begin{pmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{pmatrix} | \underline{c} \equiv 0 (mod \mathfrak{n})\}$$

on $\underline{\alpha}$ denota elements en l'anell de les àdeles de K.

Anem a precisar més aquesta representació cuspidal. Com que E/K_∞ és una corba de Tate ([Tate] thm. 5.3[14]), aleshores $\pi_E|_{Gal(K_\infty^{sep}/K_\infty)}$ és la representació especial de Galois sp o sp_l de $GL_2(K_\infty)$ que es defineix de la manera següent: Si $l \neq p = car(\mathbb{F}_q)$, definim $E_l = K_\infty^{unr}((\text{arrels } l^r\text{-èssimes de } \pi_\infty)_r)$ on π_∞ és un uniformitzant per K_∞^{unr} i r recorre tots els naturals. Llavors la representació especial es defineix per la composició següent,

$$sp : Gal(K_\infty^{sep}/K) \to Gal(E_l/K_\infty) \cong$$

$$\cong Gal(K_\infty^{unr}/K_\infty) \ltimes Gal(E_l/K_\infty^{unr}) \cong \hat{\mathbb{Z}} \ltimes \mathbb{Z}_l \xrightarrow{i} GL(2, \mathbb{Q}_l)$$

definida per $i(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & q_\infty^{-1} \end{pmatrix}$ i $i(0,1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

La representació automorfa cuspidal s'escriu $V_{\rho_E} = \otimes_v V_{\rho_E,v}$ on en la plaça ∞ és $(\rho_\infty, V_{\rho_{E,\infty}}) \cong (\rho_{sp}, V_{sp})$.

Utilitzant altre cop la correspondència de Jacquet-Langlands, obtenim que a la representació automorfa cuspidal li associem una forma automorfa cuspidal nova $\varphi_E \in V_{\rho_E}$ en un espai concret de formes automorfes cuspidals que en el nostre cas correspon a $W_{sp}(\mathcal{K}, \mathbb{C})$ (consulteu si voleu III [15] per la definició explícita de forma cuspidal), l'espai ($\mathbb{C}$-espai vectorial) format per les funcions

$$Y(\mathcal{K}) := GL(2,K) \setminus GL(2,\mathfrak{U})/\mathcal{K}Z(K_\infty) \to \mathbb{C}$$

sota certes hipòtesis, on $\mathfrak{U}$ denota les ádeles de K, i $\mathcal{K}$ és $\mathcal{K}_{fin,0}(\mathfrak{n}) \times \mathcal{I}_\infty$ amb

$$\mathcal{K}_{fin,0}(\mathfrak{n}) = \{\begin{pmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{pmatrix} | \underline{a}, \underline{b}, \underline{c}, \underline{d} \in \mathfrak{U}_{fin}, \underline{c} \equiv 0 \ mod \ \mathfrak{n}\}$$

(aquí fin denota tots els primers de K a excepció del primer fixat de K que anomenem ∞) i

$$\mathcal{I}_\infty = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in K_\infty, c \equiv 0 \ mod \infty\}$$

(el grup d'Iwahori), i el subindex sp, indica que la formes automorfes cuspidals transformen com sp a $GL(2, K_\infty)$.

La teoria de Jacquet-Langlands [2] afirma que la forma cuspidal φ_E és vector propi pels operadors de Hecke T_v (veieu §4.9[8] o [15] per la definició i propietats dels operadors de Hecke en formes cuspidals), amb $v \nmid \mathfrak{n}\infty$ i té valors propis en la nostra situació $\lambda_v = q_v + 1 - \#E(k(v)) \in \mathbb{Q}$, amb $q_v = \#k(v)$ on $k(v)$ denota el cos residual de K en la plaça v.

Observeu que $W_{sp}(\mathcal{K}, \mathbb{C})$ és un $\mathbb{C}$-espai vectorial de dimensió finita, $Y(\mathcal{K})$ és un conjunt discret i les formes cuspidals automorfes tenen suport en un subconjunt finit de $Y(\mathcal{K})$ (1.2.3 [10]). La propietat de ser cuspidal dóna una relació lineal finita de valors de $\varphi(\in W_{sp}(\mathcal{K}, \mathbb{C}))$, on els coeficients són volums de doble cosets amb nombres racionals com radis. Això ens permet tenir una estructura $\mathbb{Q}$-racional a $W_{sp}(\mathcal{K}, \mathbb{C})$, que denotarem per $W_{sp}(\mathcal{K}, \mathbb{Q})$, que compleix, per a tot cos F amb car 0,(en particular per a $F = \mathbb{C}$), que

$$W_{sp}(\mathcal{K}, \mathbb{Q}) \otimes_{\mathbb{Q}} F = W_{sp}(\mathcal{K}, F).$$

Hem obtingut una projecció

$$proj : W_{sp}(\mathcal{K}, \mathbb{Q}) \to \mathbb{Q}\varphi_E,$$

ja que podem normalitzar φ_E definida dins la $\mathbb{Q}$-estructura del fet que T_v estan definits sobre $\mathbb{Q}$ amb autovalors racionals.

10.3.1 Questió Com relacionar $\varphi_E \in W_{sp}(\mathcal{K}, \mathbb{Q})$ amb un factor 1-dimensional de la $J_0(\mathfrak{n})$ que sigui K-isògen amb E?

Recordem ([18]) que, donat $\mathcal{K}$, tenim un problema de moduli de Drinfeld de nivell $\mathfrak{n}$ definit sobre K, i tenim la corba $X_0(\mathfrak{n})$ corresponent a $\mathcal{K}_{0,f}$. En aquestes corbes de moduli hi ha uns operadors de Hecke, definits via v-isogènies (per una definció precisa consulteu (7.6) [7]) i que aquests operadors es traslladen a $J_0(\mathfrak{n})$.

El resultat clau per respondre la pregunta 10.3.1 és el següent resultat, anomenat llei de reciprocitat de Drinfeld (Prop.10.3 i Thm.2 [3]).

