NOTES DEL SEMINARI DE

teoria de nombres

ub·uab·upc

14è ANY

VARIETATS ABELIANES AMB MULTIPLICACIÓ COMPLEXA

Collbató 2000

6

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

Comitè editorial
P. Bayer E. Nart J. Quer

VARIETATS ABELIANES AMB MULTIPLICACIÓ COMPLEXA

Edició a cura de

J. Guàrdia J.C. Lario

Amb contribucions de

A. Arenas P. Bayer G. Cardona L. Dieulefait

J. Fernández V. Rotger A. Travesa

J. Guàrdia
Facultat de Matemàtiques,
Universitat de Barcelona,
Gran Via de les Corts Catalanes, 585
08007 Barcelona

J. C. Lario
Facultat de Matemàtiques i Estadística,
Universitat de Politécnica de Catalunya
C/ Pau Gargallo, 5
08028 Barcelona

Comitè editorial

P. Bayer
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de
les Corts Catalanes, 585
08007 Barcelona
Espanya

E. Nart
Facultat de Ciències
Universitat Autònoma de
Barcelona
Dep. de Matemàtiques
08193 Bellaterra
Espanya

J. Quer
Facultat de Matemàtiques
i Estadística
Universitat Politècnica de Catalunya
Pau Gargallo, 5
08028 Barcelona
Espanya

Barcelona, 2000

Amb suport parcial de DGES PB 96-0166 i PB96-0970-C02

ISBN: 84-923250-5-4

Índex

1 El problema 12 de Hilbert **3**

1.1 Teoria local de cossos de classes 5

1.1.1 La llei local de reciprocitat 6

1.1.2 El símbol de Hilbert 7

1.2 Teoria global de cossos de classes 8

1.3 Funcions L de Hecke 14

1.3.1 Caràcters de Hecke 14

1.3.2 Equació funcional de les sèries L de Hecke 16

1.3.3 Valors especials 18

1.4 Sèries L d'Artin 18

1.4.1 Conductor d'Artin d'un caràcter 19

1.5 Reformulació de la teoria global de cossos de classes 20

1.5.1 Equació funcional de les sèrie L d'Artin abelianes . . . 21

1.6 El teorema de densitat de Chebotarev 22

1.7 El somni de Noether-Artin-Hasse 24

2 Introducció a les varietats abelianes **27**

2.1 Varietats abelianes i polaritzacions 27

2.1.1 Divisors de Weil i feixos invertibles 28

2.1.2 Feixos invertibles i morfismes en l'espai projectiu . . . 28

2.2 Varietats abelianes sobre $\mathbb{C}$ 29

2.2.1 La primera classe de Chern 30

2.2.2 La matriu de períodes 33

2.3 La varietat abeliana dual 34

2.3.1 El cas dels nombres complexos $k = \mathbb{C}$ 34

2.3.2 Morfisme entre A i $\hat{A}$ definit per un feix invertible . . 35

2.3.3 El grup de Néron-Severi 35

2.4 Anell d'endomorfismes i representacions 37

2.5 Estructura de $\mathrm{End}^0(A)$ 38

2.6 Cossos de mòduli 41

3 Corbes el·líptiques amb CM i teoria de cossos de classes 43
3.1 Ordres i ideals dels cossos quadràtics imaginaris 44
3.2 Corbes el·líptiques i multiplicacions complexes 52
3.3 Els polinomis modulars 59
3.4 Teoria de cossos de classes 64
3.5 Demostració del teorema 68
3.6 Complements 71
3.7 L'equació de les classes 73

4 CM-càlculs el·líptics 83
4.1 Isogènies 85
4.2 Cossos de definició 88
4.3 L'exemple 23 90
4.4 Modularitat 95
4.5 L'exemple 23 (de nou) 99

5 Construcció de varietats abelianes amb CM 105
5.1 Varietats abelianes amb CM 106
5.2 Tors complexos amb CM 109
5.3 El teorema de construcció 111
5.4 Isogènies i grup de classes d'ideals 116
5.5 CM-tipus i teoria de Galois 119

6 Series L de variedades abelianas con CM 123
6.1 Reducción de variedades algebraicas 123
6.2 Descomposición del Frobenius 125
6.3 Series L de variedades abelianas con CM 128
6.3.1 Grumlaut ossencharacteres 128
6.3.2 Funciones Z de variedades abelianas 129
6.4 Una condición necesaria para buena reducción 134

7 Polaritzacions de varietats abelianes amb CM 137
7.1 Recordatori: polaritzacions de tors complexos generals 138
7.2 Polaritzacions de tors complexos de tipus CM 139
7.3 Varietat dual d'una varietat abeliana de tipus CM 140
7.4 Un exemple 142
7.5 CM-tipus polaritzats 146
7.6 CM-tipus polaritzats i isogènies 147
7.7 La família de les varietats abelianes amb CM 148

8 Teoria de cossos de classes i multiplicació complexa 151
8.1 El teorema principal de la multiplicació complexa 152
8.1.1 CM tipus polaritzats i formes hermítiques 152
8.1.2 El CM-símbol d'Artin 153
8.1.3 El "first main theorem" 154
8.1.4 Acotacions al teorema principal 155
8.2 El teorema principal, versió adèlica 156
8.3 Un resultat de Wei 158

9 Formes modulars de Hilbert 161
9.1 El grup modular de Hilbert 162
9.2 Formes modulars de Hilbert 166
9.3 Aplicacions 171

10 Superfícies abelianes amb CM 175
10.1 Models de corbes de gènere 2 175
10.2 Invariants d'Igusa de corbes de gènere 2 176
10.3 Formes binàries sèxtiques, covariants i invariants 177
10.4 Condicions d'isomorfisme 179
10.5 Grup d'automorfismes 180
10.6 El cos de definició 182
10.7 Construcció explícita 182
10.8 Invariants a partir de matrius 184
10.9 Endomorfismes de jacobianes de corbes hiperel·líptiques . . . 186
10.9.1 Correspondències i endomorfismes 186
10.9.2 Correspondències en corbes hiperel·líptiques 187
10.9.3 Exemples 188
10.9.4 Operacions amb correspondències 189

11 Teoria de cossos de classes efectiva (exemples CM) 191
11.1 Un exemple en dimensió 1 191
11.2 Varietats abelianes ciclotòmiques: construcció geomètrica . . 193
11.3 Varietats abelianes ciclotòmiques: construcció algebraica . . . 198
11.3.1 CM-tipus ciclotòmics 198
11.3.2 Polaritzacions 199
11.3.3 Construcció dels tors complexos 201
11.3.4 Determinació del cos de moduli 203
11.4 Corbes de gènere 2 amb CM definides sobre els racionals . . . 206
11.5 Conclusions 209

Presentació

Passejar pels camins que han obert alguns dels matemàtics més importants dels darrers tres segles és una aventura que provoca sensacions d'eufòria i de respecte alhora. En les latituds de la Teoria de la Multiplicació Complexa hi trobem paratges recòndits i raconets quiescents on podem gaudir de panoràmiques matemàtiques d'extraordinària bellesa. Camins i dreceres per a tots els gustos: alguns de ben explorats, d'altres que són rutes verges en espera d'expedicions molt ben equipades i plenes de coratge.

Cent anys després que David Hilbert deixés la seva motxilla plena de queviures i deures per a les generacions futures, el Seminari de Teoria de Nombres de Barcelona (UB-UAB-UPC) ha volgut fer una revisió modesta del Problema 12 de Hilbert.

Què podem dir avui sobre la realització geomètrica de les extensions abelianes d'un cos de nombres fixat? Els orígens del problema es remunten, com sempre, a Gauss. Però també Jacobi, Abel, Eisenstein, Klein,... hi tenen molt a veure. Després dels resultats clàssics de Kronecker, Weber, Deuring, Hasse i altres per al cas racional, als anys 1960's es van conjuntar la valentia de Taniyama, la destresa de Shimura i el *savoir-faire* de André Weil, per assentar les bases de la multiplicació complexa en dimensió superior.

Les notes que segueixen corresponen a les sessions del 14è any del *Seminari de Teoria de Nombres de Barcelona.* La reunió va tenir lloc del 29 de gener al 4 de febrer del 2000 a EADA (Collbató). Els expositors van tenir la gentilesa de redactar els continguts de la seva exposició, fent possible així l'aparició d'aquest nou volum de les *Notes del STNB.*

Volem remarcar que aquest volum és una recopilació de notes sobre la Teoria de la Multiplicació Complexa, sense voluntat de convertir-se en llibre de text i encara menys d'abastar tot el panorama que compren aquesta teoria. És més aviat un petit llibre de ruta per a no iniciats en l'alta muntanya de la CM.

Com sol passar en aquest ofici nostre, a cada frase que escrivíem ens venien al cap més i més preguntes. Algunes respostes deuen ser conegudes pels experts, d'altres segurament no encara. Al cap i a la fi, el Problema 12 de Hilbert només té cent anys i tot un mil·eni nou per endavant. Bona passejada.

Jordi Guàrdia Joan-C. Lario

Barcelona, 28 de desembre de 2000

Capítol 1

El problema 12 de Hilbert

P. Bayer[1]
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

Introducció

L'any 1900, D. Hilbert (1862-1943) presentà a l'*International Congress of Mathematicians*, celebrat a París, una llista de 23 problemes oberts. Els problemes de Hilbert han exercit una notable influència en la recerca matemàtica del segle XX. El Problema 12, titulat *Extension of Kronecker's theorem on abelian fields to any algebraic realm of rationality*, proposa la generalització de l'avui anomenat teorema de Kronecker-Weber a qualsevol cos de nombres.

El teorema de Kronecker-Weber afirma que totes les extensions abelianes de $\mathbb{Q}$ són ciclotòmiques; és a dir, generables per mitjà de valors especials de la funció exponencial. Hilbert [Hil76] observa que, en particular, aquest resultat permet determinar el nombre d'extensions de $\mathbb{Q}$ de grup de Galois un grup abelià donat i de discriminant donat.

Hilbert [Hil76] demana estendre el resultat anterior al cas, immediatament més senzill, en què la base és un cos quadràtic imaginari. Segons Hilbert, les extensions abelianes dels cossos quadràtics imaginaris s'han de poden generar mitjançant els valors especials de les funcions modulars

[1] Amb el suport parcial de la DGES: PB 96–0166.

el·líptiques, obtinguts en avaluar aquestes funcions en els mòduls singulars. Hilbert mostra la seva convicció que la teoria de la multiplicació complexa de H. Weber (1843-1913) permetrà tancar aquest cas.

Hilbert [Hil76] deixa en clar que la resolució del problema 12 requerirà trobar generalitzacions escaients de les funcions modulars el·líptiques:

> *It will be seen that in the problem just sketched the three fundamental branches of mathematics, number theory, algebra and function theory, come into closets touch with one another, and I am certain that the theory of analytical functions of several variables in particular would be notably enriched if one should succeed in finding and discussing those functions which play the part for any algebraic number field corresponding to that of the exponential function in the field of rational numbers and of the elliptic modular functions in the imaginary quadratic number field.*

El problema 12 de Hilbert explicita el «Somni de Joventut» (*Jugendtraum*) de L. Kronecker (1823-1891). Kronecker en fa referència en una carta adreçada a R. Dedekind (1831-1916) el 15 de març de 1880 [Kro68]:

> *Meinen besten Dank für Ihre freundlichen Zeilen vom 12.c.! Ich glaube darin einen willkommenen Anlaß finden zu sollen, Ihnen mitzutheilen, daß ich heute die letzte von vielen Schwierigkeiten besiegt zu haben glaube, die dem Abschluße einer Untersuchung, mit der ich mich in den letzten Monaten wieder eingehender beschäftigt habe, noch entgegenstanden. Es handelt sich um meinen liebsten Jugendtraum, nämlich um den Nachweis, daß die Abel'schen Gleichungen mit Quadratwurzeln rationaler Zahlen durch die Transformations-Gleichungen elliptischer Functionen mit singulären Moduln grade so erschöpft werden, wie die ganzzahligen Abel'schen Gleichungen durch Kreistheilungsgleichungen.*

En el simposi sobre els problemes de Hilbert, celebrat l'any 1976, R. P. Langlands [Lan76] posava de manifest la poca atenció dedicada fins aleshores al problema 12. Feia excepció, deia, el treball de G. Shimura, exposat de manera diàfana per P. Deligne:

> *Whether justly or not, the twelfth problem has received very little attention.* [...] *The bulk of this research is due to Shimura.* [...]

> *It is very likely that Shimura varieties admit a reciprocity law in this sense.* [...] *The work of Shimura has been exposed in a remarkably clear fashion by Deligne, who also added improvements of his own.*

Si bé, en l'aspecte efectiu, no podem dir tampoc que el problema 12 de Hilbert hagi progressat gaire, en el seu vessant teòric, constituït per la teoria de cossos de classes, no ha deixat d'avançar al llarg del segle. Els textos de H. Hasse, H. Hecke, E. Artin, M. Deuring, C. Chevalley, T. Takagi, G. Hochschild, J. Tate, A. Weil, T. Nakayama, J-P. Serre, S. Lang, D. A. Cox i J. Neukirch, entre altres, han fet possible que la teoria de cossos de classes s'estudiï avui amb comoditat.

Tot seguit farem un resum dels principals resultats de la teoria de cossos de classes, en la formulació local-global.

1.1 Teoria local de cossos de classes

En aquesta secció, K denotarà un cos local; és a dir, un cos valorat i complet respecte d'una valoració discreta, v_K, de cos residual finit. Sigui p un nombre primer. Tot cos local és extensió finita d'un cos $\mathbb{Q}_p$ de nombres p-àdics o bé d'un cos $\mathbb{F}_p((t))$ de sèries formals sobre un cos finit de p elements.

L'anell de la valoració de K,

$$\mathcal{O}_K = \{a \in K^* : \ v_K(a) \geq 0\},$$

és un anell de valoració discreta. Denotarem per $\mathfrak{p}$ el seu ideal maximal i per π un generador: $\mathfrak{p} = (\pi)$.

El grup de les unitats de K,

$$U_K = \{a \in K^* : \ v_K(a) = 0\},$$

admet una filtració

$$U_K = U_K^{(0)} \supseteq U_K^{(1)} \supseteq U_K^{(2)} \supseteq \dots$$

en la qual

$$U_K^{(n)} = 1 + \mathfrak{p}^n, \quad \text{per a } n > 0.$$

Donada una extensió finita i de Galois, $L|K$, el seu grup de Galois, $\mathrm{Gal}(L|K)$, admet una filtració

$$\mathrm{Gal}(L|K) = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \dots$$

donada pels grups de ramificació de Hilbert:

$$G_i(L|K) = \{\sigma \in \mathrm{Gal}(L|K) : \ v_L(\sigma(a) - a) \geq i + 1, \ \text{per a tot } a \in \mathcal{O}_L\}.$$

Els subgrups G_{-1}, G_0 són isomorfs als grups de descomposició i d'inèrcia en $\mathfrak{P}$, respectivament, on $\mathfrak{P}$ denota l'ideal maximal de $\mathcal{O}_L$.

Per formular d'una manera elegant els resultats de la teoria local de cossos de classes, convé canviar la numeració inferior dels grups de ramificació per la numeració superior, introduïda per J. Herbrand [Her31].

Considerem les funcions

$$\eta_{L|K}(s) = \int_0^s \frac{dx}{(G_0 : G_x)}, \qquad \psi_{L|K} = \eta_{L|K}^{-1}.$$

Aleshores, els grups $G^i(L|K) := G_{\psi_{L|K}(i)}(L|K)$ proporcionen la filtració

$$\mathrm{Gal}(L|K) = G^{-1}(L|K) \supseteq G^0(L|K) \supseteq G^1(L|K) \supseteq \dots$$

Més endavant necessitarem el resultat següent:

Teorema 1.1.1 (Hasse-Arf). *Donada una extensió finita i abeliana $L|K$ de cossos locals, els salts de la filtració $\{G^i(L|K)\}_{i \geq -1}$ són nombres enters.*

1.1.1 La llei local de reciprocitat

Donada una extensió finita $L|K$, denotem per $N_{L|K}$, $Tr_{L|K}$ la norma i la traça, respectivament.

Enunciem tot seguit el resultat fonamental de la teoria local de cossos de classes:

Teorema 1.1.2 (llei local de reciprocitat). *Sigui $L|K$ una extensió finita i abeliana de cossos locals. Aleshores,*

i) *Existeix un isomorfisme canònic*

$$r_{L|K} : \mathrm{Gal}(L|K) \longrightarrow K^*/N_{L|K}L^*,$$

anomenat de reciprocitat.

ii) *L'isomorfisme invers de $r_{L|K}$*

$$(\ ,L|K) : K^*/N_{L|K}L^* \longrightarrow \mathrm{Gal}(L|K)$$

defineix el símbol local de residus nòrmics.

iii) *L'isomorfisme $r_{L|K}$ transforma la filtració $\{U_K^{(i)}/N_{L|K}U_L^{\psi(i)}\}_{i\geq 0}$, del grup de les unitats, en la filtració del grup d'inèrcia $\{G^i(L|K)\}_{i\geq 0}$, donada pels grups de ramificació proveïts de la numeració superior.*

Corol·lari 1.1.3. *Sigui c l'enter més gran tal que $G_c(L|K) \neq 1$, i sigui $f = \eta_{L|K}(c) + 1$. Aleshores, $U_K^{(f)} \subseteq N_{L|K}L^*$ i f és l'enter més petit amb aquesta propietat. L'ideal*

$$\mathfrak{f}_{L|K} := \mathfrak{p}_K^{(f)}$$

s'anomena el conductor de l'extensió abeliana local $L|K$.

Quan $K = \mathbb{Q}_p$, es té que

$$N\mathbb{Q}_p(\mu_{(p^n)}) = (p) \times U_{\mathbb{Q}_p}^{(n)}.$$

Si $L|\mathbb{Q}_p$ és una extensió finita i abeliana, existeixen enters f i n tals que

$$(p^f) \times U_{\mathbb{Q}_p}^{(n)} \subseteq N_{L|\mathbb{Q}_p}L^* = ((p^f) \times U_{\mathbb{Q}_p}) \cap ((p) \times U_{\mathbb{Q}_p}^{(n)}).$$

Per tant,

$$L \subseteq \mathbb{Q}_p(\mu_{(p^f-1)p^n}),$$

atès que el conductor de l'extensió $\mathbb{Q}_p(\mu_{(p^n)})|\mathbb{Q}_p$ és $(p)^n$.

D'ací en resulta el teorema següent:

Teorema 1.1.4 (Kronecker-Weber).

i) *Tota extensió finita i abeliana $L|\mathbb{Q}_p$ és ciclotòmica.*

ii) *Tota extensió finita i abeliana $L|\mathbb{Q}$ és ciclotòmica.*

1.1.2 El símbol de Hilbert

Sigui n un nombre natural primer amb la característica de K. Suposem ara que el cos K conté les arrels n-èsimes de la unitat. Si $L = K(\sqrt[n]{K^*})$, aleshores $N_{L/K}L^* = K^*$. La teoria de Kummer i l'isomorfisme de reciprocitat proporcionen un aparellament bilineal no degenerat

$$\left(\frac{\cdot}{\mathfrak{p}}\right) : K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mu_n,$$

anomenat símbol de Hilbert.

La proposició que segueix té cura del lligam entre el símbol local de residus nòrmics i el símbol de Hilbert.

Proposició 1.1.5. *Donats $a, b \in K^*$, se satisfà que*

$$(a, K(\sqrt[n]{b})/K)\sqrt[n]{b} = \left(\frac{a,b}{\mathfrak{p}}\right)\sqrt[n]{b}.$$

Quan $K = \mathbb{Q}_p$, podem precisar una mica més.

