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 $n * z := z^n$. 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

Amb el suport parcial de MCYT, BHA2000-0180.

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 $\mathbb{C}/\mathcal{O} \cong E(\mathbb{C})$, 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 [Sil2].

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 Lemma. *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 Lemma. *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
$$\mathrm{disc}(R) \backslash \mathrm{disc}(A[\lambda_a]) \backslash \mathrm{Norm}(\phi'_a(\lambda_a))$$
ja que $\phi_a(\lambda_a) = 0$. Ara, $\phi'_a(x) = a$ i per tant b no divideix $\mathrm{disc}(R)$.

□

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