10.3.2 Teorema. (Drinfeld) *Sigui $l \neq p = carK$. Llavors*

$$J_0(\mathfrak{n}) \otimes \mathbb{Q}(-1) = H^1_{et}(X_0(\mathfrak{n}) \times C, \mathbb{Q}_l) \cong W_{sp}(\mathcal{K}_{0,f} \times \mathcal{I}_\infty, \mathbb{Q}_l) \otimes sp_l$$

canònicament, és a dir, compatible amb els operadors (no-ramificats) de Hecke i amb l'acció de $Gal(\overline{K_\infty}^{sep}/K_\infty)$ (que actua amb el terme de l'esquerra de manera natural del fet que aquest grup galoisà coincideix amb el grup d'automorfismes continus de C/K_∞ i que la corba modular de Drinfeld $X_0(\mathfrak{n})$ està definida sobre K).

Per construcció, φ_E correspon a una forma automorfa nova de pes $\mathfrak{n}$. Per construir la parametrització anem a relacionar la Jacobiana de l'anterior resultat amb el factor 1 dimensional que ens dóna a dins. Així, necessitem un endomorfisme de la Jacobiana on la imatge ens doni E o una corba K-isògena per poder acabar. Nosaltres ja tenim un endomorfisme de W_{sp} donar per *proj*; anem doncs a obtenir-lo venint de la Jacobiana. Per tal de facilitar la demostració i no haver de treballar amb formes cuspidals, introduïm les cocadenes harmòniques.

Sigui $\mathcal{T}$ l'arbre de Bruhat-Tits de $GL_2(K_\infty)$ i $Y(\mathcal{T})$ denota les arestes i $X(\mathcal{T})$ els vèrtexs (consulteu per més detalls de arbre de Bruhat-Tits, [In]).

10.3.3 Definició Denotem per B un grup abelià. Diem que φ és una co-cadena harmònica de B per un arbre de Bruhat-Tits $\mathcal{T}$ si és una aplicació

$$\varphi : Y(\mathcal{T}) \to B$$

complint

1. $\varphi(\overline{e}) = -\varphi(e)$, on $\overline{e}$ es la aresta e però en la direcció oposada,
2. $\sum_{origen(e)=v} \varphi(e) = 0$ per tot $v \in X(\mathcal{T})$. Al conjunt de cocadenes harmòniques el denotarem per

$$\underline{H}(\mathcal{T}, B).$$

Denotem per

$$\underline{H}(\mathcal{T}, B)^\Gamma \tag{10.1}$$

amb $\Gamma \subseteq GL(2, K)$ un subgrup aritmètic, al conjunt de cocadenes harmòniques que a més satisfant:

3. $\varphi(\gamma e) = \varphi(e)\ \forall \gamma \in \Gamma$.

   S'anomenen cuspidals i es denota tot el seu conjunt per

   $$\underline{H}_!(\mathcal{T}, B)^\Gamma$$

   el subconjunt de (10.1), complint que tinguin suport finit *mod* Γ; això vol dir que a l'arbre de Bruhat-Tits de $\mathcal{T}/\Gamma$ s'anul.la en cada semilinea a partir d'un cert lloc (realment després de la primera aresta).

   S'anomenen doble cuspidals i es denota per

   $$\underline{H}_{!!}(\mathcal{T}, B)^\Gamma$$

   si és cuspidal i a més s'anul.la a les puntes (és a dir s'anul.la en cadascuna i en tota aresta de les semilinees de $\mathcal{T}/\Gamma$).

10.3.4 Observació. Els conceptes cuspidal i doble cuspidal coincideixen si B és lliure de torsió, veieu prop.3.10 i)[7].

Treballar en l'arbre de Bruhat-Tits és molt més senzill, i en particular treballar en les co-cadenes harmòniques. El proper resultat ens permet traslladar el nostre estudi que necessitem en formes automorfes a un estudi dins co-cadenes harmòniques.

10.3.5 Teorema. (Drinfeld) *Sigui F un cos de característica 0, llavors,*

$$\underline{H}_!(\mathcal{T}, F)^{\Gamma_0(\mathfrak{n})} \cong W_{sp}(\mathcal{K}_{0,f} \times \mathcal{I}_\infty, F). \tag{10.2}$$

on $\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{A}_K) | c \equiv 0(\mathfrak{n}) \right\}$.

Aquest isomorfisme (10.2) és natural, en el sentit que en les co-cadenes tenim definit uns operadors de Hecke i part nova i que aquest isomorfisme es compatible amb operadors de Hecke i la part nova. Definim en les co-cadenes cuspidals aquests conceptes que ens comporten bé via l'anterior isomorfisme (10.2).

10.3.6 Definició Sigui $\mathfrak{m}$ un ideal de $\mathbb{A}$, pensem $\varphi \in GL(2, K_\infty)$, definim l'operador de Hecke $T_\mathfrak{m}$ via,

$$(T_\mathfrak{m}\varphi)(g) := \sum \varphi(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g),$$

on la suma recorre les tripletes $(a,b,d) \in \mathbb{A}^3$ amb a,d mònics, $(ad) = \mathfrak{m}$, $(a,\mathfrak{n}) = 1$ i $\deg b < \deg d$. Aquests operadors actuen dins les formes cuspidals, commuten entre ells. Els operadors de Hecke $T_\mathfrak{m}$ amb $(\mathfrak{m},\mathfrak{n}) = 1$ s'anomenem no-ramificats.

Per simplificar notació,

$$H(\mathfrak{n}) := \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(\mathfrak{n})}.$$

Tenim en l'arbre de Bruhat-Tits un producte de Peterson, $(,)_\mu$ que es defineix de la forma següent,

10.3.7 Definició Donat un grup aritmètic Γ, és defineix el producte de Peterson per Γ,

$$(,)_\mu : \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma \times \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma \to \mathbb{Z}$$

per

$$(f,g) = \sum_{e \in Y(\Gamma\backslash\mathcal{T})} f(e)g(e)vol_\mu(e),$$

on $vol_\mu(e) := \frac{\#(Z(K)\cap\Gamma)}{2\#(\Gamma_e)}$. Observem que cada aresta geomètrica $\{e,\overline{e}\}$ fa sumar dos cops aquest sumatori el mateix valor (fixem-nos que estem pensant sempre $e,\overline{e}$ son arestes de l'arbre de Bruhat-Tits). Multiplicant $\otimes_\mathbb{Z} F$ obtenim un producte escalar per qualsevol cos de característica zero.