Proposició 1.1.6. *Sigui $a = up^{v_p(a)} \in \mathbb{Q}_p$, $p \nmid u$.*

i) *Si $\zeta \in \overline{\mathbb{Q}}_p$ és una arrel primitiva m-èsima de la unitat i $p \nmid m$, aleshores*

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^{p^{v_p(a)}}.$$

ii) *Si $\zeta \in \overline{\mathbb{Q}}_p$ és una arrel primitiva p^n-èsima de la unitat, aleshores*

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^{u^{-1}}.$$

1.2 Teoria global de cossos de classes

Sigui K un cos de nombres; és a dir, una extensió finita de $\mathbb{Q}$. Un plaça $\mathfrak{p}$ de K és, per definició, una classe d'equivalència de valoracions de K. Les places definides per valoracions no arquimedianes s'anomenen places finites; estan en correspondència bijectiva amb els ideals primers de K (de l'anell d'enters $\mathcal{O}_K$). Les places definides per valoracions arquimedianes s'anomenen places de l'infinit (o places infinites); es corresponen amb les r_1 immersions reals $K \hookrightarrow \mathbb{R}$ i amb les r_2 parelles d'immersions complexes, no reals, $K \hookrightarrow \mathbb{C}$. És clar que $[K : \mathbb{Q}] = r_1 + 2r_2$.

Per a cada plaça $\mathfrak{p}$ de K i cada enter $n_\mathfrak{p} \geq 0$, on se suposa que $n_\mathfrak{p} \in \{0, 1\}$ si $\mathfrak{p}|\infty$, volem definir subgrups $U_\mathfrak{p}^{(n_\mathfrak{p})}$. Sigui, doncs:

$$U_\mathfrak{p}^{n_\mathfrak{p}} = \begin{cases} 1 + \mathfrak{p}n_\mathfrak{p}, & \text{si } n_\mathfrak{p} > 0, \\ U_{K_\mathfrak{p}}, & \text{si } n_\mathfrak{p} = 0, \mathfrak{p} \nmid \infty\ , \\ \mathbb{R}^*, & \text{si } \mathfrak{p} \text{ és real i } n_\mathfrak{p} = 0, \\ \mathbb{R}_+^*, & \text{si } \mathfrak{p} \text{ és real i } n_\mathfrak{p} = 1, \\ \mathbb{C}^*, & \text{si } \mathfrak{p} \text{ és complex.} \end{cases}$$

Denotem per I_K el grup dels ideals fraccionaris de K, per P_K el subgrup dels ideals fraccionaris principals i per

$$\mathrm{Cl}_K = I_K/P_K$$

el grup de les classes d'ideals. Recordem que aquest darrer és un grup abelià finit.

Teoremes fonamentals de la teoria de cossos de classes, obtinguts prèviament per T. Takagi [Tak90] i completats per E. Artin [Art65], varen ser interpretats en els anys 1940 per C. Chevalley [Che40] per mitjà del llenguatge de les ideles.

Segons A. Weil [Wei80], el nom idele prové d'*élément idéal*, que en alemany dóna *ideales Element* i, a partir d'aquí, Chevalley formà la paraula *idèle*. El nom adele, que és posterior, respon a la versió additiva, *adèle*, del concepte d'idèle .

Donat un cos K de nombres, recordem les definicions del seu anell d'adeles, $\mathbb{A}_K$, del seu grup d'ideles, $\mathbb{I}_K$, i dels seus grups de S-ideles, $\mathbb{I}_K^S$, on S denota un conjunt finit de places de K:

$$\mathbb{A}_K = \{(\alpha_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p} : \ \alpha_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} \text{ q.p.t.}\},$$

$$\mathbb{I}_K = \mathbb{A}_K^* = \{(\alpha_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p}^* : \ \alpha_\mathfrak{p} \in \mathcal{U}_\mathfrak{p} \text{ q.p.t.}\},$$

$$\mathbb{I}_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}, \quad \mathbb{I}_K = \bigcup_S \mathbb{I}_K^S.$$

L'anell $\mathbb{A}_K$ és un anell topològic. El grup $\mathbb{I}_K$ és un grup topològic localment compacte. Notem que $\mathbb{I}_K = \mathbf{GL}(1, \mathbb{A}_K)$. El grup multiplicatiu K^* s'identifica amb un subgrup discret i tancat de $\mathbb{I}_K$, dit de les ideles principals.

El grup topològic quocient

$$\mathbb{C}\mathrm{l}_K := \mathbb{I}_K / K^*$$

és el grup de les classes d'ideles de K. L'aplicació natural que a cada idele li assigna un ideal fraccionari,

$$\mathbb{I}_K \to I_K, \quad \alpha = (\alpha_\mathfrak{p}) \mapsto (\alpha) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})},$$

és un epimorfisme de grups que té per nucli el subgrup $\mathbb{I}_K^{S_\infty}$ de les ideles finites. Considerem $\mathbb{C}\mathrm{l}_K$ com a grup topològic, per la topologia quocient de la topologia del grup d'ideles. Al contrari del grup de classes d'ideals, el grup de classes d'ideles és un grup abelià infinit.

Proposició 1.2.1.

i) *El grup de les classes d'ideals és un quocient del grup de les classes d'ideles:*

$$\mathbb{C}\mathrm{l}_K / (\mathbb{I}_K^{S_\infty} K^* / K^*) \simeq \mathbb{I}_K / \mathbb{I}_K^{S_\infty} K^* \simeq \mathrm{Cl}_K.$$

ii) *Si S és un conjunt de places de K prou gran, aleshores*

$$\mathbb{C}\mathrm{l}_K \simeq \mathbb{I}_K^S K^*/K^*.$$

En la teoria global de cossos de classes, veurem que el grup de les classes d'ideles té un paper semblant al del grup multiplicatiu del cos en la teoria local. Per començar, veurem que $\mathbb{C}\mathrm{l}_K$ admet una xarxa de subgrups anàloga a la filtració del grup de les unitats locals.

Definició 1.2.2. *Sigui $\mathfrak{m} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{n_\mathfrak{p}}$ un ideal enter de K. Considerem el subgrup d'ideles*

$$\mathbb{I}_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U_\mathfrak{p}^{(n_\mathfrak{p})}.$$

Denotem per $I_K^{\mathfrak{m}}$ el grup dels ideals fraccionaris de K primers amb $\mathfrak{m}$. Considerem el subgrup dels ideals fraccionaris principals

$$P_K^{\mathfrak{m}} = \{(a) \in P_K : \ a \equiv 1 \,(\mathrm{mod}\, \mathfrak{m}), \ a \textit{ totalment positiu}\}.$$

El grup quocient

$$\mathrm{Cl}_K(\mathfrak{m}) = \mathrm{I}_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$$

s'anomena el grup radial de les classes d'ideals mòdul $\mathfrak{m}$.

El subgrup de classes d'ideles

$$\mathbb{C}\mathrm{l}_K^{\mathfrak{m}} = \mathbb{I}_K^{\mathfrak{m}} K^*/K^*$$

s'anomena el subgrup de congruència mòdul $\mathfrak{m}$.

El grup quocient

$$\mathbb{C}\mathrm{l}_K(\mathfrak{m}) = \mathbb{C}\mathrm{l}_K/\mathbb{C}\mathrm{l}_K^{\mathfrak{m}}$$

s'anomena el grup radial de les classes d'ideles mòdul $\mathfrak{m}$.

Proposició 1.2.3. *Un subgrup $H \subseteq \mathbb{C}\mathrm{l}_K$ és tancat i d'índex finit si, i només si, existeix un ideal enter $\mathfrak{m}$ tal que $H \supseteq \mathbb{C}\mathrm{l}_K^{\mathfrak{m}}$.*

Proposició 1.2.4. *L'homomorfisme natural $\mathbb{I}_K \to I_K$ indueix un isomorfisme entre el grup radial de classes d'ideles i el grup radial de classes d'ideals d'un mateix mòdul*

$$\mathbb{C}\mathrm{l}_K(\mathfrak{m}) \simeq \mathrm{Cl}_K^{\mathfrak{m}}.$$

Corol·lari 1.2.5. *Si $K = \mathbb{Q}$ i $\mathfrak{m} = (m)$, aleshores*

$$\mathbb{C}\mathrm{l}_\mathbb{Q}(\mathfrak{m}) \simeq \mathrm{Cl}_\mathbb{Q}(\mathfrak{m}) \simeq (\mathbb{Z}/m\mathbb{Z})^*.$$

Ho tenim tot a punt per formular el resultat fonamental de la teoria global de cossos de classes:

Teorema 1.2.6 (llei de reciprocitat d'Artin). *Sigui $L|K$ una extensió finita abeliana de cossos de nombres.*

i) *Existeix un isomorfisme canònic*

$$r_{L|K} : \mathrm{Gal}(L|K) \to \mathbb{C}\mathrm{l}_K / N_{L|K}\mathbb{C}\mathrm{l}_L,$$

anomenat de reciprocitat.

ii) *L'isomorfisme invers de $r_{L|K}$*

$$(\ ,L|K) : \mathbb{C}\mathrm{l}_K / N_{L|K}\mathbb{C}\mathrm{l}_L \longrightarrow \mathrm{Gal}(L|K)$$

defineix el símbol global de residus nòrmics.

Denoti $L_\mathfrak{p}$ el completat de L respecte d'una plaça $\mathfrak{P}|\mathfrak{p}$. En considerar l'homomorfisme natural

$$\iota : K_\mathfrak{p}^* \to \mathbb{C}\mathrm{l}_K, \quad a_\mathfrak{p} \mapsto (\dots, 1, 1, 1, a_\mathfrak{p}, 1, 1, 1, \dots),$$

les lleis de reciprocitats local i global es relacionen per mitjà del diagrama commutatiu següent:

$$\begin{array}{ccc} K_\mathfrak{p}^* & \xrightarrow{(\ ,L_\mathfrak{p}|K_\mathfrak{p})} & \mathrm{Gal}(L_\mathfrak{p}|K_\mathfrak{p}) \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle i} \\ \mathbb{C}\mathrm{l}_K & \xrightarrow{(\ ,L|K)} & \mathrm{Gal}(L|K). \end{array}$$

Donada un idele $\alpha = (\alpha_\mathfrak{p})$, s'obté que

$$(\alpha, L|K) = \prod_\mathfrak{p} (\alpha_\mathfrak{p}, L_\mathfrak{p}|K_\mathfrak{p}),$$

és a dir, el símbol global de residus nòrmics és producte del símbols locals.

Teorema 1.2.7 (d'existència). *L'aplicació $L \to \mathcal{N}_L = N_{L|K}\mathbb{C}\mathrm{l}_L$ estableix una bijecció entre el conjunt de les extensions abelianes i finites de K i el conjunt dels subgrups de $\mathbb{C}\mathrm{l}_K$ tancats i d'índex finit. Se satisfà que*

$$L_1 \subseteq L_2 \Longleftrightarrow \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}.$$

.

Definició 1.2.8. *Si H és un subgrup tancat i d'índex finit de $\mathbb{C}\mathrm{l}_K$, l'extensió abeliana $L|K$ que li correspon en la bijecció anterior s'anomena el cos de classes de H. Si $H = \mathbb{C}\mathrm{l}_K^{\mathfrak{m}}$ és el subgrup de congruència mòdul $\mathfrak{m}$, aleshores el cos $K^{\mathfrak{m}}$ que li correspon s'anomena el cos de classes radial mòdul $\mathfrak{m}$. Per tant,*

$$\mathrm{Gal}(K^{\mathfrak{m}}|K) \simeq \mathrm{Cl}_K(\mathfrak{m}).$$

El cos de classes radial mòdul (1) és el cos de classes de Hilbert $K^{(1)}$. Coincideix amb l'extensió abeliana no ramificada maximal de K i satisfà que

$$\mathrm{Gal}(K^{(1)}/K) \simeq \mathrm{Cl}_K^{(1)}.$$

Definició 1.2.9. *Tota extensió finita i abeliana L d'un cos de nombres K està continguda en un cos de classes radial $K^{\mathfrak{m}}$ de K; l'ideal enter $\mathfrak{m}$ s'anomena un mòdul de definició de l'extensió $L|K$. El conductor $\mathfrak{f}_{L|K}$ és el màxim comú divisor de tots els mòduls de definició de $L|K$. Per tant, és el mòdul més petit per al qual $K \subseteq L \subseteq K^{\mathfrak{f}}$.*

La proposició següent caracteritza el conductor d'una extensió abeliana en termes de la ramificació.

Proposició 1.2.10. *Si $L|K$ és una extensió finita i abeliana i $\mathfrak{f}_{\mathfrak{p}}$ denota el conductor de $L_{\mathfrak{p}}|K_{\mathfrak{p}}$, aleshores*

$$\mathfrak{f}_{L|K} = \prod_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p}},$$

on el producte s'estén a totes les places finites de K. Per tant, un primer finit $\mathfrak{p}$ de K ramifica en L si, i només si, divideix el conductor.

Exercici 1.2.11. *Si $K = \mathbb{Q}$ i $\mathfrak{m} = (m)$, aleshores el cos de classes radial $\mathbb{Q}^{\mathfrak{m}}$ és el subcòs totalment real $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ del cos de les arrels m-èsimes de la unitat. El cos $\mathbb{Q}(\zeta_m)$ és el cos de classes radial mòdul mp_∞, esteses les definicions de manera òbvia.*

Quan es formula la llei global de reciprocitat en termes de classes d'ideals en compte de classes d'ideles, el símbol de residus nòrmics dóna lloc al símbol d'Artin. Ho expliquem tot seguit.

Si $L|K$ és un extensió de cossos de nombres no ramificada en un primer finit $\mathfrak{p}$ de K, el grup de descomposició

$$\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}}) \subseteq \mathrm{Gal}(L|K)$$

és cíclic. Aquest grup té un generador distingit, l'automorfisme de Frobenius, $\varphi_{\mathfrak{P}}$, que es caracteritza per la congruència

$$\varphi_{\mathfrak{P}}(a) \equiv a^q \pmod{\mathfrak{P}}, \quad \text{per a tot } a \in \mathcal{O}_L,$$

on $q = \#(\mathcal{O}_K/\mathfrak{p})$.

Si $L|K$ és una extensió abeliana, posarem

$$\varphi_{\mathfrak{p}} = (\pi_{\mathfrak{p}}, L_{\mathfrak{p}}|K_{\mathfrak{p}}) = \left(\frac{L|K}{\mathfrak{p}}\right).$$

La fórmula següent defineix aleshores el *símbol d'Artin* d'un ideal $\mathfrak{a} = \prod \mathfrak{p}^{v_{\mathfrak{p}}}$ de $\mathcal{O}_K$ no divisible per cap ideal primer ramificat

$$\left(\frac{L|K}{\mathfrak{a}}\right) = \prod \left(\frac{L|K}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

S'obté d'aquesta manera el diagrama commutatiu següent:

$$\begin{tikzcd}
1 \arrow[r] & N_{L|K}\mathbb{C}\mathrm{l}_L \arrow[r] \arrow[d] & \mathbb{C}\mathrm{l}_K \arrow[r, "(\ ,L|K)"] \arrow[d] & \mathrm{Gal}(L|K) \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & H^{\mathfrak{m}}/P_K^{\mathfrak{m}} \arrow[r] & \mathrm{Cl}_K(\mathfrak{m}) \arrow[r, "\left(\frac{L|K}{}\right)"] & \mathrm{Gal}(L|K) \arrow[r] & 1,
\end{tikzcd}$$

on $H^{\mathfrak{m}} := (N_{L|K} I_K^{\mathfrak{m}}) P_K^{\mathfrak{m}}$.

El teorema següent proporciona la llei de descomposició dels ideals primers en les extensions abelianes.

Teorema 1.2.12 (llei de descomposició). *Siguin $L|K$ una extensió abeliana de grau n i $\mathfrak{p}$ un ideal primer de K no ramificat en L. Sigui $\mathfrak{m}$ un mòdul de definició de l'extensió $L|K$. Suposem que $\mathfrak{p} \nmid \mathfrak{m}$. Si f és l'enter més petit per al qual*

$$\mathfrak{p}^f \in (N_{L|K} I_L^{\mathfrak{m}}) P_K^{\mathfrak{m}},$$

aleshores $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, on $g = n/f$, i el grau residual de cada ideal primer $\mathfrak{P}|\mathfrak{p}$ és igual a f.

Del teorema ens resulten conseqüències remarcables:

Corol·lari 1.2.13. *Un ideal primer $\mathfrak{p}$ de K descompon completament en el cos de classes de Hilbert $K^{(1)}$ si, i només si, és principal en K.*

Teorema 1.2.14 (dels ideals principals). *Tot ideal de K esdevé principal en el cos de classes de Hilbert $K^{(1)}$ de K.*

La llei de reciprocitat d'Artin permet reduir la demostració del teorema del ideals principals, conjecturat per Hilbert, a la proposició de teoria de grups que enunciem a continuació.

Proposició 1.2.15 (Furtwängler). *Siguin G un grup finitament generat i G' el seu grup derivat. L'homomorfisme transferidor*

$$G/G' \to G'/G''$$

és trivial.

El teorema següent generalitza la llei de reciprocitat quadràtica de Gauss.

Teorema 1.2.16 (fórmula del producte). *Sigui K un cos de nombres que contingui les arrels n-èsimes de la unitat, $n \geq 2$. Per a tot parell d'elements $a, b \in K^*$ se satisfà que*

$$\prod_{\mathfrak{p}} \left(\frac{a,b}{\mathfrak{p}}\right) = 1.$$

1.3 Funcions L de Hecke

Els caràcters de Hecke poden definir-se sobre els grups d'ideals o bé sobre els grups d'ideles. En imposar certes condicions sobre l'infinit, s'obtenen els *Größencharaktere*. Un cas particulars d'aquests són els caràcters de Dirichlet.

Definició 1.3.1. *Donat un cos de nombres K de grau $n = r_1 + 2r_2$, escriurem*

$$\mathbf{Z} = \mathbb{Z}^{r_1+2r_2},$$
$$\mathbf{R} = \mathbb{R}^{r_1+r_2}.$$

1.3.1 Caràcters de Hecke

Definició 1.3.2. *Sigui $\mathfrak{m} \subseteq \mathcal{O}_K$ un ideal enter. Un caràcter de Hecke mòdul $\mathfrak{m}$ és un homomorfisme continu*

$$\chi : I^{\mathfrak{m}} \to S^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

A tot caràcter de Hecke li podem associar la sèrie L

$$L(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}}, \quad \mathrm{Re}(s) > 1,$$

on el sumatori s'estén a tots els ideals enters i el producte a tots els ideals primers de K. Entenem que $\chi(\mathfrak{a}) = 0$ quan $\operatorname{mcd}(\mathfrak{a}, \mathfrak{m}) \neq 1$. $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$ denota la norma absoluta.

Si es vol que aquestes funcions admetin una prolongació analítica i satisfacin equacions funcionals, cal imposar certes restriccions als caràcters. Sorgeixen aleshores els *Größencharaktere.*

Definició 1.3.3. *Un caràcter de Hecke mòdul $\mathfrak{m}$, $\chi : I^{\mathfrak{m}} \to S^1$, s'anomena un Größencharakter si existeixen dos homomorfismes continus*

$$\chi_{\mathrm{f}} : (\mathcal{O}/\mathfrak{m})^* \to S^1, \quad \chi_\infty : \mathbb{R}^* \to S^1,$$

tals que

$$\chi((a)) = \chi_{\mathrm{f}}(a)\chi_\infty(a)$$

per a tot $a \in \mathcal{O}$, $(a) \in I^{\mathfrak{m}}$.

Aleshores, existeixen nombres $p = (p_\tau) \in \mathbf{Z}$, $p_\tau \in \{0,1\}$ si τ és una plaça real i $p_\tau p_{\overline{\tau}} = 0$ si τ és una plaça complexa, i $q \in \mathbf{R}$, unívocament determinats, tals que

$$\chi_\infty(x) = N(x^p|x|^{-p+iq}).$$

El caràcter s'anomena de tipus (p,q). El mòdul de definició més petit s'anomena el conductor del Größencharakter.

Definició 1.3.4. *Un caràcter de Dirichlet mòdul $\mathfrak{m}$ és un homomorfisme*

$$\chi : \mathrm{Cl}_K(\mathfrak{m}) = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to S^1,$$

del grup radial de classes d'ideals mòdul $\mathfrak{m}$ en la circumferència unitat.

Remarca 1.3.5. *Tot caràcter de Dirichlet mòdul $\mathfrak{m}$,*

$$\chi : I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to S^1,$$

dóna lloc a un caràcter de Hecke $\chi : I_K^{\mathfrak{m}} \to S^1$ tal que $\chi(P_K^{\mathfrak{m}}) = 1$. Defineix un Größencharakter de tipus $(p,0)$, ja que satisfà la igualtat

$$\chi((a)) = \chi_{\mathrm{f}}((a))N(a^p|a|^{-p}),$$

per a un cert caràcter χ_{f} de $(\mathcal{O}/\mathfrak{m})^*$.

Proposició 1.3.6.

i) *Els caràcters de Dirichlet χ mòdul $\mathfrak{m}$ són, exactament, els Größenckaraktere mòdul $\mathfrak{m}$ de tipus $(p,0)$.*

ii) *Els caràcters del grup de les classes d'ideals* Cl_K *són els Größenckaraktere mod* (1) *per als quals* $\chi_\infty = 1$.

Definició 1.3.7. *Donat un Größencharakter* $\chi = (\chi_{\mathrm{f}}, \chi_\infty)$ *mòdul* $\mathfrak{m}$, *la suma de Gauss associada a* χ_f *és donada per la fórmula*

$$\tau_{\mathfrak{m}}(\chi_f, y) = \sum_x \chi_{\mathrm{f}}(x) e^{2\pi i \mathrm{Tr}(xy)},$$

per a tot $y \in \mathfrak{m}^{-1}\mathfrak{D}^{-1}$, *on l'ideal* $\mathfrak{D}$ *denota la diferent de* $K|\mathbb{Q}$, *i el sumatori s'estén a un sistema de representants de* $(\mathcal{O}/\mathfrak{m})^*$.

Els homomorfismes continus $\chi : \mathbb{I}_K/K^* \to S^1$ que factoritzen en homomorfismes

$$\chi : \mathbb{C}\mathrm{l}(\mathfrak{m}) = \mathbb{I}_K/\mathbb{I}_K^{\mathfrak{m}} K^* \to S^1$$

s'anomenen caràcters de Hecke sobre les classes d'ideles, de mòdul de definició $\mathfrak{m}$. En considerar la composició

$$I^{\mathfrak{m}} \xrightarrow{c} \mathbb{C}\mathrm{l}(\mathfrak{m}) \xrightarrow{\chi} S^1,$$

on c denota l'homomorfisme natural, tot caràcter de Hecke sobre les classes d'ideles dóna lloc a un *Größencharakter* del mateix mòdul.

Proposició 1.3.8. *L'aplicació* $\chi \mapsto \chi \circ c$ *estableix una correspondència bijectiva entre els caràcters de Hecke mòdul* $\mathfrak{m}$ *definits sobre les classes d'ideles i els Größencharakter mòdul* $\mathfrak{m}$ *definits sobre les classes d'ideals.*

1.3.2 Equació funcional de les sèries L de Hecke

E. Hecke [Hec70] demostrà l'equació funcional de les sèries L associades a *Größencharaktere* per mitjà de l'ús de funcions theta. La tesi de J. Tate [Tat67], dirigida per E. Artin, permet donar-ne una demostració alternativa, basada en l'anàlisi de Fourier sobre els grups multiplicatius dels cossos $\mathfrak{p}$-ádics i els grups de les ideles. Amb aquest mètode, les equacions funcionals locals són relativament senzilles d'obtenir; les equacions funcionals globals en resulten de fórmules de sumació de Poisson.

Sigui K un cos de nombres. Donats un *Größencharakter* χ, primitiu de mòdul $\mathfrak{m}$, i una classe d'ideals $A \in I_K/P_K$, es defineix la sèrie L parcial relativa a la classe A,

$$L(A, \chi, s) := \sum_{\mathfrak{a} \in A} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}, \quad \text{per a } \mathrm{Re}(s) > 1,$$

on el sumatori s'estén a tots els ideals enters continguts a la classe A. La sèrie L associada a χ descompon aleshores en una suma finita de sèries L parcials

$$L(\chi, s) = \sum_A L(A, \chi, s),$$

on A recorre el conjunt de les classes d'ideals de K. Convé ara que completem les sèries L parcials mitjançant factors d'Euler a l'infinit. Definim la sèrie L de Hecke parcial completa

$$\Lambda(A, \chi, s) = (|d_K| N(\mathfrak{m}))^{s/2} L_\infty(\chi, s) L(A, \chi, s),$$

on $L_\infty(\chi, \ ) = L_{\mathbb{R}}^{r_1} L_{\mathbb{C}}^{r_2}$, i $L_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$, $\quad L_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$, i d_K denota el discriminant de K.

Teorema 1.3.9. *Siguin A una classes d'ideals de K i χ un Größencharakter primitiu mòdul $\mathfrak{m}$, de tipus (p, q).*

i) *La sèrie $\Lambda(A, \chi, s)$ admet una prolongació analítica a tot $\mathbb{C}$ i satisfà l'equació funcional*

$$\Lambda(A, \chi, s) = W(\chi)\Lambda(A', \overline{\chi}, 1 - s),$$

on $AA' = [\mathfrak{m}\mathfrak{d}]$ i $W(\chi)$ és la suma de Gauss normalitzada

$$W(\chi) = \left[i^{\mathrm{Tr}(\overline{p})} N\left(\left(\frac{md}{|md|} \right)^{\overline{p}} \right) \right]^{-1} \frac{\tau(\chi_{\mathrm{f}})}{\sqrt{(N(\mathfrak{m}))}},$$

amb $|W(\chi)| = 1$.

ii) *La funció $\Lambda(A, \chi, s)$ és holomorfa llevat, com a molt, d'un pol simple a*

$$s = \mathrm{Tr}(-p + iq), \quad s = 1 + \mathrm{Tr}(p + iq).$$

iii) *Si $\mathfrak{m} \neq 1$ o bé $p \neq 0$, aleshores la funció $\Lambda(A, \chi, s)$ és entera.*

Corol·lari 1.3.10. *La sèrie $\Lambda(\chi, s)$ admet una prolongació analítica a*

$$\mathbb{C} \backslash \{\mathrm{Tr}(-p + iq)/n, 1 + \mathrm{Tr}(p + iq)/n\}$$

i satisfà l'equació funcional

$$\Lambda(\chi, s) = W(\chi)\Lambda(\overline{\chi}, 1 - s).$$

Si $\mathfrak{m} \neq 1$ o bé $p \neq 0$, aleshores admet una prolongació analítica en una funció entera.

1.3.3 Valors especials

Els valors sobre els enters negatius de les sèries L de Dirichlet associades a un cos de nombres totalment real són remarcables.

Teorema 1.3.11. *Suposem que K és un cos de nombres totalment real. Siguin ζ_K la seva funció zeta de Dedekind i χ un caràcter de Dirichlet. Donada una classe d'ideals A de K, se satisfan les igualtats següents.*

$$\zeta_K(A;1-k) = N(\mathfrak{a})^{k-1} \sum_{i=1}^{m} \left[(-1)^{d_i} \sum_{x \in R(A,C_i)} \frac{B_k(A_i,x)}{k^n} \right],$$

per a $k \geq 1$.

$$L(\chi,1-k) = \sum \chi(\mathfrak{a}) N(\mathfrak{a})^{k-1} \sum_{i=1}^{m} \left[(-1)^{d_i} \sum_{x \in R(A,C_i)} \frac{B_k(A_i,x)}{k^n} \right],$$

on $B_k(A,X)$ denota el k-èsim polinomi de Bernoulli generalitzat.

Corol·lari 1.3.12 (Siegel). *Donat un cos de nombres K totalment real, els valors $\zeta_K(A;1-k)$, $k \geq 1$, són racionals. Per a tot caràcter de Dirichlet χ, els valors $L(\chi,1-k)$, $k \geq 1$, pertanyen al cos $\mathbb{Q}(\chi_f)$.*

El fet anterior és el punt de partida de la construcció de les funcions L p-ádiques, en la teoria d'Iwasawa i Leopoldt.

1.4 Sèries L d'Artin

Siguin $L|K$ una extensió finita i de Galois de cossos de nombres i

$$\rho : G = \mathrm{Gal}(L|K) \to \mathrm{Aut}(V) = \mathbf{GL}(n,\mathbb{C})$$

una representació lineal del seu grup de Galois en els automorfismes d'un $\mathbb{C}$-espai vectorial complex, V, de dimensió n. Denotem per

$$\chi_\rho : G \to \mathbb{C}, \quad \chi_\rho(s) = \mathrm{Tr}\,\rho(s),$$

el caràcter de ρ. Per a cada ideal primer $\mathfrak{P}$ de L, dividint un ideal primer $\mathfrak{p}$ de K, sigui $I_{\mathfrak{P}} = G_{\mathfrak{P},0}$ el grup d'inèrcia en $\mathfrak{P}$ i denoti $V^{I_{\mathfrak{P}}}$ el subespai de V fix per la inèrcia.

Definició 1.4.1. *La sèrie L d'Artin associada a la representació ρ és donada pel producte d'Euler*

$$\mathcal{L}(L|K,\chi_\rho,s)=\prod_{\mathfrak{p}}\frac{1}{\det(1-\rho(\varphi_{\mathfrak{P}})N(\mathfrak{p})^{-s};V^{I_{\mathfrak{P}}})},\quad \textit{per a } Re(s)>1.$$

Denotem per $\mathbf{1}$ el caràcter de la representació trivial. La sèrie $\mathcal{L}$ d'Artin associada al caràcter trivial coincideix amb la funció zeta de Dedekind del cos K,

$$\mathcal{L}(L|K,\mathbf{1},s)=\zeta_K(s).$$

Conjectura 1.4.2 (Artin). *Per a tota representació de Galois irreductible*

$$\rho\colon \mathrm{Gal}(L|K)\to \mathbf{GL}(n,\mathbb{C}),$$

en què $\chi\neq\mathbf{1}$, la sèrie $\mathcal{L}(L|K,\chi_\rho,s)$ admet una prolongació analítica en una funció entera del pla.

Com veurem, la validesa de la conjectura d'Artin en dimensió $n=1$ equival a la teoria global de cossos de classes. En els darrers mesos, hi ha hagut avenços notables en la demostració de la conjectura d'Artin en dimensió 2.

A partir de la descomposició del caràcter r_G de la representació regular de $G=\mathrm{Gal}(L|K)$ com a suma de caràcters irreductibles,

$$r_G=\sum_{\chi}\chi(1)\chi,$$

s'obté el resultat que segueix.

Corol·lari 1.4.3. *Per a tota extensió de Galois de cossos de nombres és*

$$\zeta_L(s)=\zeta_K(s)\prod_{\chi\neq\mathbf{1}}\mathcal{L}(L|K,\chi,s)^{\chi(1)},$$

on el producte s'estén a tots els caràcters irreductibles de $\mathrm{Gal}(L|K)$ *no trivials.*

1.4.1 Conductor d'Artin d'un caràcter

A tot caràcter irreductible χ de $G=\mathrm{Gal}(L|K)$ li volem associar un ideal enter de K, $\mathfrak{f}(\chi)$, anomenat el seu conductor. De fet, el conductor global és producte de conductors locals:

$$\mathfrak{f}(\chi)=\prod_{\mathfrak{p}\nmid\infty}\mathfrak{f}_{\mathfrak{p}}(\chi),$$

on els conductors locals són de la forma

$$\mathfrak{f}_{\mathfrak{p}}(\chi) = \mathfrak{p}^{f_{\mathfrak{p}}(\chi)}.$$

Per tant, la definició prové d'associar a tot caràcter χ i a tot ideal primer $\mathfrak{p}$ de K un enter, $f_{\mathfrak{p}}(\chi)$, anomenat l'exponent del conductor.

Definició 1.4.4. *Sigui χ el caràcter d'una representació irreductible de* $\mathrm{Gal}(L|K)$. *Siguin $\mathfrak{P}$ un ideal primer de L i $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Siguin $G_i(L|K)$ els grups de ramificació en un primer $\mathfrak{P}$ de L. Aleshores,*

$$f_{\mathfrak{p}}(\chi) := \sum_{i \geq 0} \frac{g_i}{g_0} \dim(V/V^{G_i}),$$

on $g_i = \#G_i(L|K)$.

A partir del teorema de Hasse-Arf i de les propietats de la representació d'Artin s'obté el teorema següent:

Teorema 1.4.5. *Per a tot caràcter χ d'una representació de* $\mathrm{Gal}(L|K)$, *i per a tot ideal primer $\mathfrak{p}$ de K, els nombres $f_{\mathfrak{p}}(\chi)$ són enters ≥ 0.*

Proposició 1.4.6. *Si χ és un caràcter de grau* 1 *de* $\mathrm{Gal}(L_{\mathfrak{p}}|K_{\mathfrak{p}})$ *i $L^{\chi}_{\mathfrak{P}}$ denota el cos fix per al nucli de χ, aleshores l'ideal $\mathfrak{p}^{f_{\mathfrak{p}}(\chi)}$ és el conductor de l'extensió cíclica $L^{\chi}_{\mathfrak{P}}|K_{\mathfrak{p}}$, en el sentit de la teoria local de cossos de classes.*

En tenir present les propietats dels conductors locals, s'obté la descomposició del discriminant d'una extensió de Galois en producte de conductors locals.

Teorema 1.4.7 (*Führerdiskriminantenproduktformel*). *Per a tota extensió de Galois de cossos de nombres se satisfà la igualtat*

$$\mathfrak{d}_{L|K} = \prod_{\chi} \mathfrak{f}(\chi)^{\chi(1)},$$

on el producte s'estén a tots els caràcters irreductibles de $\mathrm{Gal}(L|K)$.

1.5 Reformulació de la teoria global de cossos de classes

En aquesta secció resumim el fet que els teoremes de la teoria global de cossos de classes equivalen a la verificació de la conjectura d'Artin en el cas abelià. Equivalentment, les sèries L d'Artin associades a caràcters de grau 1 es poden interpretar com a sèries L de Hecke associades a certs *Größencharaktere*.

1.5.1 Equació funcional de les sèrie L d'Artin abelianes

Sigui $L|K$ una extensió finita i abeliana de cossos de nombres de conductor $\mathfrak{f} = \mathfrak{f}_{L|K}$. Sabem que l'aplicació

$$I_K^{\mathfrak{f}}/P_K^{\mathfrak{f}} \to \mathrm{Gal}(L|K), \quad \mathfrak{a}\,(\mathrm{mod}\, P)^{\mathfrak{f}} \mapsto \left(\frac{L|K}{\mathfrak{a}}\right)$$

és un isomorfisme. Per composició amb el símbol d'Artin, a tot caràcter irreductible de $\mathrm{Gal}(L|K)$, necessàriament de grau 1,

$$\chi : \mathrm{Gal}(L|K) \to \mathbb{C}^*,$$

li podem associar el *Größencharakter* següent:

$$\widetilde{\chi} : \mathbb{I}_K^{\mathfrak{f}} \to I_K^{\mathfrak{f}} \to \mathbb{C}^*.$$

Teorema 1.5.1. *Siguin $L|K$ una extensió abeliana de cossos de nombres, $\mathfrak{f}_{L|K}$ el seu conductor, $\chi \neq \mathbf{1}$ un caràcter de $\mathrm{Gal}(L|K)$ irreductible i $\widetilde{\chi}$ el Größencharakter mòdul $\mathfrak{f}_{L|K}$ associat. Aleshores,*

$$\mathcal{L}(L|K,\chi,s) = \prod_{\mathfrak{p}\in S} \frac{1}{1-\chi(\varphi_{\mathfrak{P}})N(\mathfrak{p})^{-s}}\, L(\widetilde{\chi},s), \quad \mathrm{Re}(s) > 1,$$

on $S = \{\mathfrak{p} | \mathfrak{f}_{L|K} : \chi(I_{\mathfrak{P}}) = 1\}$ i $\varphi_{\mathfrak{P}}$ denota l'element de Frobenius de $\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$.

A la vista d'aquest resultat, s'imposa completar les sèries L d'Artin amb factors gamma. Sigui χ un caràcter de $\mathrm{Gal}(L|K)$, $L|K$ una extensió no necessàriament abeliana.

Definició 1.5.2. *Definim*

$$\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s) = \begin{cases} L_{\mathbb{C}}(s)^{\chi(1)}, & \textit{si } \mathfrak{p} \textit{ és complex,} \\ L_{\mathbb{R}}(s)^{n^+} L_{\mathbb{R}}(s+1)^{n^-}, & \textit{si } \mathfrak{p} \textit{ és real,} \end{cases}$$

on $n^+ = \frac{\chi(1)+\chi(\varphi_{\mathfrak{P}})}{2}$, $n^- = \frac{\chi(1)-\chi(\varphi_{\mathfrak{P}})}{2}$. Com abans,

$$L_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \quad L_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s).$$

Definició 1.5.3. *Donat un caràcter χ de $\mathrm{Gal}(L|K)$, la sèrie L d'Artin completa es defineix per*

$$\Lambda(L|K,\chi,s) = c(L|K,\chi)^{s/2}\mathcal{L}_{\infty}(L|K,\chi,s)\mathcal{L}(L|K,\chi,s), \quad \mathrm{Re}(s) > 1,$$

on

$$\mathcal{L}_{\infty}(L|K,\chi,s) = \prod_{\mathfrak{p}|\infty} \mathcal{L}_{\mathfrak{p}}(L|K,\chi,s), \quad c(L|K,\chi) = |d_K|^{\chi(1)} N(\mathfrak{f}_{L|K}(\chi)).$$

Proposició 1.5.4. *Si χ és un caràcter de grau 1, aleshores les sèries d'Artin i de Hecke completes, associades a χ, coincideixen:*

$$\Lambda(L|K,\chi,s) = \Lambda(\widetilde{\chi},s).$$

A partir dels resultats obtinguts fins ara i del teorema de Brauer de la teoria de caràcters, segons el qual tot caràcter irreductible d'un grup finit és combinació lineal amb coeficients *enters* dels caràcters induïts pels subgrups elementals, resulta el teorema següent:

Teorema 1.5.5. *Sigui $L|K$ una extensió finita i de Galois de cossos de nombres. Aleshores,*

i) *Per a tot caràcter χ de $\mathrm{Gal}(L|K)$, la sèrie L d'Artin $\Lambda(L|K,\chi,s)$ admet una prolongació analítica en una funció meromorfa de $\mathbb{C}$ i satisfà l'equació funcional*

$$\Lambda(L|K,\chi,s) = W(\chi)\Lambda(L|K,\overline{\chi},1-s),$$

on la constant $W(\chi)$ és un nombre complex de mòdul 1.

ii) *Si l'extensió $L|K$ és resoluble i $\chi \neq \mathbf{1}$, la funció d'Artin $\Lambda(L|K,\chi,s)$ és entera.*

1.6 El teorema de densitat de Chebotarev

Mantenim les notacions de la secció precedent. El teorema que segueix és clau en la prova dels teoremes de densitat.

Teorema 1.6.1 (*Coronidis loco*). *Sigui $\chi : I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to \mathbb{C}^*$ un caràcter de Hecke no trivial i irreductible; és a dir, de grau 1. Per a la sèrie L de Hecke*

$$L(\chi,s) = \prod \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}},$$

on $\chi(\mathfrak{p}) = 0$ si $\mathfrak{p}|\mathfrak{m}$, se satisfà que

$$L(\chi,1) \neq 0.$$

Demostració: Sigui $K^{\mathfrak{m}}$ el cos de classes radial $\bmod \mathfrak{m}$. Aleshores tenim un isomorfisme $\mathrm{Gal}(K^{\mathfrak{m}}|K) \simeq \mathbb{C}\mathrm{l}_K(\mathfrak{m})$, i χ pot ser interpretat com a un caràcter de Galois. Llevat d'un nombre finit de factors d'Euler, les sèries $L(\chi,s)$ de

Hecke i $\mathcal{L}(\chi, s)$ d'Artin coincideixen i cap de les dues no té un pol en $s = 1$. A partir de la igualtat

$$\zeta_{K^{\mathfrak{m}}}(s) = \zeta_K(s) \prod_{\chi \neq \mathbf{1}} \mathcal{L}(K^{\mathfrak{m}}|K, \chi, s)^{\chi(1)},$$

i atès que les dues funcions zeta de Dedekind tenen un pol simple en $s = 1$, se segueix que $\mathcal{L}(K^{\mathfrak{m}}|K, \chi, 1) \neq 0$, per a tot $\chi \neq 1$. Per tant, $L(\chi, 1) \neq 0$. $\square$

Arribem ara a una de les aplicacions de més utilitat de la teoria.

Definició 1.6.2. *Donats un cos de nombres K i un subconjunt $M \subseteq I_K$ d'ideals fraccionaris, la densitat de Dirichlet $\delta(M)$ es defineix per la igualtat*

$$\delta(M) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{p} \in M} N(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}},$$

sempre que el límit existeixi.