Si $\mathfrak{n}'|\mathfrak{n}$ tenim un morfisme natural per cada divisor mònic a de $\mathfrak{n}/\mathfrak{n}'$,

$$i_{a,\mathfrak{n}'} : H(\mathfrak{n}') \to H(\mathfrak{n})$$

donat per,

$$i_{a,\mathfrak{n}'}(\varphi)(g) := \varphi(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g).$$

10.3.8 Definició La part nova de les formes cuspidals de $H(\mathfrak{n}) \otimes \mathbb{Q}$ és, ho anotarem per $(H(\mathfrak{n}) \otimes \mathbb{Q})^{new}$, el complement ortogonal en $H(\mathfrak{n}) \otimes \mathbb{Q}$ respecte al producte de Peterson de les images de tots els $i_{a,\mathfrak{n}'} \otimes \mathbb{Q}$ on $\mathfrak{n}'$ recorre tots els divisor propis de $\mathfrak{n}$. Denotem per $H(\mathfrak{n})^{new} := H(\mathfrak{n}) \cap (H(\mathfrak{n}) \otimes \mathbb{Q})^{new}$.

Els operadors de Hecke $T_{\mathfrak{m}}$ actuen en $H(\mathfrak{n})^{new}$. Denotem per $\mathfrak{H}(\mathfrak{n})$ la $\mathbb{Z}$-algebra generada pels operadors no-ramificats de Hecke, i $\mathfrak{H}(\mathfrak{n})\otimes\mathbb{Q}$ la $\mathbb{Q}$-àlgebra que és commutativa i semisimple, per tant un producte de cossos totalment reals. Com l'acció dels operadors de Hecke es compatible amb els dos isomorfismes de Drinfeld anteriors (10.3.2,10.3.5), això ens permet explicitar *proj* com un morfisme de la Jacobiana. Efectivament, per això recordeu ([In]):

1. tot endomorfisme de $Jac(X_0(\mathfrak{n}))$ es puja al seu tor associat $T_{\Gamma_0(\mathfrak{n})} := Hom(\overline{\Gamma_0(\mathfrak{n})}, \mathbb{G}_m)$, on $\overline{\Gamma} := \Gamma^{ab}/tor(\Gamma^{ab})$;

2. hi ha una equivalència de categories,

$$\overline{\Gamma} \leftrightarrow T_{\Gamma};$$

3. hi ha una aplicació injectiva natural,

$$j : \overline{\Gamma_0(\mathfrak{n})} \to H(\mathfrak{n})$$

que correspon a la composició de les aplicacions canòniques següents: $\overline{\Gamma} \cong (\Gamma/\Gamma_f)^{ab} =: (\Gamma^*)^{ab}$, ($\Gamma_f$ és el subgrup normal de Γ generat pels elements d'ordre finit); recordant que Γ^* s'identifica canònicament amb el grup fonamental de $\Gamma \setminus \mathcal{T}$, obtenim $(\Gamma^*)^{ab} \cong H_1(\Gamma \setminus \mathcal{T}, \mathbb{Z})$, definim l'aplicació

$$\tilde{} : H_1(\Gamma \setminus \mathcal{T}, \mathbb{Z}) \to \underline{H_!}(\mathcal{T}, \mathbb{Z})^{\Gamma}$$

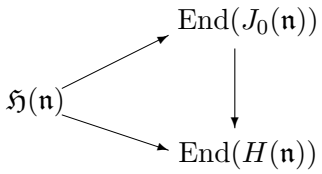
$$(\tilde{\varphi})(e) := \frac{\#(\Gamma_e)}{\#(\Gamma \cap Z(K_\infty))}\varphi(\tilde{e})$$

on e denota les arestes de $\mathcal{T}$ mod Γ (veieu una definició explícita de j en 3.3[8] orientant l'arbre de Bruhat-Tits).

10.3.9 Conjectura *L'aplicació j és bijectiva per tot Γ grup aritmètic de $GL_2(K_\infty)$.*

L'anterior conjectura està provada pel cas concret de $C = \mathbb{P}^1$ en que estem treballant (no ho està per C genèrica).

De les consideracions 1,2 i 3 anteriors tenim el diagrama commutatiu,



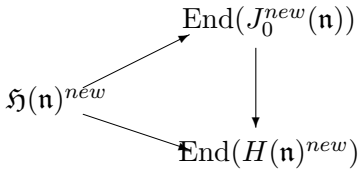
(10.3)

Recordem que $T_\mathfrak{m}$ són morfismes K-racionals de $J_0(\mathfrak{n})$, per tant $\mathfrak{H}(n)$ ens dóna una descomposició llevat de K-isogènia per $J_0(\mathfrak{n})$, és a dir,

$$J_0(\mathfrak{n}) \sim_K \prod A_i$$

amb A_i varietats abelianes definides sobre K.

Observem que $T_\mathfrak{m}$ els podem restringir en la part nova i via l'isomorfismes canònics, teoremes 10.3.2,10.3.5, tenim que la part nova de les co-cadenes cuspidals correspon a la part nova de la Jacobiana (definida de la manera usual). Denotem per $\mathfrak{H}(n)^{new}$ la $\mathbb{Z}$-àlgebra de Hecke $\mathfrak{H}(n)$ que pensem com l'algebra generada pels operadors de Hecke no ramificats, però pensant els operadors actuant en la part nova. Tenim el diagrama



(10.4)

La $\mathbb{Q}$-algebra $\mathfrak{H}(\mathfrak{n})^{new} \otimes \mathbb{Q}$ és commutativa semisimple i per tant un producte de cossos totalment reals, on obtenim que $H^{new}(\mathfrak{n}) \otimes \mathbb{C}$ té una base de vectors propis φ per l'acció de $\mathfrak{H}(\mathfrak{n})^{new}$. Sigui $\lambda(\varphi, \mathfrak{m})$ el valor propi per $T_\mathfrak{m}$. A més, tenim el
principi de multiplicitat fort: donats $\varphi, \varphi' \in H^{new}(\mathfrak{n}) \otimes \mathbb{C}$ amb $\lambda(\varphi, \mathfrak{m}) = \lambda(\varphi', \mathfrak{m})$ per quasi tot $\mathfrak{m}$ llavors $\varphi' = \text{cte}\ \varphi$.

D'aquí, $\mathfrak{H}^{new}(\mathfrak{n})\otimes\mathbb{Q}$ és una $\mathbb{Q}$-algebra semisimple de dimensió $g^{new} := \dim J_0(\mathfrak{n})^{new} = \operatorname{rang}_{\mathbb{Z}} H^{new}(\mathfrak{n})$, i per tant per la classificació dels anells d'endomorfismes per varietats abelianes dóna l'acció de l'àlgebra de Hecke una descomposició completa de la $J_0(\mathfrak{n})^{new}$ via K-isogènea.

Per tant, *proj* poden pensar-lo $proj \in \operatorname{End}(J_0(\mathfrak{n})^{new})\otimes\mathbb{Q}$ donat per φ_E (via l'isomorfisme 10.3.5) amb $\lambda(\varphi_E, \mathfrak{m})$ són enters, per tant corresponent a un factor 1-dimensional en la descomposició de la jacobiana en K, és a dir tenim E' una corba el·líptica definida sobre K, que és un K-factor dins $J_0^{new}(\mathfrak{n})$, i tenim una parametrització de Weil de E' que correspon a la composició de l'aplicació natural de $X_0(\mathfrak{n})$ a la jacobiana i la projecció de la jacobiana a la corba E'.

Per acabar ens falta únicament demostrar que les corbes E' i E, ambdues definides sobre K, son K-isògenes, obtenint així una parametrització de Weil per a E. Com E i E' coincideixen com $Gal(K^{sep}/K)$-submòduls de $H^1_{et}(X_0(\mathfrak{n})\times C, \mathbb{Q}_l)$ concloem.

La prova anterior ens dóna l'anàleg d'equivalencies del teorema 10.1.1 pel cas de cossos de funcions,

10.3.10 Teorema. *Hi ha una bijecció entre,*

1. *conjunt de classes de K-isogènia de corbes el·líptiques definides sobre K amb conductor $\mathfrak{n}\infty$;*
2. *factors 1-dimensionals (mòdul K-isogènies) en la K-descomposició de $J_0^{new}(\mathfrak{n})$ de $Jac(X_0(\mathfrak{n}))$;*
3. *classes (mòdul multiplicació d'escalars no nul) de vectors propis pels operadors de Hecke amb valors racionals en l'espai de formes cuspidals*

$$W_{sp}^{new}(\mathcal{K}_{f,0}(\mathfrak{n})\times\mathcal{I}_\infty, \mathbb{C})$$

o en l'espai de co-cadenes cuspidals $\underline{H}_!^{new}(\mathfrak{n})^{\Gamma_0(\mathfrak{n})}\otimes\mathbb{C}$.

10.4 Vers parametritzacions fortes de Weil

Sigui E una corba el·líptica definida sobre K and $cond(E) = \infty\mathfrak{n}$. Hem construït en l'apartat anterior una corba el·líptica E' definida

sobre K i K-isògena a E, que és un factor de la $Jac(X_0(\mathfrak{n}))$, i a més per construcció aquesta E' és única. Recordeu que anomenem parametrització (dèbil) de Weil per la corba el·lípitica E a un morfisme no trivial K-definit, $\pi : X_0(\mathfrak{n}) \to E$, diem que és forta si via K-morfismes tota parametrització dèbil de Weil per corbes el·líptiques K-isògenes a E factoritza via π. Observem que donada E l'apartat anterior ens prova l'existènica de la parametrització forta de Weil donada per la projecció de la $Jac(X_0(\mathfrak{n}))$ a E' factor K-isògen a E la corba el·liptica inicial, on la parametrització de Weil $X_0(\mathfrak{n}) \to E'$ és forta.

Anem a explicitar la construcció de parametritzacions fortes de Weil.

Estudiem primer sobre C, busquem E' i per tant una xarxa en C^*. De ([In]),

$$1 \to \overline{\Gamma_0(N)} \xrightarrow{\bar{c}} \mathrm{Hom}(\overline{\Gamma_0(\mathfrak{n})}, \mathbb{C}^*) \to J_0(\mathfrak{n})(C) \to 0;$$

i de la identificació $j : \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(N)} \to \overline{\Gamma_0(N)}$, triem $\varphi \in \underline{H}_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})}$, vector propi amb valors propis enters, i a més primitiu, és a dir $\varphi \in j(\overline{\Gamma_0(\mathfrak{n})})$ però $\varphi \notin nj(\overline{\Gamma_0(\mathfrak{n})})$ per $n \in \mathbb{N}_+$. Definim així l'aplicació

$$ev_\varphi : Hom(\overline{\Gamma_0(\mathfrak{n})}, C^*) \to C^*$$
$$f \mapsto f(\varphi).$$

10.4.1 Teorema. (Gekeler-Reversat) *Denotem per*

$$\Lambda := Imag(ev_\varphi) \subset C^*$$

(realment $\subset K_\infty$). Llavors $\exists t \in C^*$, $|t| < 1$ on $\Lambda = t^{\mathbb{Z}}$.

10.4.2 Observació. Quan $\mathbb{A}$ no és $\mathbb{F}_q[T]$, $\Lambda = \mu_d \times t^{\mathbb{Z}}$ on μ_d són les arrels d-èssimes de la unitat en K_∞^* on d és un divisor de $q_\infty - 1$, (9.5.1,2 [8]).