Teorema 1.6.3 (Chebotarev). *Siguin $L|K$ una extensió finita i de Galois. Donada una transformació $\sigma \in \mathrm{Gal}(L|K)$, sigui*

$$P_{L|K}(\sigma) = \left\{ \mathfrak{p} : \left(\frac{L|K}{\mathfrak{P}} \right) = \sigma \ \text{ per a un } \mathfrak{P}|\mathfrak{p} \right\}.$$

El conjunt $P_{L|K}(\sigma)$ té densitat de Dirichlet donada per la fórmula

$$\delta(P_{L|K}(\sigma)) = \frac{\#\langle \sigma \rangle}{\#\mathrm{Gal}(L|K)},$$

on $\langle \sigma \rangle = \{\tau\sigma\tau^{-1} : \tau \in \mathrm{Gal}(L|K)\}$ és la classe de conjugació de σ.

El resultats que segueixen són conseqüència del teorema de densitat de Chebotarev. Permeten interpretar les extensions de Galois dels cossos de nombres com a veritables màquines distribuïdores d'ideals primers.

Teorema 1.6.4 (Bauer). *Siguin $L|K$ una extensió finita de cossos de nombres, $P_1(L|K)$ el conjunt de tots els ideals primers de K divisibles per un divisor primer $\mathfrak{P}$ de L de grau 1, i $P(L|K)$ el conjunt de tots els ideals primers de K que descomponen completament en L. Aleshores,*

i) *L'extensió $L|K$ és de Galois si, i només si $P(L|K) = P_1(L|K)$.*

ii) *Si $L|K$ és de Galois i M/K és una extensió arbitrària, se satisfà que*

$$P(L|K) \supseteq P(M|K) \Longleftrightarrow L \subseteq M.$$

1.7 El somni de Noether-Artin-Hasse

Possibles generalitzacions de la teoria de cossos de classes cap a una teoria de cossos de classes no abeliana han estat cercades per diversos autors. A. Weil [Wei80] ens ho recorda:

> *E. Noether, E. Artin and H. Hasse had hoped in vain that their theory of simple algebras would lead to a non-abelian theory but that by* 1947 *Artin confided that he was no longer sure that such theory existed.*

L'any 1947 la tesi de Harish-Chandra, dirigida per P. Dirac (un dels pares de la mecànica quàntica relativista), donà un fort impuls a l'estudi dels espais de funcions $L^2(G)$, on G denota un grup algèbric reductiu definit sobre un cos de nombres. Les representacions automorfes de $G(\mathbb{A}_K)$, així com les seves funcions L associades, formarien part del corpus inherent a la filosofia de Langlands.

Bibliografia

[Art65] E. Artin. *Collected Papers.* Addison-Wesley, 1965.

[AT67] E. Artin and J. Tate. *Class Field Theory.* Benjamin, 1967.

[BT97] P. Bayer and A. Travesa, editors. *Representacions automorfes de $GL(2)$, I-II.* Notes del Seminari de Teoria de Nombres (UB-UAB-UPC), 1997.

[CF67] J.W.S. Cassels and A. Froehlich, editors. *Algebraic Number Theory.* Thompson, 1967.

[Che40] C. Chevalley. La theorie du corps de classes. *Ann. of Math.*, 41:394–418, 1940.

[Cox89] D.A. Cox. *Primes of the form $X^2 + nY^2$. Fermat, Class Field Theory, and Complex Multiplication.* Wiley and Sons, 1989.

[Fro77] J. Froehlich, editor. *Algebraic Number Fields. L-functions and Galois properties.* Academic Press, 1977.

[Fur30] Ph. Furtwaengler. Beweis des Hauptidealsatzes fuer Klassenkoerper algebraischer Zahlkoerper. *Abh. Math. Sem. Univ. Hamburg*, 7:14–36, 1930.

[Gol71] L.J. Goldstein. *Analytic Number Theory.* Prentice-Hall, 1971.

[Has67] H. Hasse. History of Class Filed Theory. In *Algebraic Number Theory*, pages 266–279, Washington, D.C., 1967. Thompson.

[HC84] Harish-Chandra. *Collected Papers.* Springer, 1984.

[Hec70] E. Hecke. *Mathematische Werke.* Vandenhoeck and Ruprecht, 1970.

[Her31] J. Herbrand. Sur la theorie des groupes de decomposition, d'inertie et de ramification. *J. Math. pures et appl.*, 10:481–498, 1931.

[Hil76] D. Hilbert. Mathematical problems. Lecture delivered before the International Congress of Mathematics at Paris in 1900. In *Mathematical developments arising from Hilbert problems*, pages 1–34. AMS, Providence, Rhode Island, 1976.

[Hil98] D. Hilbert. *The Theory of algebraic Number Fields.* Springer, 1998.

[Kro68] L. Kronecker. *Mathematische Werke.* Chelsea, 1968.

[Lan71] S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1971.

[Lan76] R.P. Langlands. Some contemporary problems with origins in the Jugendtraum (Hilbert's problem 12)). In *Mathematical developments arising from Hilbert problems*, pages 401–418. AMS, Providence, Rhode Island, 1976.

[Neu86] J. Neukirch. *Class Field Theory.* Springer, 1986.

[Neu99] J. Neukirch. *Algebraic Number Theory.* Springer, 1999.

[Ser79] J.P. Serre. *Local Fields.* Springer, 1979.

[Sie69] C.L. Siegel. Berechnung von Zetafunktionen an ganzzahligen Stellen. *Goettinger Nachr. Akad. Wiss.*, 10:87–102, 1969.

[Tak90] T. Takagi. *Collected Papers.* Springer, 1990.

[Tat67] J. Tate. Fourier analysis in number fields and Hecke's zeta function.Thesis. Princeton, 1950. Cassels, J.W.S. and Froehlich (eds.). In *Algebraic Number Theory*, pages 305–347, Washington, D.C., 1967. Thompson.

[Wei67] A. Weil. *Basic Number Theory.* Springer, 1967.

[Wei80] A. Weil. *Oeuvres Scientifiques. Collected Papers, I-II-III.* Springer, 1980.

Capítol 2

Introducció a les varietats abelianes

V. Rotger
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

Introducció

L'objectiu d'aquesta exposició és donar una visió general dels conceptes bàsics de varietats abelianes que es necessiten per a entendre la teoria de multiplicació complexa que es desenvolupa en la resta de les exposicions d'aquest volum. Ni de bon tros pretén donar un tractament exhaustiu d'aquest tema. La bibliografia que hem utilitzat és [Mu 74], [Mu 83], [Lg 92], [Sh 98] i [La 83].

2.1 Varietats abelianes i polaritzacions

Definició 2.1.1. *Una* varietat abeliana definida sobre un cos k *és una varietat algebraica completa* A *definida sobre* k *juntament amb un punt* $k-$*racional* $o \in A(k)$ *i morfismes definits sobre* k

$$m : A \times A \to A$$

$$i : A \to A$$

satisfent les propietats habituals de grup.

Propietats 2.1.2. *La completitud de A força la llei de grup ser abeliana. A més, A és no singular, per homogeneïtat.*

2.1.1 Divisors de Weil i feixos invertibles

Definició 2.1.3. *Un* divisor de Weil en A *és una suma formal*

$$D = \sum n_Y Y,$$

amb $n_Y \in \mathbb{Z}$ i Y subvarietats irreductibles de codimensió 1. Escrivim

$$\mathrm{CH}^1(A) = \{\textit{Divisors de Weil en } A\}/\{\textit{Divisors principals en } A\},$$

el primer grup de Chow.

Definició 2.1.4. *Un feix invertible en A és un feix L localment lliure de rang 1 en A. El conjunt* $\mathrm{Pic}(A)$ *de classes d'isomorfisme de feixos invertibles en A té una estructura natural de grup amb el producte tensorial de feixos i amb $\mathcal{O}_A$, el feix estructural de A, com a element neutre.*

Com A és no singular,

$$\mathrm{CH}^1(A) \simeq \mathrm{Pic}(A)$$

i per tant és equivalent parlar de feixos invertibles i de divisors de Weil en A.

Si D és un divisor de Weil en A, notem $L = \mathcal{O}_A(D)$ el feix invertible associat.

2.1.2 Feixos invertibles i morfismes en l'espai projectiu

Per a $L \in \mathrm{Pic}(A)$, sigui $H^0(A, L)$ el $k-$espai vectorial de les seccions globals. Si $L = \mathcal{O}_A(D)$, aleshores

$$H^0(A, L) \simeq \{f \in k(A)^\times, \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

L indueix un morfisme

$$\begin{array}{rcl} \phi_L : A & \to & \mathbb{P}^{n-1} \\ a & \to & \{s_1(a), ..., s_n(a)\} \end{array},$$

on $H^0(A, L) =< s_1, ..., s_n >_k$.

Definició 2.1.5. *Les seccions globals $s \in H^0(A, L)$ es diuen les funcions theta de A respecte la polarització L.*

Definició 2.1.6. *Diem que L és un* feix invertible molt ample *si Φ_L indueix una immersió tancada. Diem que L és un* feix ample o una polarització *si $L^{\otimes n}$ és molt ample per algun $n \geq 1$.*

Teorema 2.1.7 (Lefschetz). *Si A és una varietat abeliana i L és ample, aleshores $L^{\otimes n}$ és molt ample per a $n \geq 3$.*

De les mateixes definicions es desprén que *una varietat algebraica és projectiva si i només si existeix una polarització.*

Exemples 2.1.8. *Si C és una corba algebraica, un divisor D és ample si, i només si deg$(D) > 0$. Si C no és una corba hiperel·líptica, el divisor canònic K_C és un divisor molt ample. La immersió tancada que indueix s'anomena l'aplicació canònica.*

2.2 Varietats abelianes sobre $\mathbb{C}$

Si A és una varietat abeliana complexa de dimensió g, aleshores

$$A \simeq \mathbb{C}^g/U,$$

on U és una xarxa completa de $\mathbb{C}^g$. Recíprocament, no és cert que tot tor complex $\mathbb{C}^g/U$ sigui algebraic, és a dir, sigui una varietat abeliana. La pregunta natural és doncs: *Quan un tor complex és una varietat abeliana?* Ja hem vist que existeix una immersió tancada

$$\phi : \mathbb{C}^g/U \to \mathbb{P}^N$$

$$\Updownarrow$$

existeix una polarització, és a dir, un feix invertible o fibrat de línia ample.

Teorema 2.2.1 (Chow). *Si $M \subset \mathbb{P}^N(\mathbb{C})$ és una varietat complexa, aleshores és algebraica.*

Per tant, combinant aquests fets amb el GAGA obtenim que $A = \mathbb{C}^g/U$ és una varietat abeliana si i només si existeix una polarització L en A.

2.2.1 La primera classe de Chern

La primera classe de Chern $c_1(L)$ d'un feix $L \in \mathrm{Pic}(A)$ pot interpretar-se com una forma hermítica

$$c_1(L) = H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$$

tal que $\mathrm{Im}H(U \times U) \subset \mathbb{Z}$. O equivalentment, com una forma $\mathbb{Z}$-bilineal alternada

$$\mathrm{Im}H = E : U \times U \to \mathbb{Z}$$

tal que l'extensió

$$E \otimes \mathbb{R} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

satisfà

$$E(ix, iy) = E(x, y)\ \forall x, y \in \mathbb{C}^g.$$

Observació 2.2.2. *El teorema d'Apple-Humbert precisa quina és la relació entre els feixos invertibles L en A i les formes hermítiques H en $\mathbb{C}^g$. Més endavant, quan disposem dels elements necessaris, en donarem l'enunciat concret.*

Teorema 2.2.3 (Lefschetz). *L és una polarització si i només si $H = c_1(L)$ és definida positiva. En aquest cas,*

$$\dim_{\mathbb{C}} H^0(A, L) = \sqrt{\det(E)}.$$

Definició 2.2.4. *Es defineix el grau de la polarització com*

$$\deg(L) = \sqrt{\det(E)}.$$

La polarització es diu principal si $\deg(L) = 1$. *Una varietat abeliana juntament amb una polarització (principal) es diu una varietat abeliana (principalment) polaritzada.*

Com a conseqüència dels teoremes de Chow, Lefschetz i Apple-Humbert obtenim el

Teorema 2.2.5. *$\mathbb{C}^g/U$ és una varietat abeliana si i només si existeix una forma hermítica i definida positiva H en $\mathbb{C}^g$ tal que la restricció de* $\mathrm{Im}H$ *a la xarxa U pren valors enters. O equivalentment, si existeix una forma de Riemann: una forma $\mathbb{Z}$-bilineal alternada*

$$\mathrm{Im}H = E : U \times U \to \mathbb{Z}$$

tal que l'extensió

$$E \otimes \mathbb{R} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

satisfà

$$E(ix, iy) = E(x, y) \quad \forall x, y \in \mathbb{C}^g.$$

i la forma hermítica en $\mathbb{C}^g$ donada per $E(ix, y)$ és definida positiva.

Exemples.

1. Corbes el·líptiques.

Sigui $A_\tau = \mathbb{C}/U_\tau$, $U_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\mathrm{Im}(\tau) > 0$ un tor complex de dimensió complexa 1. A continuació veurem que sempre són algebraics, és a dir, tots els tors complexos de dimensió 1 són corbes el·líptiques. Considerem la forma hermítica

$$\begin{array}{rcl} H_\tau : \mathbb{C} \times \mathbb{C} & \to & \mathbb{C} \\ (1,1) & \to & 1/\mathrm{Im}(\tau) \end{array}$$

Pel teorema anterior és senzill comprovar que és la primera classe de Chern d'una polarització principal en A. Deduïm que tot tor complex és una corba el·líptica principalment polaritzada. De fet admet una única forma de Riemann E per a cada grau. Considerant la polarització principal H_τ donada, sabem que

$$\dim_{\mathbb{C}} H^0(A, H_\tau) = 1$$

La teoria clàssica de les funcions theta ens dóna un generador d'aquest espai vectorial:

$$\vartheta_\tau(z) := \sum_{n \in \mathbb{Z}} \exp(\pi i n^2 \tau + 2\pi i n z).$$

Diem que ϑ_τ és una funció theta de A_τ respecte H_τ. És a dir,

$$H^0(A_\tau, H_\tau) = \mathbb{C}\vartheta_\tau$$

Tal com hem vist, pel teorema de Lefschetz podem assegurar que per $l \geq 2$, $l^2 H_\tau$ és un feix molt ample en A_τ. Això vol dir que indueix una immersió tancada que en aquest cas és coneguda explícitament i està donada per una base de les funcions theta de A_τ respecte $l^2 L(H)$, on L és un feix molt ample amb classe de Chern $c_1(L) = H$. El teorema d'Apple-Humbert ens diu que sempre existeix un cert L, tot i que no és únic. Aquesta base de $H^0(A, L)$ es construeix mitjançant traslladats de la funció theta clàssica donada anteriorment.

2. La jacobiana d'una corba.

Si C és una corba regular irreductible de gènere g sobre un cos k, aleshores $\mathrm{Pic}^0_{\bar{k}}(C)$ són els punts $\bar{k}$-racionals d'una varietat abeliana, la jacobiana de C. Té una polarització principal natural:

$$\Theta = \{D \in \mathrm{Pic}^0(C), h^0(\mathcal{O}_C(D)) = \ell(D) > 0\}$$

és un divisor de Weil ample principal de $\mathrm{Pic}^0(C)$.

3. Superfícies abelianes amb multiplicació quaterniònica.

Sigui H una àlgebra de quaternions sobre $\mathbb{Q}$ tal que $H \otimes \mathbb{R} \simeq M_2(\mathbb{R})$. Sigui $\mathcal{O} \subset H$ un ordre d'enters maximal. Com a exemples podem considerar:

$$\mathcal{O} = M_2(\mathbb{Z}) \subset M_2(\mathbb{Q})$$

i

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+ij}{2} \subset \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$$

amb $i^2 = -1, j^2 = 23, ij = -ji$. Fixat $\tau \in \mathbb{C}$, $\mathrm{Im}(\tau) > 0$, podem construir el tor complex de dimensió 2

$$A_\tau = \mathbb{C}^2/U_\tau, U_\tau = \mathcal{O}\begin{pmatrix}\tau\\1\end{pmatrix}$$

on els elements de $\mathcal{O}$ actuen en el vector $\begin{pmatrix}\tau\\1\end{pmatrix} \in \mathbb{C}^2$ via la inclusió natural de $\mathcal{O}$ en $M_2(\mathbb{R})$. Els tors complexos A_τ són superfícies abelianes amb la forma de Riemann

$$\begin{array}{rcl} E : \mathcal{O} \times \mathcal{O} & \to & \mathbb{Z} \\ (x, y) & \to & \mathrm{tr}(\mu x \bar{y}), \end{array}$$

on $\mu \in \mathcal{O}, \mu^2 + D = 0$, i $D = 1, 46$ respectivament. En el primer cas obtenim la superfície

$$A_\tau = E_\tau \times E_\tau \in X(1) = \text{la recta } j$$

i en el segon cas obtenim una superfície abeliana

$$A_\tau \in X(46, 1),$$

la corba de Shimura de nivell 1 i discriminant $2{\cdot}23$. Una equació per a aquesta corba és $(x^2 - 45)^2 + 23 + 2y^2 = 0$ (Kurihara).

2.2.2 La matriu de períodes

Fixem $A = V/U, E : U \times U \to \mathbb{Z}$ una varietat abeliana polaritzada. A continuació expliquem com li podem associar una matriu de períodes $\Omega \in \hbar_g$. Primer, busquem una $\mathbb{Z}$ - base simplèctica de la xarxa U respecte E. Això és una base $\lambda_1, ..., \lambda_g, \mu_1, ..., \mu_g$ on E té l'expressió matricial

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$$

amb $D = \mathrm{diag}(d_1, ..., d_g), d_i \in \mathbb{N}, d_i \mid d_{i+1}$. D'aquí podem llegir el grau de la polarització:

$$\deg(E) = d_1 \cdot ... \cdot d_g.$$

L'expressió de λ_i, μ_i en la $\mathbb{C}$ - base de V donada per $e_i = \mu_i / d_i$ és

$$\Pi = (\Omega, D),$$

on $\Omega \in \hbar_h : \Omega$ és simètrica i la seva part imaginària és definida positiva.

Definició 2.2.6. *Així construïda, Ω s'anomena la matriu de períodes de A respecte la polarització E.*

Observem que en el cas de la corba el·líptica E_τ,

$$\Omega = \tau \in \hbar$$

és un element del semiplà superior de Poincaré. *Recíprocament,* donada $\Omega \in \hbar_g$, retrobem

$$A_\Omega = \mathbb{C}^g / \mathbb{Z}^g + \Omega \mathbb{Z}^g$$

i

$$H = D(\mathrm{Im}\Omega)^{-1}$$

polarització del tipus $D = \mathrm{diag}(d_i)$. En particular, $H = (\mathrm{Im}\Omega)^{-1}$ és principal. D'aquesta manera, a $\Omega \in \hbar_g$ li podem associar una varietat abeliana principalment polaritzada. De manera anàloga al cas el·líptic, tornem a tenir

$$\deg(H) = 1 \Rightarrow H^0(A_\Omega, H_\Omega) = \mathbb{C}\vartheta_\omega$$

on

$$\vartheta_\omega(z_1, ..., z_g) := \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^t \cdot \Omega \cdot n + 2\pi i n^t \cdot z)$$

és la funció theta de Riemann generalitzada. De nou, translacions de la funció theta generalitzada ens donen una base de l'espai de les seccions globals d'una polarització molt ampla $l^2 L(H), l \geq 2$ i per tant una immersió tancada de A en $\mathbb{P}_{\mathbb{C}}^{l^{2g}-1}$.

2.3 La varietat abeliana dual

Sigui A una varietat abeliana definida sobre un cos k qualsevol.