Tenim el següent diagrama commutatiu,

$$\begin{array}{ccccccccc} 1 & \to & \overline{\Gamma_0(\mathfrak{n})} & \xrightarrow{\bar{c}} & \mathrm{Hom}(\overline{\Gamma_0(\mathfrak{n})}, C^*) & \longrightarrow & J_0(\mathfrak{n})(C) & \to & 0 \\ & & \downarrow & & ev_\varphi \downarrow & & pr_\varphi(C) \downarrow & & \\ 1 & \to & \Lambda & \longrightarrow & C^* & \longrightarrow & C^*/\Lambda & \to & 0 \end{array} .$$

Observem:
- C^*/Λ és isomorf als C-punts de la corba el·líptica de Tate $Tate(t)$, per tant C^*/Λ correspon a una corba el·líptica E_φ definida sobre K_∞ amb C-punts C^*/Λ (Tate, thm.5.3 [14]),
- tenim que pr_φ és una aplicació analítica de varietats abelianes definida sobre K_∞, utilitzant GAGA (treballs de Raynaud i Kiehl) obtenim que pr_φ és algebraica.
-cada $T_\mathfrak{m}$ no ramificat dóna un $\mathrm{End}_{K_\infty}(E_\varphi)$ (realment $T_\mathfrak{m}$ estan definits en K en el cas $A = \mathbb{F}_q[T]$)que correspon a multiplicar per $\lambda(\varphi, \mathfrak{m})$ que per les hipòtesis de φ és enter (a $\mathbb{Z}$). Per tant la classe isogènia de E_φ correspon al subespai $\mathbb{Q}\varphi \subseteq W_{sp}(\mathcal{K}_0(\mathfrak{n}) \times \mathcal{I}_\infty, \mathbb{Q})$.
-obtenim del punt anterior que pr_φ pertany a l'algebra de Hecke dels operadors no ramificats que estan definits en el nostre cas sobre K per tant pr_φ està definida sobre K
-$X_0(\mathfrak{n})$ i $J_0(\mathfrak{n})$ estan definides sobre K; considerem l'algebra de Hecke dels operadors no ramificats dins $\mathrm{End}(J_0(\mathfrak{n}))$. Tenim $E_\varphi = J_0(\mathfrak{n})/M$ on M és una varietat abeliana K-racional que correspon a l'ortogonal de pr_φ en l'algebra de Hecke dins $\mathrm{End}(J_0(\mathfrak{n}))$. Per thm.1[Shimura] [13] E_φ està definida sobre K.

10.4.3 Observació. Els tres punts anteriors en la situació $\mathbb{A}$ general, són correctes sobre el cos de classes de Hilbert H de K. Per obtenir la parametrització modular forta de Weil que busquem i E_φ a K en el cas general, necessitem treballar cada element de S en la partició de la Jacobiana, on $\#S = cl(K)$, i recordeu que $J_0(\mathfrak{n})(C) = \prod_{x \in S} J_{\Gamma_x}(C)$.

Fixem ∞ com K-punt racional, obtenim la parametrització forta de Weil π_φ per la composició,

$$X_0(\mathfrak{n}) \to J_0(\mathfrak{n}) \to E_\varphi$$

on la primera aplicació és la inclusió usual amb el punt K-racional triat i la segona correspon a pr_φ.

10.4.4 Observació. Pel cas de corbes modulars clàssiques $X_0(N)$ sobre $\mathbb{Q}$, per determinar la classe isogènia de E_φ és suficient donar la forma cuspidal i per la parametrització forta de Weil, via la conjectura de la constant de Manin, la forma modular ens la determina. Pel cas de cossos de funcions no serà suficient com ho veurem en un exemple, però si que donada una parametrització modular poder

associar-hi una forma modular. Anem a associar-li. Denotem per u_φ la funció theta associada a $\varphi \in \overline{\Gamma_0(\mathfrak{n})}([\mathrm{In}])$, tenim el següent diagrama commutatiu,

$$\begin{array}{ccccc} \Omega & \overset{u_\varphi}{\to} & C^* & \to & C^*/\Lambda \\ \downarrow & & & & \| \\ \Gamma \backslash \Omega & & & & E_\varphi(C) \\ \downarrow & & & & \| \\ Y_0(\mathfrak{n})(C) & \to & X_0(\mathfrak{n})(C) & \overset{\pi_\varphi}{\to} & E_\varphi(C) \end{array}$$

C^* denotem amb la coordenada w, la diferencial associada a E_φ és $\frac{dw}{w}$, tenim llavors

$$\pi_\varphi^*(\frac{dw}{w}) = \frac{u'_\varphi(z)}{u_\varphi(z)}dz$$

on obtenim $f(z) := \frac{u'_\varphi(z)}{u_\varphi(z)}$ dóna una forma cuspidal en $M^2_{2,1}(\Gamma_0(\mathfrak{n}))$ (veieu [11]).

10.5 Alguns exemples de parametritzacions de Weil.

Tenim el següent diagrama commutatiu (6.5 [8]),

(10.5)

$$\begin{array}{ccccc} & \overline{u} \swarrow & \overline{\Gamma} & \searrow j & \\ \Theta_h(\Gamma)/C^* & \underset{\cong}{\overset{\overline{r}}{\longrightarrow}} & & & \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma \\ \downarrow \theta & & & & \downarrow red \\ M^2_{2,1}(\Gamma,\mathbb{F}_p) & & \overset{residu}{\underset{\cong}{\longrightarrow}} & & \underline{H}_{!!}(\mathcal{T},\mathbb{F}_p)^\Gamma \end{array}$$

on j definida anteriorment, red denota reducció de coeficients modul p, $residu(f)$ li associem la forma diferencial holomorfa ω (veieu [11]), triem $e \in Y(\mathcal{T})$, es tria un disc convenient en geometria rígida (veieu §1.8 [8]), i $residu(f)(e)$ és el residu del desenvolupant de la forma en aquest disc que correspon a la variable z de l'aplicació edifici amb $\lambda(z) = origen(e)$(veieu tot seguit); $\overline{u}(\varphi) = u_\varphi$ és l'aplicació natural

que a cada forma cuspidal li associem la funció theta; $\theta(u_\varphi) = \frac{u'_\varphi}{u_\varphi}$. L'aplicació $\overline{r}$ es defineix de la manera següent, sigui $\lambda : \Omega \to \mathcal{T}(\mathbb{R})$ l'aplicació edifici, definim $r(u_\varphi)(e) := log_{q_\infty}|\frac{f(w)}{f(z)}|$ on $\lambda(z) = origen(e)$ i $\lambda(w) = final(e)$, definim $\overline{r}$ el pas mòdul C^*.

Observeu que tenim un producte escalar de Petersson, aquest es pot traslladar a $\underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ (fent el càlcul més simple) de la manera següent: siguin $\alpha, \beta \in \underline{H}_!(\mathcal{T},\mathbb{Z})^\Gamma$ llavors

$$(\alpha,\beta) = \sum_{e \in Y(\Gamma\backslash\mathcal{T})} \alpha(e)\beta(e)vol_\mu(e)$$

on $vol_\mu(e) = \frac{1}{2\#\tilde{\Gamma}_e}$, (aquest 2 apareix del fet que $e, \overline{e} \in Y(\Gamma\backslash\mathcal{T})$, estem pensant que no hi ha orientació). Saber-ne el valor ens permetrà calcular grau de π_φ;

10.5.1 Proposició. (Gekeler) *Sigui $\varphi \in \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(\mathfrak{n})}$ com en §4 primitiu.*

1. *Sigui $\mathbf{m}(\varphi) := min\{(\varphi,\alpha) > 0 | \alpha \in \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(\mathfrak{n})}\}$. Llavors*

$$\mathbf{m}(\varphi) = -v_\infty(j(E_\varphi)),$$

   és a dir la valoració a ∞ del j-invariant de la corba el·liptica de la parametrització modular forta de Weil.

2. *Denotem $\mathbf{r}(\varphi) := (\varphi,\varphi)/m(\varphi)$. Llavors $\mathbf{r}(\varphi) \in \mathbb{N}$ i $\mathbf{r}(\varphi) = deg\pi_\varphi$, és a dir el grau de la parametrització forta de Weil.*

Anem a donar dos exemples de buscar les equacions de los corbes el·liptiques que donen totes les parametritzacions modulars d'una corba modular i el grau de la parametrització.

10.5.2 Exemple. Cas $X_0(T^2(T-1))$ en $\mathbb{A} = \mathbb{F}_2[T]$.
L'arbre de Bruhat-Tits $\Gamma \setminus \mathcal{T}$ està representat a 10.1.

Observem que

$$\overline{\Gamma_0(T^2(T-1))} \cong \underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(T^2(T-1))} \cong H_1(\Gamma_0(T^2(T-1)) \setminus \mathcal{T},\mathbb{Z}).$$

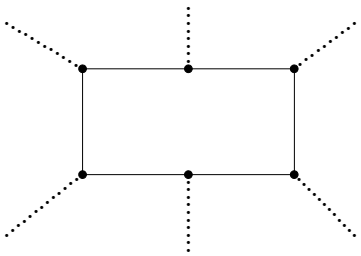


Figura 10.1: Arbre $\Gamma \setminus \mathcal{T}$.

Sigui φ el generador de $\underline{H}_!(\mathcal{T},\mathbb{Z})^{\Gamma_0(T^2(T-1))}$. Recordem que φ s'anul.la en les semi-liníes (prop.3.1.4[8]) i que $\sum_{terminal(aresta\ e)=v,en\ \Gamma\setminus\mathcal{T}}[\Gamma_v : \Gamma_e]\varphi(e)=0$, i $\sum[\Gamma_e:\Gamma_v]=q_\infty+1=3$. Com tenim sempre tres arestes que van a cada punt $[\Gamma_e:\Gamma_v]=1$, tenim $\varphi(e_i)=-\varphi(\tilde{e_{i+1}})$ i recordant $\varphi(e_i)=-\varphi(\tilde{e_i})$, tenim ($\varphi$ és un generador)

$$(\varphi,\varphi)=\sum_{i=1}^{6}(\varphi(e_i)^2 vol_\mu(e_i)+\varphi(\tilde{e_i})^2 vol_\mu(\tilde{e_i}))=$$

$$\sum_{i=1}^{6}(1^2\frac{1}{2}+(-1)^2\frac{1}{2})=6.$$

D'aquí obtenim $\mathbf{m}(\varphi)=6$ i $\mathbf{r}(\varphi)=1$, (on el valor de $\mathbf{m}(\varphi)$ era evident que de l'arbre de Bruhat-Tits). Sabem que $\mathbf{m}(\varphi)=-v_\infty(E_\varphi)$ i tenim un isomorfisme

$$X_0(T^2(T-1))=E_\varphi\to Tate(t)$$

sobre K_∞ on $v_\infty(t)=\mathbf{m}(\varphi)$. Anem però a descriure explícitament E_φ.

Considerem $E: Y^2+TXY+TY=X^3$ corba el·líptica definida sobre $\mathbb{F}_2(T)$. Un càlcul prova $cond(E)=T^2(T-1)\infty$, per tant té una parametrització de Weil, on obtenim per §2 que és K-isògena amb E_φ. Sigui $\eta: E_\varphi\to E$ aquesta parametrització. Observem que $j(E)=T^8/(T-1)^2$ per tant $E_\varphi\cong Tate(t)$ i $E\cong Tate(t')$ sobre K_∞ amb $v_\infty(t)=v_\infty(t')$. Recordem llavors si $Tate(t)$ és isògena a $Tate(t')$ sobre K_∞ amb $v_\infty(t)=v_\infty(t')$ llavors és isomorfisme. Aplicant-ho a

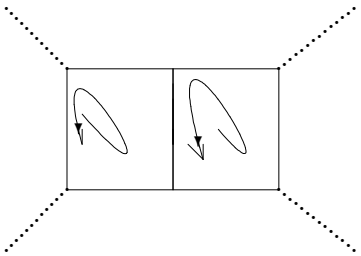


Figura 10.2: Exemple 2.

η obtenim que sobre K_∞ és isomorfisme, per tant obtenim que η és isomorfisme sobre K, d'on

$$X_0(T^2(T-1)) \cong_{/K} (Y^2 + TXY + TY = X^3).$$

10.5.3 Exemple. Cas $X_0(T(T^2+T+1))$ en $\mathbb{A} = \mathbb{F}_2[T]$. Denotem per $\Gamma = \Gamma_0(T(T^2+T+1))$. L'arbre de Bruhat-Tits està representat a 10.2.