Definició 2.3.1. *Si $D \in \mathrm{CH}^1(A)$ és un divisor de Weil i $x \in A(\bar{k})$, definim*

$$D_x := D + x$$

el divisor en A traslladat per x. Definim

$$\mathrm{Pic}^0(A)(\bar{k}) = \{D \in \mathrm{CH}^1(A)(\bar{k}), D_x - D \text{ és un divisor principal } \forall x \in A(\bar{k})\}.$$

Teorema 2.3.2 (Grothendieck). *Es satisfà que* $\mathrm{Pic}^0(A)(\bar{k})$ *són els punts $\bar{k}$-racionals d'una varietat abeliana definida sobre k. L'anomenem la* varietat abeliana dual de A *i la notem $\hat{A}$.*

2.3.1 El cas dels nombres complexos $k = \mathbb{C}$

Si $A = V/U$ és una varietat abeliana complexa, aleshores

$$\hat{A} = \bar{V}^*/U^*$$

on

$$\bar{V}^* := \{w : V \to \mathbb{C} \text{ antilineals:} w(v_1 + v_2) = w(v_1) + w(v_2), w(\lambda v) = \bar{\lambda} v\}$$

i

$$U^* = \{w \in \overline{V}^*, w(U) \subset \mathbb{Z}\}.$$

Mitjançant la forma $\mathbb{R}$-bilineal simètrica i no-degenerada de $V = \mathbb{C}^g$:

$$< v, w >= \sum_{i=1,\ldots,g} (v_i \bar{w}_i + \bar{v}_i w_i)$$

podem identificar $\bar{V}^*$ amb $\mathbb{C}^g$. Amb aquesta identificació,

$$U^* = \{w \in \mathbb{C}^g, < U, w > \subset \mathbb{Z}\}.$$

Així obtenim que en el cas complex, la varietat abeliana dual de $\mathbb{C}^g/U$ la identifiquem amb $\mathbb{C}^g/U^*$.

2.3.2 Morfisme entre A i $\hat{A}$ definit per un feix invertible

Tornem al cas d'un cos k qualsevol. Sigui $L = \mathcal{O}_A(D) \in \mathrm{Pic}(A)$ un feix invertible. L indueix un morfisme entre la varietat abeliana A i la seva dual $\hat{A}$:

$$\begin{array}{rcl} \Phi_L : A & \to & \hat{A} \\ x & \mapsto & D_x - D. \end{array}$$

El teorema del quadrat ens assegura que és un morfisme de grups. De nou, en el cas complex, aquest morfisme es pot explicar d'una manera més senzilla. Notem $A = V/U$ i $H = c_1(L)$ la forma hermítica associada a L via la primera classe de Chern. Aleshores, Φ_L tan sols depèn de H i es pot expressar així:

$$\begin{array}{rcl} \Phi_H : A & \to & \hat{A} \\ v & \mapsto & H(v, \cdot). \end{array}$$

Identificant $\bar{V}^*$ amb $\mathbb{C}^g$ tal com hem fet abans, obtenim

$$\begin{array}{rcl} \Phi_H : \mathbb{C}^g/U & \to & \mathbb{C}^g/U^* \\ v & \mapsto & \Phi_H(v) \end{array}$$

on $\Phi_H(v) \in \mathbb{C}^g$ està determinat per $H(v,w) =< \Phi_H(v), w > \forall w \in \mathbb{C}^g$.

Observació 2.3.3. *Triem $\mathbb{Z}-$bases de les xarxes $U = \mathbb{Z}[e_1, ..., e_{2g}]$ i $U^* = \mathbb{Z}[u_1, ..., u_{2g}]$ tals que $< e_i, u_j >= \delta_{ij}$. Aleshores la representació matricial de l'acció de Φ_H en aquestes bases coincideix amb la matriu de $E = \mathrm{Im}H$ en la base $\{e_i\}$.*

2.3.3 El grup de Néron-Severi

Mitjançant la construcció anterior, a un feix invertible L en una varietat abeliana A li sabem associar un morfisme $\Phi_L : A \to \hat{A}$. Obtenim doncs de manera natural el següent morfisme de grups:

$$\begin{array}{rcl} \Phi : \mathrm{Pic}(A) & \to & \mathrm{Hom}(A, \hat{A}) \\ L & \mapsto & \Phi_L. \end{array}$$

Observem que de la mateixa definició obtenim que

$$\mathrm{Pic}^0(A) = \mathrm{Ker}\Phi$$

induint per tant la inclusió

$$\mathrm{Pic}(A)/\mathrm{Pic}^0(A) \subset \mathrm{Hom}(A, \hat{A}).$$

Definició 2.3.4. $NS(A) := \mathrm{Pic}(A)/\mathrm{Pic}^0(A) \subset \mathrm{Hom}(A, \hat{A})$ *és el* grup de Néron-Severi de A.

En el cas complex $k = \mathbb{C}$, la primera classe de Chern $c_1(L)$ d'un feix invertible L en $A = \mathbb{C}^g/U$ es pot identificar amb una forma hermítica H. El següent teorema d'Apple-Humbert, esmentat anteriorment sense donar-ne l'enunciat, ens aclareix la relació entre els feixos invertibles L en A i les formes hermítiques H en $\mathbb{C}^g$:

Teorema 2.3.5 (Apple-Humbert). *Sigui $A = \mathbb{C}^g/U$ una varietat abeliana complexa. Tenim una successió exacta de grups*

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \xrightarrow{c_1} \{H \textit{ forma hermítica} : \ \mathrm{Im}H(U \times U) \subset \mathbb{Z}\} \to 0.$$

Observació 2.3.6. *Com a conseqüència del teorema d'Apple-Humbert obtenim aquesta caracterització important del grup de Néron-Severi d'una varietat abeliana complexa $A = \mathbb{C}^g/U$:*

$$NS(A) \cong \{H \textit{forma hermítica de } \mathbb{C}^g \quad : \ \mathrm{Im}H(U \times U) \subset \mathbb{Z}\}$$

Definició 2.3.7. *Es diu que $L = \mathcal{O}_A(D) \in \mathrm{Pic}(A)$ un feix invertible és* no degenerat *si Φ_L és una isogènia, és a dir, si el nucli*

$$K(L) := Ker\Phi_L = \{x \in A, D_x - D = 0\}$$

és finit.

Observació 2.3.8. *En $k = \mathbb{C}$, L és no degenerat si i només si $H = c_1(L)$ és una forma hermítica no degenerada, tal i com es desprèn de les mateixes definicions.*

Proposició 2.3.9. *Si L és una polarització, aleshores L és un feix invertible no degenerat:*

$$\Phi_L : A \to \hat{A} \textit{ és una isogènia.}$$

El grau de la isogènia és

$$\deg(\Phi_L) = det(E)$$

on E és la forma de Riemann associada a L. En particular, si A admet una polarització principal, aleshores

$$\Phi_L : A \simeq \hat{A}.$$

Observació 2.3.10. *En el cas complex $k = \mathbb{C}$, hem vist que L és una polarització $\Longleftrightarrow H = c_1(L)$ és definida positiva i es pot comprovar que L és un feix no degenerat $\Longleftrightarrow H = c_1(L)$ és no degenerada. Per tant, la proposició anterior és trivial quan $k = \mathbb{C}$.*

Exemple: La jacobiana $J(C)$ d'una corba C coincideix amb la seva dual perquè el divisor Θ és principal. En el cas complex $k = \mathbb{C}$, l'isomorfisme entre la varietat jacobiana d'una corba i la seva varietat dual és un isomorfisme clàssic:

$$H^0(C, \Omega^1_C)^*/H_1(C, \mathbb{Z}) \cong H^1(C, \mathcal{O}_C)/H^1(C, \mathbb{Z}).$$

2.4 Anell d'endomorfismes i representacions

Definició 2.4.1. *Sigui A una varietat abeliana de dimensió g definida sobre un cos k. Notem $\mathrm{End}(A)$ l'anell d'endomorfismes de A, $End_k(A)$ l'anell d'endomorfismes definits sobre k, $End^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}, End^0_k(A) = End_k(A) \otimes \mathbb{Q}$.*

Definició 2.4.2. *En $k = \mathbb{C}$, sigui $A = V/U$ on V és un $\mathbb{C}$-espai vectorial de dimensió g i U és una $\mathbb{Z}$-xarxa completa. Considerem $\Pi \in M_{2g\times g}(\mathbb{C})$ la matriu de períodes de A respecte unes bases fixades de V i U. Tenim dues representacions naturals:*

$$\begin{array}{rcl} \rho_a : \mathrm{End}(A) & \to & \mathrm{End}(A) \cong M_g(\mathbb{C}) \\ f & \mapsto & A_f \end{array}$$

la representació analítica i

$$\begin{array}{rcl} \rho_r : \mathrm{End}(A) & \to & \mathrm{End}(U) \cong M_{2g}(\mathbb{Z}) \\ f & \mapsto & R_f \end{array}$$

la representació racional.

Corol·lari 2.4.3. *Se satisfà que $\mathrm{rang}_{\mathbb{Z}} \mathrm{End}(A) \leq 4g^2 < +\infty$ per a una varietat abeliana complexa A.*

Observació 2.4.4. *La representació racional és isomorfa a la suma directa de la representació analítica i la seva conjugada:*

$$\rho_r \cong \rho_a \oplus \bar{\rho}_a.$$

Si k és un cos qualsevol, no disposem de les representacions racional i analítica. Introduïrem les representacions ℓ-àdiques, que són en molts sentits anàlogues a la representació racional. En particular permeten generalitzar el corol·lari anterior al cas d'un cos k qualsevol.

Definició 2.4.5.

$$T_\ell(A) := \lim_{\leftarrow} A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}, \forall \ell \neq p = \mathrm{car}(k)$$

és el mòdul de Tate ℓ-àdic de A. Anàlogament al cas complex tenim la representació ℓ-àdica de $\mathrm{End}(A)$*:*

$$\begin{array}{rcl} \rho_\ell : \mathrm{End}(A) & \to & \mathrm{End}(T_\ell(A)) \cong M_{2g}(\mathbb{Z}_{2g}) \\ f & \to & \rho_\ell(f) \end{array}$$

que s'obté en prendre el límit directe de l'acció dels endomorfismes de A sobre la torsió $A[\ell^n]$.

Proposició 2.4.6.

$$\rho_\ell : \mathrm{End}(A) \otimes \mathbb{Z}_\ell \to M_{2g}(\mathbb{Z}_\ell)$$

és una injecció, $\forall \ell \neq p$.

Com a corol·lari (no obvi) s'obté de nou el resultat següent:

Corol·lari 2.4.7. $\mathrm{End}(A)$ *és $\mathbb{Z}$- finit generat, de rang $\leq 4g^2$.*

Observació 2.4.8. *Si A està definida sobre un cos k, les conjectures de Tate diuen que tenim un isomorfisme*

$$\rho_\ell : \mathrm{End}_k(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}_{\mathrm{Gal}(\bar{k}/k)}(T_\ell(A)).$$

Aquestes conjectures estan provades per a cossos finits (Tate) i cossos de nombres (Faltings).

2.5 Estructura de $\mathrm{End}^0(A)$

L'objectiu d'aquesta secció és conèixer amb més detall com és la $\mathbb{Q}$-àlgebra associativa de rang finit $\mathrm{End}^0(A)$. El següent teorema és el punt de partida.

Teorema 2.5.1 (Poincaré). *Sigui A una varietat abeliana sobre un cos k. Aleshores:*

i) Si A és k-simple aleshores $\mathrm{End}_k^0(A)$*és una $\mathbb{Q}$-àlgebra de divisió, és a dir,* $\mathrm{End}_k^0(A)$ *és un cos, no necessàriament commutatiu.*

ii) A és k-isògena a un producte de varietats abelianes simples: $A \sim \Pi A_i^{n_i}$ per certes A_i/k varietats abelianes simples no k-isògenes entre elles, $n_i \geq 1$. En aquest cas, $\mathrm{End}_k^0(A) \cong \oplus M_{n_i}(D_i)$*, on $D_i = \mathrm{End}_k^0(A_i)$ són àlgebres de divisió. En particular obtenim que* $\mathrm{End}_k^0(A)$ *és una àlgebra associativa semisimple.*

En l'àlgebra semisimple $\mathrm{End}_k^0(A)$ disposem de la següent norma i traça:

Definició 2.5.2. *La norma de* $\mathrm{End}_k^0(A)$ *és*

$$\begin{array}{rcl} N : \mathrm{End}_k^0(A) & \to & \mathbb{Q} \\ f & \mapsto & \deg(f) = \det \rho_\ell(f) \end{array} \quad \forall \ell \neq p.$$

La traça de $\mathrm{End}_k^0(A)$ *és*

$$\begin{array}{rcl} T : \mathrm{End}^0(A) & \to & \mathbb{Q} \\ f & \mapsto & \mathrm{tr}\, \rho_\ell(f) \end{array} \quad \forall \ell \neq p.$$

Observació 2.5.3. *Sabem que per $\ell \neq p, \rho_\ell(f) \in M_{2g}(\mathbb{Q}_\ell)$ i per tant cal justificar que les definicions de norma i traça són coherents. Pot comprovar-se que el polinomi característic $P(\rho_\ell(f)) \in \mathbb{Q}[X]$ i no depèn de $\ell \neq p$. Això es deu a què els coeficients d'aquests polinomis característics poden interpretar-se com a productes d'intersecció de cicles algebraics.*

També disposem de manera natural d'una (anti)involució en l'àlgebra $\mathrm{End}_k^0(A)$:

Definició 2.5.4 (La involució de Rosati). *Sigui A/k una varietat abeliana i L una polarització en A. Sigui*

$$\begin{array}{rcl} \Phi_L : A & \to & \hat{A} \\ x & \mapsto & D_x - D \end{array}$$

la isogènia induïda per la polarització. Aleshores la involució de Rosati *de* $\mathrm{End}_k^0(A)$ *associada a L és*

$$\begin{array}{rcl} ' : \mathrm{End}_k^0(A) & \to & \mathrm{End}_k^0(A) \\ f & \mapsto & \Phi_L^{-1} \cdot f \cdot \Phi_L \end{array}$$

Proposició 2.5.5. *La involució de Rosati és una involució positiva de* $\mathrm{End}_k^0(A)$ *respecte la traça* T*:*

$$\begin{array}{ccc} \mathrm{End}_k^0(A) \times \mathrm{End}_k^0(A) & \to & \mathbb{Q} \\ (f,g) & \mapsto & T(f \cdot g') \end{array}$$

és definida positiva.

Corol·lari 2.5.6. *Sigui* K *el centre de* $\mathrm{End}_k^0(A)$*. Aleshores* K *és un cos totalment real o bé un cos de multiplicació complexa (CM): una extensió quadràtica imaginària d'un cos totalment real.*

Teorema 2.5.7. (classificació sobre cossos algebraicament tancats) *Sigui* (A, L) *una varietat abeliana polaritzada i simple sobre* $k = \bar{k}$*. Notem per* $F = \mathrm{End}^0(A)$ *l'àlgebra de divisió dels endomorfismes* ($\otimes\mathbb{Q}$) *de* A *i seguim notant* $K = Z(F)$*. Sigui* $K_0 = \{f \in K, f = f'\}$*, subcòs totalment real de* K*, on* $'$ *és la involució de Rosati associada a* L*. Sigui* $e = [K : \mathbb{Q}]$*,* $e_0 = [K_0 : \mathbb{Q}]$*,* $d^2 = [F : K]$*. Aleshores només es poden donar les següents quatre possibilitats:*

I) $F = K = K_0$ *i* $' = Id_F$*. En aquest cas, necessàriament* $e \mid g$*.*

II) $K = K_0$ *és un cos totalment real.* F *és una àlgebra de quaternions sobre* K*, és a dir,* $d = 2$*, tal que* $\forall \sigma : K \to \mathbb{R}$ *automorfisme sobre* $\mathbb{Q}$*, tenim* $F \otimes_\sigma \mathbb{R} \cong M_2(\mathbb{R})$*. En aquest cas, necessàriament* $2e \mid g$*.*

III) $K = K_0$ *és un cos totalment real.* F *és una àlgebra de quaternions sobre* K *tal que* $\forall \sigma : K \to \mathbb{R}$ *automorfisme sobre* $\mathbb{Q}$*, tenim* $F \otimes_\sigma \mathbb{R} \cong \mathcal{H}$*, els quaternions de Hamilton. En aquest cas, necessàriament* $2e \mid g$ *si car* $k = 0$*;* $e \mid g$ *si car* $k = p > 0$*.*

IV) K *és un cos CM, extensió quadràtica de* K_0*, un cos totalment real.* F *és una àlgebra de divisió sobre* K*. En aquest cas, necessàriament* $e_o d^2 \mid g$ *si car* $k = 0$*;* $e_0 d \mid g$ *si car* $k = p > 0$*.*

Exemples: Si A és una corba el·líptica sobre $\mathbb{C}$, aleshores $\mathrm{End}^0(A)$ és isomorfa a $\mathbb{Q}$ o bé a un cos quadràtic imaginari. Si A és una corba el·líptica sobre un cos k algebraicament tancat de característica positiva, aleshores $\mathrm{End}^0(A)$ és isomorfa a $\mathbb{Q}$, a un cos quadràtic imaginari, o bé una àlgebra de quaternions ramificada en p i en ∞.

2.6 Cossos de mòduli

Definició 2.6.1. *Sigui A una varietat abeliana definida sobre un cos $k \subset \mathbb{C}$. Aleshores $k_0 \subset k$ és cos de mòduli de $A \iff \forall \sigma \in \mathrm{Gal}(\mathbb{C}/k_0)$, $A^\sigma \cong_{/\mathbb{C}} A$. Anàlogament, si (A, L) és una varietat abeliana polaritzada definida sobre k, aleshores k_0 és cos de mòduli de $(A, L) \iff \forall \sigma \in \mathrm{Gal}(\mathbb{C}/k_0)$, $(A^\sigma, L^\sigma) \cong_{/\mathbb{C}} (A, L)$. Si A és una varietat abeliana definida sobre k i $\iota : R \hookrightarrow \mathrm{End}_k(A)$ és una immersió d'anells, aleshores k_0 és cos de moduli del parell (A, ι) $\iff \forall \sigma \in \mathrm{Gal}(\mathbb{C}/k_0)$, $(A^\sigma, \iota^\sigma) \cong_{/\mathbb{C}} (A, \iota)$.*

Proposició 2.6.2. *Si A (i anàlogament per a (A, L), (A, ι), ...) està definida sobre un cos de nombres k amb $k/\mathbb{Q}$ extensió de Galois, aleshores $k_0 = k^H$, on $H = \{\sigma \in \mathrm{Gal}(k/\mathbb{Q}) / A^\sigma \cong_{/\mathbb{C}} A\}$.*

Observació 2.6.3. *Si A està definida sobre un cos k, aleshores clarament $k_0 \subset k$. En canvi, no és cert que sempre existeixi A' definida sobre k_0 amb $A \cong_{/\mathbb{C}} A'$.*

Exemples:

1. Si A és una corba el·líptica definida sobre un cos k, aleshores el cos de mòduli k_0 de A és el mínim cos de definició de la corba.

2. La corba de Shimura $X(6, 1)$ de discriminant 6 i nivell 1 té gènere 0. Una equació del model canònic sobre $\mathbb{Q}$ la va trobar Kurihara: $x^2 + y^2 + 3 = 0$. Sigui $S_\mathbb{Q}$ la corba definida sobre $\mathbb{Q}$ definida per aquesta equació. Segons el treball de Shimura, la corba $S_\mathbb{Q}$ té la següent interpretació modular:

$$S_\mathbb{Q}(k_0) \longleftrightarrow \{(A, \iota, L), k_0 \text{ com a cos de mòduli}\}$$

on A és una superfície abeliana, $\iota : H(6) \hookrightarrow \mathrm{End}^0(A)$ una immersió de l'àlgebra de quaternions de discriminant $D = 6$, L una polarització principal. Cal afegir una condició de compatibilitat entre la immersió ι i la involució de Rosati donada per L que obviem. Breument, les corbes de Shimura parametritzen superfícies abelianes de multiplicació quaterniònica. Observem que $(\sqrt{-7}, 2) \in S_\mathbb{Q}(\mathbb{Q}(\sqrt{-7}))$. Per la interpretació modular, deduïm que existeix una superfície abeliana principalment polaritzada i amb multiplicació quaterniònica (A, ι, L) amb $\mathbb{Q}(\sqrt{-7})$ com a cos de mòduli. En canvi, no pot existir cap model de (A, ι, L) sobre $\mathbb{Q}(\sqrt{-7})$ perquè aquest cos no escindeix l'àlgebra de quaternions $H(6)$!

Bibliografia

[La 83] S. Lang. *Complex Multiplication*, volume 255 of *Grund. der math. Wiss.* Springer V., 1 edition, 1983.