Aquí tenim $H_1(\Gamma \setminus \mathcal{T}, \mathbb{Z}) = \underline{H}_!(\mathcal{T}, \mathbb{Z})^\Gamma = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$ on triem l'orientació de γ_1, γ_2 indicada en l'arbre de Bruhat-Tits. Es pot provar que una base de vectors propis pels operadors de Hecke a coeficients racionals són,

$$\varphi_1 = \gamma_1 + \gamma_2,\ \varphi_2 = -\gamma_1 + \gamma_2.$$

Amb consideracions semblants a l'exemple anterior s'obté,

$$(\varphi_1, \varphi_1) = \sum_{i=1}^{7} \frac{1}{2}((\gamma_1+\gamma_2)(e_i)^2 + (\gamma_1+\gamma_2)(\tilde{e_i})^2) =$$

$$(\sum_{1}^{6} 1) + \frac{1}{2}((\gamma_1+\gamma_2)(e_7)^2 + (\gamma_1+\gamma_2)(\tilde{e_7})^2) = 6 + 0$$

per la orientació triada de γ_1 i γ_2 que un pren positiu i l'altre negatiu, semblantment

$$(\varphi_2, \varphi_2) = 6 + \frac{1}{2}((\gamma_1+\gamma_2)(e_7)^2 + (\gamma_1+\gamma_2)(\tilde{e_7})^2) = 10.$$

Per calcular els valors minimals pel producte de Peterson s'obté,

$$(\varphi_1,\gamma_1)=\frac{1}{2}(2(1^2+1^2+1^2+0\times 1+0^2+0^2+0^2))=3,$$

$$(\varphi_2,\gamma_2)=\frac{1}{2}(2(0+0+0+2\times 1+1^2+1^2+1^2))=5,$$

d'aquí obtenim que els graus de les parametritzacions $\mathbf{r}(\varphi_1)=6/3=2=10/5=\mathbf{r}(\varphi_2)$ obtenim que $X_0(T(Y^2+T+1))$ és una corba modular de Drinfeld biel·líptica. Tenim

$$Jac(X_0(T(T^2+T+1)))\sim_{K-isog} E_1\times E_2$$

on E_i són corbes el·líptiques definides sobre K on sobre K_∞, $E_i\cong Tate(t_i)$ amb $v_\infty(t_i)=\begin{cases}3, & i=1\\ 5, & i=2\end{cases}$
Amb arguments semblants al exemple anterior obtenim

$$E_1=(Y^2+(T+1)XY+Y=X^3+T(T^2+T+1))$$

amb $j(E_1)=(T+1)^{12}/(T(T^2+T+1))^3$, i

$$E_2=(Y^2+(T+1)XY+Y=X^3+X^2+T+1)$$

amb $j(E_2)=(T+1)^{12}/T^5(T^2+T+1)$.

Notem que en corbes modulars de Drinfeld hi tenim també involucions Atkin-Lehner, definides anàlogament al cas clàssic, denotades per $w_{\mathfrak{a}}$ amb $\mathfrak{a}$ un ideal de K dividint $\mathfrak{n}$ i coprimer amb $\mathfrak{n}/\mathfrak{a}$. En aquest exemple es pot provar,

$$E_1=X_0(T(T^2+T+1))/w_{(T)}$$

$$E_2=X_0(T(T^2+T+1))/w_{(T^2+T+1)},$$

on tenim una corba biel·líptica amb involucions biel·líptiques donades per involucions del tipus Atkin-Lehner.

10.5.4 Observació. El cas clàssic de corbes modulars, les formes modulars ens donen la decomposició en factors K-isògens de la Jacobiana. En el cas de mòduls de Drinfeld necessitem formes automorfes, no es suficient l'estudi de formes modulars en $M^2_{2,1}(\Gamma,\mathbb{F}_p)$ (mireu el diagrama (10.5)). En el nostre exemple ($\mathbb{F}_p=\mathbb{F}_2$) tenim que $\varphi_1\equiv\varphi_2(mod\ 2)$. Això implica $u'_{\varphi_1}/u_{\varphi_1}=u'_{\varphi_2}/u_{\varphi_2}$, com formes modulars són la mateixa però defineixen diferent factors no K-isògens en la jacobiana de la corba modular de Drinfeld.

10.6 Algunes Taules

Centrem-nos en el cas $\mathbb{F}_q(T)$. Considerem $\mathfrak{n}$ com abans amb el grup que correspon a $X_0(\mathfrak{n})$, i anem a intentar trobar quantes parametritzacions fortes hi ha per nivell $\mathfrak{n}$, amb $\mathfrak{n}$ petit, és a dir en restringirem amb $deg(\mathfrak{n}) \leq 3$. Ens restringim com sempre al cas $(\mathbb{F}_q[T], \infty = 1/T, \mathbb{F}_q(T))$. Consulteu per les proves i com Gekeler [6]. Anem a entendre primer l'espai de formes cuspidals.

10.6.1 Lema. (Gekeler, prop.2.1 and §3.1 [6]) *Si* $deg(\mathfrak{n}) \leq 2$ *no hi ha cap forma automorfa cuspidal amb conductor* $\mathfrak{n}\infty$. *Per cas* $deg(\mathfrak{n}) = 3$ *es segueix de la taula següent:*

tipus	$\dim W_{sp}$
$\mathfrak{q}_1\mathfrak{r}_1\mathfrak{s}_1$	*q*
$\mathfrak{q}_1\mathfrak{r}_2$	*q*
$\mathfrak{q}_3$	*q*
$\mathfrak{q}_1\mathfrak{r}_1^2$	*q-1*
$\mathfrak{q}_1^3$	*q-1*

on els subindexs $1, 2$ *o* 3 *denota el grau de l'ideal de* $\mathbb{A}$, *on aquests ideals corresponen a la descomposició en ideals primers de* $\mathfrak{n}$.

Es pot estudiar l'àlgebra de Hecke $\mathfrak{H}(\mathfrak{n}) \otimes \mathbb{Q}$ i tots els factors en $\mathbb{Q}$ ens donaran corbes K definides. La següent taula ens dóna una llista de casos per a q's petits. Per a veure l'algorisme i com es pot fer consulteu [6] (observeu que els dos primers exemples de la taula són precisament els exemples de la §5). En la taula em utilitzat l'abreviatura altre per a significar altres cossos $\neq \mathbb{Q}$. La última columna ens dóna el nombre de corbes el·líptiques amb conductor igual a $\infty\mathfrak{n}$.

$q(\ \mathbb{F}_q(T))$	Polinomi=$\mathfrak{n}$	$\mathfrak{H}(\mathfrak{n})\otimes\mathbb{Q}$	#c.e. amb $cond=\infty\mathfrak{n}$
2	$T(T^2+T+1)$	$\mathbb{Q}\times\mathbb{Q}$	2
2	T^3+T+1	$\mathbb{Q}(\sqrt{2})$	0
2	$T^2(T-1)$	$\mathbb{Q}$	1
2	T^3	$\mathbb{Q}$	1
3	$T(T^2-1)$	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}$	3
3	$T(T^2+T+2)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{17})$	1
3	$T(T^2-2)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{5})$	1
3	T^3+T^2+2	$\mathbb{Q}(X^3+3X^2-X-4)$	0
3	T^3-T+1	$\mathbb{Q}(X^3+X^2-4X+1)$	0
3	$T^2(T-1)$	$\mathbb{Q}\times\mathbb{Q}$	2
3	T^3	$\mathbb{Q}\times\mathbb{Q}$	2
4	$T(T^2+T+v)$	$\mathbb{Q}(\sqrt{6})\times\mathbb{Q}(\sqrt{2})$	0
4	T^3+T+1	$\mathbb{Q}(\sqrt{2})\times\mathbb{Q}(\sqrt{6})$	0
4	T^3-v	$\mathbb{Q}\times\mathbb{Q}(X^3+X^2-9X+1)$	1
4	$T^2(T-1)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{5})$	1
4	T^3	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}$	3
5	$T(T-1)(T-2)$	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}(\sqrt{3})$	3
5	$T(T^2+T+1)$	$\mathbb{Q}(\sqrt{7}\times\mathbb{Q}(X^3-4X+2))$	0
5	$T(T^2+T+2)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{37})\times\mathbb{Q}(\sqrt{17})$	1
5	$T(T^2-2)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{13})\times\mathbb{Q}(\sqrt{21})$	1
5	T^3+T^2+1	cos de grau 5	0
5	T^3+2T+1	cos de grau 5	0
5	$T^2(T-1)$	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}$	4
7	$T(T-1)(T-2)$	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times$altr.	3
7	$T(T-1)(T-3)$	$\mathbb{Q}\times$altr.	1
7	$T(T^2+T+3)$	$\mathbb{Q}\times$altr.	1
7	$T(T^2+T+4)$	altr.	0
7	$T(T^2+T+6)$	altr.	0
7	$T(T^2-3)$	$\mathbb{Q}\times$altr.	1
7	T^3+T+1	altr.	0
7	T^3+3T+2	altr.	0
7	T^3-2	$\mathbb{Q}\times$altr.	1
7	T^3-4	$\mathbb{Q}\times$altr.	1
7	$T^2(T-1)$	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times$altr.	4
8	$T(T^2+T+1)$	$\mathbb{Q}\times\mathbb{Q}\times$altr.	2
..	...	...	...
9	$T(T^2-1)$	$\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times$altr.	3
9	$T(T-1)(T-v)$	$\mathbb{Q}\times$altr.	1
	.....	.....	...

Bibliografia

[1] *C.Breuil,B.Conrad,F.Diamond,R.Taylor*:On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.

[2] *P. Deligne*: Les constantes des équations fonctionnelles des fonctions L, in Modular Functions of One Variable II, LNM 349, pp.501-597 (1972).

[3] *V.G. Drinfeld*: Elliptic Modules. Math.Sbornik 94, 594-627(1974); English Transl.:Math. USSR-Sbornik 23, 561-592 (1976).

[4] *C. Infante*: Uniformización de curvas de Mumford y Jacobianas, capítol 7 de [16].

[5] *H.Jacquet, R.P.Langlands*:Automorphic forms on GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970. vii+548 pp

[6] *E.U. Gekeler*: Automorphe Formen über $\mathbb{F}_q(T)$ mit kleinem Führer. Abh.Math.Sem.Univ.Hamburg 55, 111-146 (1985).

[7] *E.-U. Gekeler* : Jacquet-Langlands theory over K and relations with elliptic curves. Lecture 12, 224-257 in [9].

[8] *E.-U.Gekeler, M. Reversat*:Jacobians of Drinfeld modular curves. J. Reine Angew. Math. 476 (1996), 27–93.

[9] *Gekeler,van der Put,Reversat,Van Geel ed.*: Drinfeld modules, modular schemes and applications. Proceedings of the workshop held in Alden-Biesen, September 9–14, 1996. World Scientific Publishing Co., Inc., River Edge, NJ, 1997. xiv+361 pp.

[10] *G. Harder*:Chevalley groups over function fields and automorphic forms. Ann. Math. 100, 249-306 (1974).

[11] *E.Nart*: en [16].

[12] *K.A. Ribet*:On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. Invent. Math. 100 (1990), no. 2, 431–476.

[13] *G.Shimura*:On the factors of the Jacobian variety of a modular function field. J.Math.Soc.Japan 25, 523-544 (1973).

[14] *J.H. Silverman*: Advanced Topics in the arithmetic of elliptic curves. GTM 151, Springer (1994).

[15] STNB 1996-97, *P.Bayer i al.*: Representacions automorfes de $GL(2)$. Notes del Seminari, UB-UAB-UPC, Barcelona (1997).

[16] STNB 2001-2002, *F. Bars,E. Nart,X. Xarles i al.*: Mduls de Drinfeld. Notes del Seminari Teoria de Nombres UB-UAB-UPC, Barcelona (2002).

[17] *A. Wiles*:Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) 141 (1995), no. 3, 443–551.

[18] *X. Xarles*: Corbes modulars de Drinfeld, capítol 8 de [16].

F. Bars
Departament de Matemàtiques
Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
francesc@mat.uab.es