[Lg 92] C. Lange, H. & Birkenhake. *Complex Abelian Varieties*, volume 302 of *Grund. der math. Wiss.* Springer V., 1992.

[Mu 74] D. Mumford. *Abelian Varieties.* Oxford U.P., 1974.

[Mu 83] D. Mumford. *Tata Lectures on Theta I*, volume 28 of *Prog. Math.* Birkhäuser, 1983.

[Sh 98] G. Shimura. *Abelian Varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series.* Princeton Univ. Press, 1a edition, 1998.

Capítol 3

Corbes el·líptiques amb CM i teoria de cossos de classes

A. Travesa[1]
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

El contingut d'aquest capítol és, bàsicament, el de la conferència impartida el dia 1 de febrer de 2000 a EADA, Collbató, dins del Seminari de Teoria de Nombres (UB-UAB-UPC). L'objectiu principal és demostrar el teorema següent.

Teorema 3.0.1. *Siguin $\mathcal{O}$ un ordre d'un cos quadràtic imaginari K i $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionari invertible de K. Llavors, l'invariant j de $\mathfrak{a}$, $j(\mathfrak{a})$, és un nombre enter algebraic i el cos de classes de l'ordre $\mathcal{O}$ és el cos $K(j(\mathfrak{a}))$.*

La versió escrita de la conferència conté detalls que no van ésser desenvolupats en l'exposició oral i està basada, essencialment, en el text [Co 89]. Per a la secció tercera, que tracta dels polinomis modulars, hem reproduït una part del text d'una conferència impartida l'any 1990 en el Seminari de Teoria de Nombres (UB-UAB-UPC), del qual hem suprimit la majoria de les demostracions.

Comencem l'exposició amb l'estudi dels conceptes que apareixen a l'enunciat. A la secció primera, recordem les propietats principals dels ordres

[1] Amb el suport parcial de la DGES: PB 96–0166.

dels cossos quadràtics, dels seus ideals, dels grups de classes, i la relació d'aquests conceptes amb les formes quadràtiques binàries enteres. A la secció segona, repassem la definició i les propietats de la funció j per a relacionar-la amb les corbes el·líptiques amb multiplicació complexa. A la secció tercera, introduïm els polinomis modulars, establim les congruències de Kronecker i relacionem els polinomis modulars amb les isogènies cícliques entre corbes el·líptiques. A la secció quarta, recordem algunes qüestions relatives a la teoria de cossos de classes; essencialment, el teorema de densitat de Txebotarev, la caracterització de les inclusions entre extensions de Galois de cossos de nombres en funció dels primers que hi descomponen completament, i la definició i les propietats bàsiques del cos de classes associat a un ordre d'un cos quadràtic.

La demostració del **teorema 0.1** ocupa tota la secció cinquena. A la secció sisena, enunciem algunes conseqüències del teorema i alguns altres resultats relacionats, especialment, amb la llei de reciprocitat. I, finalment, a la secció setena, estudiem l'equació de les classes i la factorització dels polinomis modulars; hi incloem la discussió d'una afirmació errònea de [Co 89].

3.1 Ordres i ideals dels cossos quadràtics imaginaris

Encara que moltes coses que direm són vàlides per a tots els cossos de nombres, i algunes són vàlides per a tots els cossos quadràtics, ens centrarem principalment en els cossos quadràtics imaginaris.

Recordem que un ordre d'un cos de nombres K és un subanell $\mathcal{O} \subseteq K$ que, com a grup abelià, és lliure de dimensió $n := [K : \mathbb{Q}]$. Equivalentment, un ordre de K és un subanell $\mathcal{O} \subseteq K$ que, com a grup abelià, és finitament generat i conté una $\mathbb{Q}$-base de K. En particular, un ordre $\mathcal{O}$ és un domini d'integritat de cos de fraccions K.

L'anell dels enters algebraics de K, que denotarem per $\mathcal{O}_K$, és un ordre de K. El fet que tot ordre $\mathcal{O}$ de K és finitament generat com a grup abelià implica que tots els elements de $\mathcal{O}$ són enters algebraics de K; en particular, $\mathcal{O} \subseteq \mathcal{O}_K$ i, en conseqüència, $\mathcal{O}_K$ és l'ordre màxim de K. A més a més, com que $\mathcal{O}$ i $\mathcal{O}_K$ són grups abelians lliures de la mateixa dimensió finita, $\mathcal{O}$ és un subgrup d'índex finit de $\mathcal{O}_K$.

Definició 3.1.1. *S'anomena conductor de $\mathcal{O}_K$ en $\mathcal{O}$ l'índex $f = [\mathcal{O}_K : \mathcal{O}]$ de $\mathcal{O}$ en $\mathcal{O}_K$.*

Com a conseqüència, obtenim que $f\mathcal{O}_K \subseteq \mathcal{O}$, de manera que se satisfà

la inclusió $\mathbb{Z} + f\mathcal{O}_K \subseteq \mathcal{O}$. El cas dels ordres dels cossos quadràtics és particularment senzill, i hi val la igualtat. El resultat següent ens proporciona una bona descripció dels ordres dels cossos quadràtics.

Proposició 3.1.2. *Suposem que K és un cos quadràtic i sigui $d \in \mathbb{Z}$, $d \neq 0, 1$, i d lliure de quadrats, tal que $K = \mathbb{Q}(\sqrt{d})$. Posem $D := d$, si $d \equiv 1 \pmod 4$, $D := 4d$, si $d \equiv 2, 3 \pmod 4$, i sigui $\omega_D := \dfrac{D + \sqrt{D}}{2}$. Llavors:*

a $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega_D$.

b Per a tot nombre enter $f \geq 1$ hi ha un i només un ordre de conductor f en $\mathcal{O}_K$; és l'ordre $\mathcal{O}_{Df^2} := \mathbb{Z} \oplus \mathbb{Z}f\omega_D = \mathbb{Z} + f\mathcal{O}_K$. $\square$

Notem que $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\omega_D) = \mathbb{Q}(f\omega_D)$ i que $\mathcal{O}_K = \mathcal{O}_D$.

Observació 3.1.3. *Tal com hem definit D a partir de d, el discriminant de $\mathcal{O}_K$ és exactament D i el discriminant de $\mathcal{O}_{Df^2}$ és exactament Df^2. Així, els ordres dels cossos quadràtics són determinats unívocament pel seu discriminant, que pot ser qualsevol nombre enter no quadrat $\Delta \equiv 0, 1 \pmod 4$.*

Siguin K un cos de nombres, $\mathcal{O} \subseteq K$ un ordre de K i $\mathfrak{a} \subseteq \mathcal{O}$ un ideal no nul. Com que $\mathfrak{a}$ conté una $\mathbb{Q}$-base de K, $\mathfrak{a}$ també és un grup abelià lliure de dimensió $n = [K : \mathbb{Q}]$; en particular, l'anell quocient $\mathcal{O}/\mathfrak{a}$ és finit. La norma de $\mathfrak{a}$ relativa a l'ordre $\mathcal{O}$ és, per definició, el cardinal de l'anell quocient $\mathcal{O}/\mathfrak{a}$; és a dir, $\mathrm{N}(\mathfrak{a}) := \#(\mathcal{O}/\mathfrak{a})$.

Com que tot domini d'integritat finit és un cos, tot ideal primer no nul de $\mathcal{O}$ és maximal i $\mathcal{O}$ és un domini de dimensió 1. D'altra banda, $\mathcal{O}$ és noetherià, perquè, donat un ideal no nul, $\mathfrak{a} \subseteq \mathcal{O}$, l'anell quocient només té una quantitat finita d'ideals, de manera que totes les cadenes d'ideals $\mathfrak{a}_0 := \mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathcal{O}$ estacionen.

Un ordre $\mathcal{O} \subseteq K$ no és, en general, un subanell íntegrament tancat de K; de fet, i per definició, només és íntegrament tancat l'ordre màxim. En particular, els ordres no són anells de Dedekind i no disposem, a priori, d'una bona teoria multiplicativa d'ideals; per exemple, no podem suposar que disposem de factorització única dels ideals com a producte d'ideals primers. Però ens interessa parlar dels ordres dels cossos quadràtics i dels seus grups de classes d'ideals. A fi de posar en evidència algunes particularitats dels ordres i dels ideals, començarem amb un exemple.

Exemple. Considerem el cos quadràtic $K := \mathbb{Q}(\sqrt{-3})$; el seu ordre màxim és $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-3})/2]$, de discriminant -3. D'altra banda, l'anell

$\mathcal{O} := \mathbb{Z}[\sqrt{-3}]$ és l'ordre de K de discriminant -12; el conductor de $\mathcal{O}_K$ en $\mathcal{O}$ és 2. Considerem el $\mathcal{O}$-ideal $\mathfrak{a} \subseteq \mathcal{O}$ generat per 2 i $1+\sqrt{-3}$. Les igualtats

$$\begin{aligned} \frac{1+\sqrt{-3}}{2} \cdot 2 &= 1+\sqrt{-3} \in \mathfrak{a}, \\ \frac{1+\sqrt{-3}}{2} \cdot (1+\sqrt{-3}) &= -1+\sqrt{-3} = -2+(1+\sqrt{-3}) \in \mathfrak{a}, \end{aligned}$$

i el fet que $1, \dfrac{1+\sqrt{-3}}{2}$ generen $\mathcal{O}_K$ com a grup abelià, ens diuen que $\mathfrak{a}$ també és un $\mathcal{O}_K$-ideal. D'altra banda, i com a conseqüència, tenim que $\mathfrak{a} = 2\mathcal{O}_K + (1+\sqrt{-3})\mathcal{O}_K = 2\mathcal{O}_K$, la darrera igualtat en virtut del fet que $1+\sqrt{-3} = 2 \cdot \dfrac{1+\sqrt{-3}}{2} \in 2\mathcal{O}_K$.

En particular, veiem que un $\mathcal{O}$-ideal pot ser, també, un $\mathcal{O}_K$-ideal; dit d'una altra manera, un $\mathcal{O}_K$-ideal pot estar inclòs en algun subordre propi i ésser, per tant, un $\mathcal{O}$-ideal.

Recordem la definició d'ideal fraccionari en el cas general.

Definició 3.1.4. *Siguin K un cos de nombres i $\mathcal{O} \subseteq K$ un ordre de K. Un $\mathcal{O}$-ideal fraccionari de K és un $\mathcal{O}$-submòdul de K no nul i finitament generat. De manera equivalent, un $\mathcal{O}$-ideal fraccionari de K és un $\mathcal{O}$-submòdul de K de la forma $\alpha\mathfrak{a}$, per a algun element $\alpha \in K$, $\alpha \neq 0$, i algun ideal no nul $\mathfrak{a} \subseteq \mathcal{O}$.*

Els ideals $\mathfrak{a} \subseteq \mathcal{O}$ són $\mathcal{O}$-ideals fraccionaris de K; se'ls anomena $\mathcal{O}$-ideals enters. Si un $\mathcal{O}$-ideal fraccionari $\mathfrak{a} \subseteq K$ és de la forma $\mathfrak{a} = \alpha\mathcal{O}$, per a algun element no nul $\alpha \in K$, es diu que $\mathfrak{a}$ és un $\mathcal{O}$-ideal fraccionari principal. En particular, tot $\mathcal{O}$-ideal fraccionari és un grup abelià lliure de dimensió finita $n = [K : \mathbb{Q}]$.

Proposició 3.1.5. *Siguin $\mathcal{O}$ un ordre d'un cos de nombres K i $\mathfrak{a} \subseteq K$ un $\mathcal{O}$-ideal fraccionari. Llavors, l'anell de multiplicadors de $\mathfrak{a}$,*

$$\mathcal{O}(\mathfrak{a}) := \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\},$$

és un ordre de K que conté $\mathcal{O}$ com a subordre. $\square$

Definició 3.1.6. *Un $\mathcal{O}$-ideal fraccionari $\mathfrak{a} \subseteq K$ s'anomena propi si $\mathcal{O} = \mathcal{O}(\mathfrak{a})$; és a dir, si $\mathcal{O}$ és l'anell de multiplicadors de $\mathfrak{a}$.*

Per exemple, l'anell de multiplicadors del $\mathcal{O}$-ideal de l'exemple anterior és l'ordre màxim, de manera que $\mathfrak{a}$ és un $\mathcal{O}$-ideal que no és propi; en canvi, $\mathfrak{a}$ és un $\mathcal{O}_K$-ideal propi.

Proposició 3.1.7. *Sigui $\mathcal{O} \subseteq K$ un ordre d'un cos de nombres. Tot $\mathcal{O}$-ideal fraccionari principal de K és propi.* □

Observació 3.1.8. *Donat un $\mathcal{O}$-ideal fraccionari $\mathfrak{a} \subseteq K$, se satisfà que $\mathcal{O} \subseteq \mathcal{O}(\mathfrak{a})$; però, en general, no se satisfà la igualtat. En qualsevol cas, el mateix conjunt $\mathfrak{a}$ també és un $\mathcal{O}(\mathfrak{a})$-ideal fraccionari; i sempre és un $\mathcal{O}(\mathfrak{a})$-ideal fraccionari propi. Si $\mathcal{O} = \mathcal{O}_K$, tot $\mathcal{O}$-ideal fraccionari és propi.*

Recordem que un $\mathcal{O}$-ideal fraccionari $\mathfrak{a} \subseteq K$ s'anomena invertible si existeix un $\mathcal{O}$-ideal fraccionari $\mathfrak{b} \subseteq K$ tal que $\mathfrak{a}\mathfrak{b} = \mathcal{O}$, on el producte $\mathfrak{a}\mathfrak{b}$ designa el $\mathcal{O}$-ideal fraccionari generat pels productes $\alpha\beta$, on $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$.

A fi de disposar d'una bona teoria multiplicativa d'ideals en el cas dels ordres dels cossos quadràtics, una primera restricció als ideals consisteix a prendre els ideals fraccionaris propis. En efecte, en el cas dels cossos quadràtics, no necessàriament imaginaris, els ideals fraccionaris propis i els ideals fraccionaris invertibles coincideixen. Per a veure-ho, és útil el resultat següent, que ens proporciona ordres i ideals fraccionaris propis a partir de qualsevol nombre algebraic quadràtic.

Lema 3.1.9. *Siguin τ un nombre algebraic quadràtic, $K := \mathbb{Q}(\tau)$ el cos quadràtic generat per τ, i $aX^2 + bX + c \in \mathbb{Z}[X]$, $a, b, c \in \mathbb{Z}$, $a > 0$, $\operatorname{mcd}(a, b, c) = 1$, el polinomi minimal de τ de coeficients enters. Llavors:*

a) $\mathcal{O} := \mathbb{Z} + \mathbb{Z}a\tau = \mathbb{Z} \oplus \mathbb{Z}a\tau$ és un ordre de K.

b) $\mathfrak{a} := \mathbb{Z} \oplus \mathbb{Z}\tau$ és un $\mathcal{O}$-ideal fraccionari propi de K. □

Proposició 3.1.10. *Siguin K un cos quadràtic, $\mathcal{O} \subseteq K$ un ordre de K i $\mathfrak{a} \subseteq K$ un $\mathcal{O}$-ideal fraccionari de K. Llavors, $\mathfrak{a}$ és propi si, i només si, $\mathfrak{a}$ és invertible.* □

Per als $\mathcal{O}$-ideals fraccionaris de K, encara no és suficient demanar que siguin propis per a disposar de factorització única, ni tan sols en el cas dels cossos quadràtics imaginaris. Però ja podem definir el grup de classes d'ideals.

Definició 3.1.11. *Siguin K un cos quadràtic i $\mathcal{O} \subseteq K$ un ordre de K. Escriurem $\mathbf{I}(\mathcal{O})$ per a denotar el conjunt dels $\mathcal{O}$-ideals fraccionaris propis i $\mathbf{P}(\mathcal{O})$ per a denotar el conjunt dels $\mathcal{O}$-ideals fraccionaris principals. En virtut de la proposició anterior, $\mathbf{I}(\mathcal{O})$ és un grup commutatiu amb el producte d'ideals fraccionaris i $\mathbf{P}(\mathcal{O}) \subseteq \mathbf{I}(\mathcal{O})$ n'és un subgrup. S'anomena grup de classes d'ideals de $\mathcal{O}$ el grup quocient $\mathbf{Cl}(\mathcal{O}) := \mathbf{I}(\mathcal{O})/\mathbf{P}(\mathcal{O})$.*

En el cas en què $\mathcal{O} = \mathcal{O}_K$ és l'ordre màxim, aquesta definició coincideix amb la definició usual del grup de classes d'ideals de $\mathcal{O}_K$ ja que, per a l'ordre màxim, tots els ideals fraccionaris són propis. En aquest cas, indicarem per $\mathbf{I}_K$, $\mathbf{P}_K$ els grups $\mathbf{I}(\mathcal{O}_K)$, $\mathbf{P}(\mathcal{O}_K)$, respectivament.

Ens interessa una altra descripció del grup de classes d'ideals d'un ordre $\mathcal{O}$. Per a això, ens caldrà utilitzar propietats de la norma d'ideals fraccionaris en el cas d'ordres de cossos quadràtics imaginaris. Recordem que només hem definit la noció de norma per als ideals enters $\mathfrak{a} \subseteq \mathcal{O}$; per tant, cal definir-la, també, per als ideals fraccionaris. El resultat següent permet fer-ho.

Lema 3.1.12. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre, $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ ideals enters propis, $\alpha, \beta \in \mathcal{O}$, $\alpha, \beta \neq 0$, elements no nuls, i indiquem per $x \mapsto x'$ l'automorfisme no trivial de K. Llavors:*

a) $\mathrm{N}(\alpha\mathcal{O}) = \mathrm{N}(\alpha)$.

b) $\mathrm{N}(\alpha\mathfrak{a}) = \mathrm{N}(\alpha)\mathrm{N}(\mathfrak{a})$.

c) Si α, β és una $\mathbb{Z}$-base de $\mathfrak{a}$, i si posem $\tau := \dfrac{\beta}{\alpha}$ i $aX^2 + bX + c \in \mathbb{Z}[X]$, $a, b, c \in \mathbb{Z}$, $a > 0$, $\mathrm{mcd}(a, b, c) = 1$, el polinomi minimal de τ de coeficients enters, tenim que $\mathfrak{a} = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ i que $\mathrm{N}(\mathfrak{a}) = \dfrac{\mathrm{N}(\alpha)}{a}$.

d) $\mathfrak{a}\mathfrak{a}' = \mathrm{N}(\mathfrak{a})\mathcal{O}$.

e) $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$. □

Notem que demanem que els ideals siguin, a més a més d'enters, propis, i que utilitzem el símbol N tant per a la norma d'un element, cas en el qual és $\mathrm{N}(\alpha) = \alpha\alpha'$, com per a la norma d'un ideal.

Ara, podem definir la norma d'un $\mathcal{O}$-ideal fraccionari propi, no necessàriament enter, de la manera següent. Donat un $\mathcal{O}$-ideal fraccionari propi $\mathfrak{a} \subseteq K$, existeixen $\alpha \in K$, $\alpha \neq 0$, i $\mathfrak{b} \subseteq \mathcal{O}$ un $\mathcal{O}$-ideal enter propi, tals que $\mathfrak{a} = \alpha\mathfrak{b}$. Com que el producte $\mathrm{N}(\alpha)\mathrm{N}(\mathfrak{b})$ no depèn de la representació particular elegida $\mathfrak{a} = \alpha\mathfrak{b}$, amb $\alpha \in K$, $\alpha \neq 0$, $\mathfrak{b} \subseteq \mathcal{O}$, podem definir la norma del $\mathcal{O}$-ideal fraccionari propi $\mathfrak{a}$ com $\mathrm{N}(\mathfrak{a}) := \mathrm{N}(\alpha)\mathrm{N}(\mathfrak{b})$.

L'argument d'escriure els ideals fraccionaris en la forma $\alpha\mathfrak{a}$, amb $\alpha \in K$, $\alpha \neq 0$, i $\mathfrak{a} \subseteq \mathcal{O}$ un ideal enter, ens permet resoldre de manera senzilla l'exercici següent, que ens proporciona les propietats principals de la norma per als $\mathcal{O}$-ideals fraccionaris propis de K.

Exercici. Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre, $\mathfrak{a}, \mathfrak{b} \subseteq K$ $\mathcal{O}$-ideals fraccionaris propis de K, i $\alpha \in K$, $\alpha \neq 0$. Llavors:

a) $\mathrm{N}(\alpha\mathcal{O}) = \mathrm{N}(\alpha)$.

b) $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.

c) $\mathfrak{a}\mathfrak{a}' = \mathrm{N}(\mathfrak{a})\mathcal{O}$.

Observem que la norma pren valors en $\mathbb{Q}_{>0}$, de la mateixa manera que ho fa la norma sobre els elements de K, que ens proporciona una aplicació $\mathrm{N} : K \to \mathbb{Q}$.

A fi d'aplicar la teoria de cossos de classes, cal relacionar els $\mathcal{O}$-ideals fraccionaris propis de K amb els $\mathcal{O}_K$-ideals fraccionaris de K, on $\mathcal{O}_K$ és l'ordre màxim d'un cos quadràtic imaginari K; per a això, i per a obtenir la finitud del grup de classes d'ideals, per exemple, és útil relacionar-los amb les formes quadràtiques binàries enteres.

Teorema 3.1.13. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i $D < 0$ el discriminant de $\mathcal{O}$.*

a) Sigui $f(X,Y) = aX^2 + bXY + cY^2$, $a,b,c \in \mathbb{Z}$, una forma quadràtica binària entera primitiva definida positiva i de discriminant D. Llavors, $\mathbb{Z}a \oplus \mathbb{Z}\dfrac{-b+\sqrt{D}}{2}$ és un $\mathcal{O}$-ideal enter propi de K.

b) L'aplicació que envia la forma $f(X,Y)$ a l'ideal $\mathbb{Z}a \oplus \mathbb{Z}\dfrac{-b+\sqrt{D}}{2}$ indueix un isomorfisme entre el grup $\mathbf{Cl}(D)$, de classes de $\mathbf{SL}(2,\mathbb{Z})$-equivalència de formes quadràtiques binàries enteres primitives definides positives de discriminant D, i el grup de classes d'ideals $\mathbf{Cl}(\mathcal{O})$.

c) Un nombre enter m és representat per una forma $f(X,Y)$ si, i només si, en la classe de $\mathbf{Cl}(\mathcal{O})$ que correspon a la classe de la forma $f(X,Y)$ existeix algun $\mathcal{O}$-ideal enter propi $\mathfrak{a} \subseteq \mathcal{O}$ tal que $\mathrm{N}(\mathfrak{a}) = m$.

d) Un nombre enter m és representat primitivament per una forma $f(X,Y)$ si, i només si, en la classe de $\mathbf{Cl}(\mathcal{O})$ que correspon a la classe de la forma $f(X,Y)$ existeix algun $\mathcal{O}$-ideal enter propi i primitiu $\mathfrak{a} \subseteq \mathcal{O}$ tal que $\mathrm{N}(\mathfrak{a}) = m$ (per a la definició i les propietats dels ideals primitius, cf. **1.27, 1.28, 1.29**). □

Corol·lari 3.1.14. *Siguin K un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ un ordre qualsevol. Donat un nombre enter $M \neq 0$, cada classe d'ideals de $\mathbf{Cl}(\mathcal{O})$ conté un $\mathcal{O}$-ideal enter propi $\mathfrak{a} \subseteq O$ tal que $\mathrm{mcd}(\mathrm{N}(\mathfrak{a}), M) = 1$.* □

Ara estem en disposició de relacionar els $\mathcal{O}$-ideals fraccionaris propis de K amb els $\mathcal{O}_K$-ideals fraccionaris de K, on $\mathcal{O}_K$ és l'ordre màxim d'un cos quadràtic imaginari K.

Definició 3.1.15. *Siguin K un cos quadràtic, $\mathcal{O}_K \subseteq K$ l'ordre màxim, $\mathcal{O} \subseteq K$ un ordre de K, i $\mathfrak{a} \subseteq \mathcal{O}$ un $\mathcal{O}$-ideal enter no nul. Sigui f el conductor de $\mathcal{O}_K$ en $\mathcal{O}$. Es diu que $\mathfrak{a}$ és primer amb f si $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$. A més a més, si $m \in \mathbb{Z}$ és un nombre enter no nul i $\mathfrak{a} \subseteq \mathcal{O}_K$ és un $\mathcal{O}_K$-ideal enter no nul, es diu que $\mathfrak{a}$ és primer amb m si $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$.*

Proposició 3.1.16. *Siguin K un cos quadràtic, $f \geq 1$ un nombre enter, $\mathcal{O}_K \subseteq K$ l'ordre màxim, i $\mathcal{O} \subseteq K$ l'ordre de K de conductor f. Llavors:*

a) Un $\mathcal{O}$-ideal enter no nul $\mathfrak{a} \subseteq \mathcal{O}$ és primer amb f si, i només si, la seva norma no té factors comuns amb f; és a dir, si $\mathrm{mcd}(\mathrm{N}(\mathfrak{a}), f) = 1$.

a') Un $\mathcal{O}_K$-ideal enter no nul $\mathfrak{a} \subseteq \mathcal{O}_K$ és primer amb un nombre enter no nul qualsevol m si, i només si, $\mathrm{mcd}(\mathrm{N}(\mathfrak{a}), m) = 1$.

b) Tot $\mathcal{O}$-ideal enter primer amb f és un $\mathcal{O}$-ideal propi. $\square$

Com a conseqüència d'aquest resultat, tots els $\mathcal{O}$-ideals enters primers amb el conductor pertanyen a $\mathbf{I}(\mathcal{O})$; a més a més, com que per a $\mathcal{O}$-ideals propis es té que $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$, si $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ són $\mathcal{O}$-ideals enters primers amb f, també ho és el producte $\mathfrak{a}\mathfrak{b}$; és a dir, el conjunt dels $\mathcal{O}$-ideals enters primers amb el conductor és un submonoide multiplicatiu de $\mathbf{I}(\mathcal{O})$.

Definició 3.1.17. *Denotarem el subgrup de $\mathbf{I}(\mathcal{O})$ generat pels $\mathcal{O}$-ideals enters primers amb f per $\mathbf{I}(\mathcal{O}, f) \subseteq \mathbf{I}(\mathcal{O})$; i el subgrup generat pels $\mathcal{O}$-ideals principals $\alpha\mathcal{O}$, $\alpha \in \mathcal{O}$, $\alpha \neq 0$, tals que* $\mathrm{mcd}(\mathrm{N}(\alpha), f) = 1$, *per $\mathbf{P}(\mathcal{O}, f) \subseteq \mathbf{I}(\mathcal{O}, f)$.*

El resultat següent identifica el grup de classes d'ideals $\mathbf{Cl}(\mathcal{O})$ amb el grup quocient $\mathbf{I}(\mathcal{O}, f)/\mathbf{P}(\mathcal{O}, f)$.

Proposició 3.1.18. *Siguin K un cos quadràtic, $f \geq 1$ un nombre enter i $\mathcal{O}$ l'ordre de K de conductor f. La inclusió $\mathbf{I}(\mathcal{O}, f) \subseteq \mathbf{I}(\mathcal{O})$ indueix un isomorfisme*

$$\frac{\mathbf{I}(\mathcal{O}, f)}{\mathbf{P}(\mathcal{O}, f)} \simeq \frac{\mathbf{I}(\mathcal{O})}{\mathbf{P}(\mathcal{O})} = \mathbf{Cl}(\mathcal{O}). \ \square$$

Definició 3.1.19. *Siguin K un cos quadràtic imaginari, $\mathcal{O}_K \subseteq K$ l'ordre màxim de K i $m \in \mathbb{Z}$, $m \neq 0$ un nombre enter. Escriurem $\mathbf{I}_K(m)$ per a indicar el subgrup de $\mathbf{I}_K$ generat pels $\mathcal{O}_K$-ideals enters primers amb m.*

La relació entre els $\mathcal{O}$-ideals enters primers amb el conductor de $\mathcal{O}$ i els ideals de $\mathcal{O}_K$ és donada en la proposició següent.

Proposició 3.1.20. *Siguin K un cos quadràtic imaginari, $\mathcal{O}_K \subseteq K$ l'ordre màxim de K, $f \geq 1$ un nombre enter, i $\mathcal{O} \subseteq \mathcal{O}_K$ l'ordre de K de conductor f.*

a) Si $\mathfrak{a} \subseteq \mathcal{O}_K$ és un $\mathcal{O}_K$-ideal primer amb f, llavors $\mathfrak{a} \cap \mathcal{O} \subseteq \mathcal{O}$ és un $\mathcal{O}$-ideal enter primer amb f de la mateixa norma que $\mathfrak{a}$.

b) Si $\mathfrak{a} \subseteq \mathcal{O}$ és un $\mathcal{O}$-ideal enter primer amb f, llavors $\mathfrak{a}\mathcal{O}_K \subseteq \mathcal{O}_K$ és un $\mathcal{O}_K$-ideal enter primer amb f de la mateixa norma que $\mathfrak{a}$.

c) L'aplicació $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ indueix un isomorfisme $\mathbf{I}_K(f)@ > \simeq >> \mathbf{I}(\mathcal{O}, f)$, amb invers donat per l'assignació $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. $\square$

Corol·lari 3.1.21. *Siguin K un cos quadràtic imaginari, $\mathcal{O}_K \subseteq K$ l'ordre màxim de K, $f \geq 1$ un nombre enter, $\mathcal{O} \subseteq \mathcal{O}_K$ l'ordre de K de conductor f i $\mathfrak{a} \subseteq \mathcal{O}$ un $\mathcal{O}$-ideal enter primer amb f. Llavors, $\mathfrak{a}$ admet descomposició única com a producte de $\mathcal{O}$-ideals enters primers que són primers amb f.* $\square$

Teorema 3.1.22. *Siguin K un cos quadràtic imaginari, $\mathcal{O}_K \subseteq K$ l'ordre màxim de K, $f \geq 1$ un nombre enter i $\mathcal{O} \subseteq \mathcal{O}_K$ l'ordre de K de conductor f. Designem per $\mathbf{P}_{K,\mathbb{Z}}(f)$ el subgrup de $\mathbf{I}_K(f)$ generat pels $\mathcal{O}_K$-ideals enters principals de la forma $\alpha\mathcal{O}_K$, on $\alpha \in \mathcal{O}_K$ és tal que $\alpha \equiv a \pmod{f}$, per a algun nombre enter $a \in \mathbb{Z}$ tal que $\operatorname{mcd}(a, f) = 1$. Llavors, existeixen isomorfismes naturals*

$$\mathbf{Cl}(\mathcal{O}) \simeq \frac{\mathbf{I}(\mathcal{O}, f)}{\mathbf{P}(\mathcal{O}, f)} \simeq \frac{\mathbf{I}_K(f)}{\mathbf{P}_{K,\mathbb{Z}}(f)}. \ \square$$

Recordem que el símbol de Kronecker és l'extensió del símbol de Legendre definida per

$$\left(\frac{d}{2}\right) = \begin{cases} 0, & \text{si 2 divideix } d; \\ 1, & \text{si } d \equiv 1 \pmod 8; \\ -1, & \text{si } d \equiv 5 \pmod 8. \end{cases}$$

El símbol de Kronecker permet escriure còmodament una relació entre els nombres de classes de diferents ordres. Posarem $h(\mathcal{O})$ per a denotar l'ordre de $\mathbf{Cl}(\mathcal{O})$, per a tot ordre quadràtic imaginari $\mathcal{O}$.

Teorema 3.1.23. *Siguin K un cos quadràtic imaginari, $\mathcal{O}_K \subseteq K$ l'anell dels enters de K, $\mathcal{O} \subseteq \mathcal{O}_K$ l'ordre d'índex f en $\mathcal{O}_K$, i d_K el discriminant de $\mathcal{O}_K$. Llavors, $h(\mathcal{O})$ és un múltiple enter de $h(\mathcal{O}_K)$ i se satisfà la igualtat*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid f} \left(1 - \left(\frac{d_k}{p}\right)\frac{1}{p}\right). \ \square$$

Corol·lari 3.1.24. *Siguin $D < 0$ un nombre enter no quadrat i tal que $D \equiv 0,1 \pmod 4$, i $f \geq 1$ un nombre enter qualsevol. Siguin $\mathcal{O} := \mathcal{O}_D$, $\mathcal{O}' := \mathcal{O}_{Df^2}$, els ordres de $K := \mathbb{Q}(\sqrt{D})$ de discriminants D i Df^2, respectivament. Llavors,*

$$h(Df^2) = \frac{h(D)f}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{p|f} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right). \square$$

Per a acabar l'estudi dels ordres dels cossos quadràtics imaginaris i els seus ideals, ens cal establir dos resultats que usarem a la demostració del **teorema 0.1**.

Definició 3.1.25. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i $\mathfrak{a} \subseteq \mathcal{O}$ un $\mathcal{O}$-ideal enter propi. Es diu que $\mathfrak{a}$ és un $\mathcal{O}$-ideal primitiu si $\mathfrak{a}$ no és de la forma $\mathfrak{a} = d\mathfrak{b}$, amb $d \in \mathbb{Z}$, $d > 1$, i $\mathfrak{b} \subseteq \mathcal{O}$ un $\mathcal{O}$-ideal enter propi. Un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, s'anomena primitiu si no és de la forma $\alpha = d\beta$, on $d \in \mathbb{Z}$, $d > 1$, i $\beta \in \mathcal{O}$; equivalentment, si el $\mathcal{O}$-ideal $\alpha\mathcal{O} \subseteq \mathcal{O}$ és primitiu.*

Proposició 3.1.26. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K, $\mathfrak{a} \subseteq \mathcal{O}$ un $\mathcal{O}$-ideal enter propi, i $\mathfrak{b} \subseteq K$ un $\mathcal{O}$-ideal fraccionari propi. Llavors:*

a) $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$ és un subgrup d'índex $\mathrm{N}(\mathfrak{a})$.

b) Com a grups abelians, el grup quocient $\dfrac{\mathfrak{b}}{\mathfrak{a}\mathfrak{b}}$ és cíclic si, i només si, $\mathfrak{a}$ és un $\mathcal{O}$-ideal primitiu. $\square$

Corol·lari 3.1.27. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K, $\mathfrak{b} \subseteq K$ un $\mathcal{O}$-ideal fraccionari propi, i $\alpha \in \mathcal{O}$, $\alpha \neq 0$, un element qualsevol. Llavors:*

a) $\alpha\mathfrak{b} \subseteq \mathfrak{b}$ és un subgrup d'índex $\mathrm{N}(\alpha)$.

b) Com a grups abelians, el grup quocient $\dfrac{\mathfrak{b}}{\alpha\mathfrak{b}}$ és cíclic si, i només si, α és un element primitiu de $\mathcal{O}$. $\square$

3.2 Corbes el·líptiques i multiplicacions complexes

Recordem que una $\mathbb{Z}$-xarxa de $\mathbb{C}$ és, per definició, un subgrup additiu $L \subseteq \mathbb{C}$ generat per una $\mathbb{R}$-base de $\mathbb{C}$. En altres paraules, una xarxa és un subgrup $L \subseteq \mathbb{C}$ de la forma $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, on $\omega_1, \omega_2 \in \mathbb{C}$ són $\mathbb{R}$-linealment independents. En particular, una xarxa és un grup abelià lliure de dimensió

2. Per exemple, tot ordre $\mathcal{O}$ d'un cos quadràtic imaginari K i tot $\mathcal{O}$-ideal fraccionari de K són xarxes.

D'altra banda, una corba el·líptica complexa és un grup abelià quocient $\mathbb{C}/L$, on $L \subseteq \mathbb{C}$ és una $\mathbb{Z}$-xarxa. Les funcions de Weierstrass ens proporcionen coordenades per a les corbes el·líptiques complexes i ens permeten obtenir-ne equacions algebraiques.

Definició 3.2.1. *Sigui $L \subseteq \mathbb{C}$ una xarxa fixa. Una funció el·líptica per a L és una funció meromorfa $f : \mathbb{C} \to \mathbb{C}$ tal que per a tot $z \in \mathbb{C}$ i tot $\omega \in L$ és $f(z+\omega) = f(z)$.*

Si ω_1, ω_2 és una $\mathbb{Z}$-base de L, la condició que per a tot $z \in \mathbb{C}$ i tot $\omega \in L$ sigui $f(z+\omega) = f(z)$ és equivalent a la condició que per a tot $z \in \mathbb{C}$ siguin $f(z+\omega_1) = f(z)$ i $f(z+\omega_2) = f(z)$. Dit d'una altra manera, una funció el·líptica per a L és una funció meromorfa i doblement periòdica $f : \mathbb{C} \to \mathbb{C}$; o, si es vol, una funció meromorfa complexa del tor complex $\mathbb{C}/L$. Les funcions el·líptiques per a una xarxa L formen un cos, que s'anomena el cos de les funcions el·líptiques per a L.

Definició 3.2.2. *Donada una xarxa $L \subseteq \mathbb{C}$, sigui*

$$\wp(z; L) := \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

La sèrie $\wp(z; L)$ s'anomena la sèrie $\wp$ de Weierstrass associada a L.

Resumim les propietats fonamentals de la sèrie $\wp$ de Weierstrass, de la funció que defineix, i de la seva derivada, en l'enunciat següent.

Proposició 3.2.3. *Siguin $L \subseteq \mathbb{C}$ una xarxa i $\wp(z; L)$ la sèrie de Weierstrass associada a L. Llavors:*

a) La sèrie $\wp(z; L)$ és absolutament i uniformement convergent en tots els compactes de $\mathbb{C} - L$. Per tant, defineix una funció holomorfa en $\mathbb{C} - L$.

b) La funció $\wp(z; L)$ té un pol doble en cada punt $\omega \in L$. Per tant, la funció $\wp(z; L)$ definida per la sèrie és una funció meromorfa de $\mathbb{C}$.

c) Per a tot $z \in \mathbb{C} - L$, $\wp(-z; L) = \wp(z; L)$; és a dir, $\wp(z; L)$ és una funció parella.

d) La funció $\wp(z; L)$ és doblement periòdica de grup de períodes L. Per tant, la funció $\wp(z; L)$ és una funció el·líptica per a L, les singularitats de la qual són exactament pols dobles en els punts de L. Notem que podem recuperar L com el conjunt format pels pols de la funció $\wp(z; L)$.

e) La funció $\wp'(z;L)$, derivada de $\wp(z;L)$, és una funció el·líptica per a L. A més a més, és una funció senar; és a dir, per a tot $z \in \mathbb{C} - L$ és $\wp'(-z;L) = -\wp'(z;L)$.

f) Per a $z \in \mathbb{C}$, $z \notin L$, és $\wp'(z;L) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^3}$. $\square$

Proposició 3.2.4. *Sigui $L \subseteq \mathbb{C}$ una xarxa. Llavors:*

a) El cos de les funcions el·líptiques per a L és el cos $\mathbb{C}(\wp(z;L), \wp'(z;L))$, generat sobre $\mathbb{C}$ per les funcions $\wp$ i $\wp'$ de Weierstrass.

b) Les funcions el·líptiques parelles per a L formen un subcòs del cos de les funcions el·líptiques; és el cos $\mathbb{C}(\wp(z;L))$, generat sobre $\mathbb{C}$ per la funció $\wp$ de Weierstrass associada a la xarxa L. $\square$

A fi d'obtenir el desenvolupament en sèrie de Laurent de la funció $\wp(z;L)$ considerem, per a tot $r > 2$, la sèrie $G_r(L) := \sum_{\omega \in L - \{0\}} \frac{1}{\omega^r}$.

Proposició 3.2.5. *Sigui $L \subseteq \mathbb{C}$ una xarxa. Llavors:*

a) Per a $r > 2$, la sèrie $G_r(L)$ és absolutament convergent.

b) En un cert entorn de l'origen, se satisfà la igualtat

$$\wp(z;L) = \frac{1}{z^2} + \sum_{n \geq 1} (2n+1) G_{n+2}(L) z^{2n}.$$

c) Si posem $g_2(L) := 60G_4(L)$ i $g_3(L) := 140G_6(L)$, per a la funció $\wp(z;L)$ se satisfà l'equació diferencial

$$\wp'(z;L)^2 = 4\wp(z;L)^3 - g_2(L)\wp(z;L) - g_3(L).$$

d) Siguin $z, w \in \mathbb{C}$, $z, w \notin L$. Llavors, $\wp(z;L) = \wp(w;L)$ si, i només si, $z \pm w \in L$.

e) Si $z \in \mathbb{C}$, $z \notin L$, llavors $\wp'(z;L) = 0$ si, i només si, $2z \in L$.

f) Se satisfà la llei d'addició següent: si $z, w \in \mathbb{C}$ són tals que $z, w, z+w \notin L$, llavors

$$\wp(z+w;L) + \wp(z;L) + \wp(w;L) = \frac{1}{4}\left(\frac{\wp'(z;L) - \wp'(w;L)}{\wp(z;L) - \wp(w;L)}\right)^2.$$

g) Se satisfà la llei de duplicació següent: si $z \in \mathbb{C}$ és tal que $z, 2z \notin L$, llavors

$$\wp(2z; L) = -2\wp(z; L) + \frac{1}{4}\left(\frac{\wp''(z; L)}{\wp'(z; L)}\right)^2. \square$$

Observació 3.2.6. *Considerem la corba el·líptica $\mathbb{C}/L$; si a cada punt $z \in \mathbb{C}/L$ li fem correspondre les coordenades de Weierstrass $(\wp(z; L), \wp'(z; L))$, l'equació de (c) és l'equació d'una corba plana afí, de manera que, efectivament, una corba el·líptica complexa no només és un grup abelià, sinó que també és una corba. D'altra banda, (f) i (g) ens proporcionen equacions algebraiques, en les coordenades de Weierstrass, per a la suma de punts i per a la duplicació de punts de la corba el·líptica $\mathbb{C}/L$. Doncs, una corba el·líptica és una varietat abeliana de dimensió* 1.

Un cop establertes les primeres propietats fonamentals de les funcions el·líptiques, ens proposem definir la funció j, que ens permetrà classificar les corbes el·líptiques mòdul isomorfisme.

Definició 3.2.7. *Siguin $L, L' \subseteq \mathbb{C}$ dues xarxes. Es diu que L i L' són homotètiques si existeix un nombre complex no nul $\lambda \in \mathbb{C}$ tal que $L' = \lambda L$.*

Clarament, aquesta noció és una relació d'equivalència i classifica les xarxes en classes de xarxes homotètiques. Per exemple, si $\mathcal{O} \subseteq K$ és un ordre d'un cos quadràtic imaginari i $\mathfrak{a}, \mathfrak{b} \subseteq K$ són $\mathcal{O}$-ideals fraccionaris propis de K tals que $\mathfrak{b} = \alpha\mathfrak{a}$, per a algun element $\alpha \in K$, $\alpha \neq 0$, les xarxes $\mathfrak{a}, \mathfrak{b}$ són homotètiques; així, tots els $\mathcal{O}$-ideals de la mateixa classe defineixen la mateixa classe de xarxes homotètiques de $\mathbb{C}$.

Lema 3.2.8. *Siguin $L \subseteq \mathbb{C}$ una xarxa i $L' := \lambda L$, amb $\lambda \in \mathbb{C}$, $\lambda \neq 0$.*

a) Si $f(z)$ és una funció el·líptica per a L, llavors $z \mapsto f(z/\lambda)$ és una funció el·líptica per a L'.

b) Les funcions $\wp$ i $\wp'$ de Weierstrass per a L i L' estan relacionades per $\wp(\lambda z; \lambda L) = \lambda^{-2}\wp(z; L)$, $\wp'(\lambda z; \lambda L) = \lambda^{-3}\wp'(z; L)$. $\square$

Per a tota xarxa $L \subseteq \mathbb{C}$, escriurem $\Delta(L) := g_2(L)^3 - 27g_3(L)^2$, on $g_2(L)$, $g_3(L)$ són els nombres definits a la **proposició 2.5**, (c); el nombre $\Delta(L)$ s'anomena l'invariant Δ de la xarxa L, o de la corba el·líptica $\mathbb{C}/L$.

Observació 3.2.9. *Notem que si anomenem e_1, e_2, e_3 les arrels del polinomi $4X^3 - g_2(L)X - g_3(L)$, llavors $\Delta(L) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$, de manera que el discriminant del polinomi $4X^3 - g_2X - g_3$ és $16\Delta(L)$.*

El resultat següent es pot obtenir com a corol·lari de la **proposició 2.5**, (e).

Corol·lari 3.2.10. *Sigui $L \subseteq \mathbb{C}$ una xarxa. Llavors, $\Delta(L) \neq 0$.* $\square$

Observació 3.2.11. *D'aquí es dedueix que tota corba el·líptica complexa és, en particular, una corba no singular.*

Definició 3.2.12. *Sigui $L \subseteq \mathbb{C}$ una xarxa. Es defineix l'invariant j de la xarxa L, i de la corba el·líptica $\mathbb{C}/L$, com*

$$j(L) := 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = 1728\frac{g_2(L)^3}{\Delta(L)}.$$

Teorema 3.2.13. *Siguin $L, L' \subseteq \mathbb{C}$ xarxes. Les xarxes L i L' són homotètiques si, i només si, $j(L) = j(L')$. Equivalentment, les corbes el·líptiques $\mathbb{C}/L$ i $\mathbb{C}/L'$ són isomorfes si, i només si, $j(L) = j(L')$.* $\square$

Observació 3.2.14. *Si tenim en compte la fórmula de duplicació per a la funció $\wp$ de Weierstrass i l'equació diferencial que relaciona $\wp$ i $\wp'$, obtenim la fórmula*

$$\wp(2z; L) = -2\wp(z; L) + \frac{(12\wp(z; L)^2 - g_2(L))^2}{16(4\wp(z; L)^3 - g_2(L)\wp(z; L) - g_3(L))},$$

de manera que $\wp(2z; L)$ és una funció racional de $\wp(z; L)$. De fet, es pot demostrar per inducció que, per a tot $n \in \mathbb{Z}$, $n \geq 1$, la funció $\wp(nz; L)$ és una funció racional de $\wp(z; L)$.

Així, tots els endomorfismes $z \mapsto \alpha z$, $\alpha \in \mathbb{Z}$, del grup abelià $\mathbb{C}/L$ són endomorfismes de la corba el·líptica $\mathbb{C}/L$; el teorema següent caracteritza els nombres complexos $\alpha \in \mathbb{C}$ tals que $\wp(\alpha z; L)$ és una funció racional de $\wp(z; L)$; o sigui, tals que l'assignació $z \mapsto \alpha z$ defineix un endomorfisme de la corba.

Teorema 3.2.15. *Siguin $L \subseteq \mathbb{C}$ una xarxa i $\alpha \in \mathbb{C}$, $\alpha \notin \mathbb{Z}$. Les tres propietats següents són equivalents.*

a) $\wp(\alpha z; L)$ és una funció racional de $\wp(z; L)$.

b) $\alpha L \subseteq L$.

c) Existeix un ordre $\mathcal{O}$ en un cos quadràtic imaginari K tal que $\alpha \in \mathcal{O}$ i L és una xarxa homotètica a un $\mathcal{O}$-ideal fraccionari propi de K.
A més a més, en aquest cas, la funció $\wp(\alpha z; L)$ es pot escriure en la forma

$$\wp(\alpha z; L) = \frac{A(\wp(z; L))}{B(\wp(z; L))},$$

on $A(X), B(X) \in \mathbb{C}[X]$ són polinomis primers entre si per als graus dels quals se satisfan les igualtats

$$\mathrm{gr}(A(X)) = \mathrm{gr}(B(X)) + 1 = [L : \alpha L] = \mathrm{N}(\alpha). \ \square$$

Aquest teorema ens diu que l'anell de multiplicadors d'una xarxa $L \subseteq \mathbb{C}$, $\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$, o equivalentment, l'anell d'endomorfismes de la corba el·líptica $\mathbb{C}/L$, és, o bé $\mathbb{Z}$, o bé un ordre $\mathcal{O} \subseteq K$ d'un cert cos quadràtic imaginari K. A més a més, en aquest cas, existeix un nombre complex no nul $\lambda \in \mathbb{C}$ tal que $\lambda L \subseteq K$ i λL és un $\mathcal{O}$-ideal fraccionari propi de K.

Corol·lari 3.2.16. *Siguin K un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ un ordre de K. Existeix una correspondència bijectiva entre el grup de classes d'ideals $\mathbf{Cl}(\mathcal{O})$ i el conjunt de classes d'homotècia de xarxes que tenen $\mathcal{O}$ com a anell complet de multiplicacions complexes; si es vol, amb el conjunt de les classes d'isomorfisme de corbes el·líptiques complexes que tenen $\mathcal{O}$ com a anell d'endomorfismes de la corba.* $\square$

Així, les corbes el·líptiques complexes que tenen multiplicació complexa per un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K són les corbes isomorfes a les corbes $\mathbb{C}/\mathfrak{a}$, on $\mathfrak{a}$ és qualsevol $\mathcal{O}$-ideal fraccionari propi de K; els correspon l'invariant $j(\mathfrak{a})$.

Observem que tota xarxa és homotèticament equivalent a una xarxa del tipus $\mathbb{Z} \oplus \mathbb{Z}\tau$, on $\tau \in \mathbb{C}$ és tal que $\Im(\tau) > 0$; com que la funció j és invariant per a les classes d'homotècia de xarxes, podem definir la funció j, més que com una funció de xarxes, com una funció d'una variable complexa.

Definició 3.2.17. *Sigui $\mathbb{H} := \{z \in \mathbb{C} : \Im(z) > 0\}$ el semiplà superior de Poincaré. Donat un element qualsevol $\tau \in \mathbb{H}$, considerem la xarxa $L_\tau := \mathbb{Z} \oplus \mathbb{Z}\tau \subseteq \mathbb{C}$ i definim $j(\tau) := j(L_\tau)$.*

Anàlogament, definim $G_r(\tau) := G_r(L_\tau)$, $g_2(\tau) := g_2(L_\tau)$, $g_3(\tau) := g_3(L_\tau)$, i $\Delta(\tau) := \Delta(L_\tau)$. Així, tenim que

$$\begin{aligned}
g_2(\tau) &= 60G_4(\tau) = 60 \textstyle\sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \dfrac{1}{(m+n\tau)^4}, \\
g_3(\tau) &= 140G_6(\tau) = 140 \textstyle\sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \dfrac{1}{(m+n\tau)^6}, \\
\Delta(\tau) &= g_2(\tau)^3 - 27g_3(\tau)^2, \\
j(\tau) &= 1728\frac{g_2(\tau)^3}{\Delta(\tau)}.
\end{aligned}$$

Podem resumir les propietats de la funció j en el teorema següent.

Teorema 3.2.18. *a) La funció $j : \mathbb{H} \to \mathbb{C}$ és una funció holomorfa.*

b) Si $\tau, \tau' \in \mathbb{H}$, llavors $j(\tau) = j(\tau')$ si, i només si, existeix una matriu $\gamma := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{Z})$ tal que $\tau' = \gamma\tau := \dfrac{a\tau + b}{c\tau + d}$. En particular, la funció j és invariant per a l'acció del grup $\mathbf{SL}(2,\mathbb{Z})$ en $\mathbb{H}$.

c) L'aplicació $j : \mathbb{H} \to \mathbb{C}$ és exhaustiva.

d) Per a $\tau \in \mathbb{H}$, és $j'(\tau) \neq 0$, excepte per als casos (d1) $\tau = \gamma i$, $\gamma \in \mathbf{SL}(2,\mathbb{Z})$, *en què $j'(\tau) = 0$, però $j''(\tau) \neq 0$;* (d2) $\tau = \gamma\rho$, $\rho = \dfrac{-1+\sqrt{-3}}{2}$, *i $\gamma \in \mathbf{SL}(2,\mathbb{Z})$, en què és $j'(\tau) = j''(\tau) = 0$, però $j'''(\tau) \neq 0$.* □

Corol·lari 3.2.19. *Siguin $g_2, g_3 \in \mathbb{C}$ nombres arbitraris tals que $g_2^3 - 27g_3^2 \neq 0$. Llavors, existeix una xarxa $L \subseteq \mathbb{C}$ tal que $g_2(L) = g_2$ i $g_3(L) = g_3$.* □

La invariància de la funció j per a l'acció del grup $\mathbf{SL}(2,\mathbb{Z})$, ens ensenya que la funció j és periòdica de període 1 (ja que $\gamma := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathbf{SL}(2,\mathbb{Z})$ actua sobre $z \in \mathbb{H}$ en la forma $\gamma(z) = z + 1$). Per tant, el canvi de variables $q := e^{2\pi i\tau}$ ens diu que $j(q)$ és una funció holomorfa de la corona $0 < |q| < 1$. A més a més, $j(q)$ admet una expressió en sèrie de Laurent

$$j(q) = \sum_{n\in\mathbb{Z}} c_n q^n,$$

$c_n \in \mathbb{C}$. L'expressió de la funció $j(q)$ com a sèrie de Laurent de potències de q és donada en la forma següent.

Considerem les sèries de potències de q

$$\begin{aligned} c_2(q) &:= 1 + 240\textstyle\sum_{n\geq 1}\sigma_3(n)q^n \in \mathbb{Z}[[q]], \\ c_3(q) &:= 1 - 504\textstyle\sum_{n\geq 1}\sigma_5(n)q^n \in \mathbb{Z}[[q]], \\ \delta(q) &:= c_2(q)^3 - c_3(q)^2 \in \mathbb{Z}[[q]], \\ j(q) &:= 1728c_2(q)^3/\delta(q) \in \mathbb{Q}((q)), \end{aligned}$$

on $\sigma_r(n) := \sum_{d|n} d^r$ és la funció suma de les potències r-èsimes dels divisors positius de n.

Lema 3.2.20. *$j(q) \in \dfrac{1}{q}\mathbb{Z}[[q]]^*$; és a dir, $j(q)$ és el producte de $1/q$ per una sèrie de potències invertible de coeficients enters.* □

Observació 3.2.21. *Una mica de càlcul ens permetria donar alguns coeficients de la sèrie $j(q)$:*

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

Lema 3.2.22. *Per a tot $\tau \in \mathbb{H}$ i tot $r \geq 1$ se satisfà que*

$$G_{2r}(\tau) = 2\zeta(2r) + 2\frac{(2\pi i)^{2r}}{(2r-1)!}\sum_{n\geq 1}\sigma_{2r-1}(n)e^{2\pi i n\tau},$$

on $\zeta(\tau)$ designa la funció zeta de Riemann. □

Si ara tenim en compte els valors de la funció zeta

$$\zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945},$$

obtenim que

$$\Delta(\tau) = \frac{(2\pi)^{12}}{2^6 \cdot 3^3}(c_2(e^{2\pi i\tau})^3 - c_3(e^{2\pi i\tau})^2) = \frac{(2\pi)^{12}}{2^6 \cdot 3^3}\delta(e^{2\pi i\tau});$$

i, d'aquí, obtenim que, si $q = e^{2\pi i\tau}$, llavors, per a $\tau \in \mathbb{H}$ és $j(\tau) = j(q)$.

Recordem que una funció modular de pes zero és una funció meromorfa $f : \mathbb{H} \to \mathbb{C}$ invariant per a l'acció de $\mathbf{SL}(2,\mathbb{Z})$ i que admet una q-expansió, on $q := e^{2\pi i z}$; és a dir, una funció meromorfa tal que $f \circ \alpha = f$ per a tota matriu $\alpha \in \mathbf{SL}(2,\mathbb{Z})$ i tal que $f(z) = \sum_{n\geq n_0} c_n q^n$, $n_0 \in \mathbb{Z}$, $c_n \in \mathbb{C}$. Acabem de veure que la funció j és una funció modular de pes zero; no només això.

Proposició 3.2.23. *Siguin $f : \mathbb{H} \to \mathbb{C}$ una funció modular holomorfa en $\mathbb{H}$ i $f(q) := \sum_{n\geq n_0} c_n q^n$, $n_0 \geq 0$, la seva q-expansió, i posem $C := \sum_{n\geq n_0} \mathbb{Z}c_n \subseteq \mathbb{C}$. Llavors, $f(q) \in C[j(q)]$; és a dir, $f(q)$ és un polinomi en $j(q)$ de coeficients en el grup abelià generat pels coeficients c_n.* □

Corol·lari 3.2.24. *El cos de les funcions modulars de pes zero és el cos $\mathbb{C}(j)$, generat per la funció j.* □

3.3 Els polinomis modulars

Un cop definida la funció j i estudiades les seves propietats principals, anem a definir els polinomis modulars.

Sigui $\mathbf{M}_2^+(\mathbb{Z}) := \left\{\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, \det\alpha > 0\right\}$. Llavors, $\mathbf{M}_2^+(\mathbb{Z}) = \biguplus_{n\geq 1} \Delta_n$, on $\Delta_n := \{\alpha \in \mathbf{M}_2^+(\mathbb{Z}) : \det\alpha = n\}$.

Donada $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M}_2^+(\mathbb{Z})$, direm que α és primitiva si els coeficients a, b, c i d són primers entre si; és a dir, si $\mathrm{mcd}(a,b,c,d) = 1$. Per a tot $n \geq 1$, posarem $\Delta_n^* := \{\alpha \in \Delta_n : \alpha \text{ és primitiva}\}$.

Observació 3.3.1. $\Delta_1^* = \Delta_1 = \Gamma(1) := \mathbf{SL}_2(\mathbb{Z})$. *Més generalment, si n és un nombre enter lliure de quadrats, aleshores $\Delta_n^* = \Delta_n$.*

El grup $\Gamma(1)$ actua per l'esquerra en el conjunt Δ_n^* de manera natural. En efecte, si $\gamma \in \Gamma(1)$ i $\alpha \in \Delta_n^*$, aleshores $\gamma\alpha \in \Delta_n$ i és primitiva, ja que, en cas contrari, la matriu α no seria primitiva.

Proposició 3.3.2. *El conjunt $C(n)$ format per les matrius $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ tals que $a \geq 1$, $a|n$, $ad = n$, $\mathrm{mcd}(a,b,d) = 1$ i $0 \leq b < d$, és un sistema de representants de les òrbites $\Gamma(1)\alpha$, $\alpha \in \Delta_n^*$.* □

Observació 3.3.3. *Anàlogament, podem pensar en un sistema de representants format per les matrius $\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$ amb $a, d > 0$, $\mathrm{mcd}(a,c,d) = 1$, $0 \leq c < a$ i $ad = n$.*

Si transposem totes les matrius, obtenim el resultat següent.

Proposició 3.3.4. *El grup $\Gamma(1)$ actua per la dreta en Δ_n^* de manera natural, i el conjunt format per les matrius $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ tals que $a \geq 1$, $a|n$, $d = n/a$, $\mathrm{mcd}(a,b,d) = 1$ i $0 \leq b < a$, és un sistema de representants de les òrbites $\alpha\Gamma(1)$, $\alpha \in \Delta_n^*$. També ho és el conjunt format per les matrius $\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$ amb $a, d > 0$, $\mathrm{mcd}(a,c,d) = 1$, $0 \leq c < d$ i $ad = n$.* □

Les accions de $\Gamma(1)$ en Δ_n^* per l'esquerra i per la dreta estan relacionades de la manera següent.

Proposició 3.3.5. *Per a tota matriu $\alpha \in \Delta_n^*$ és $\Gamma(1)\alpha\Gamma(1) = \Delta_n^*$.* □

En particular, obtenim el resultat següent relatiu a les òrbites.

Corol·lari 3.3.6. *El grup* $\Gamma(1)$ *actua transitivament per la dreta en el conjunt de les òrbites* $\Gamma(1)\alpha$, $\alpha \in \Delta_n^*$, *i recíprocament; actua transitivament per l'esquerra en el conjunt de les òrbites* $\alpha\Gamma(1)$, $\alpha \in \Delta_n^*$. □

Proposició 3.3.7. $\#(\Delta_n^*/\Gamma(1)) = \#(\Gamma(1)\backslash\Delta_n^*) = \psi(n) = n\prod_{p|n}(1+p^{-1})$. □

Considerem fixat un sistema qualsevol, $\{\alpha_1, \ldots, \alpha_{\psi(n)}\}$, de representants de les òrbites $\Gamma(1)\alpha$, per a $\alpha \in \Delta_n^*$.

Lema 3.3.8. *L'acció de* $\Gamma(1)$ *permuta transitivament les funcions* $j \circ \alpha_i$. □

Definició 3.3.9. *Per a tot nombre enter* $n \geq 1$, *escriurem* $\Phi_n(X,j) := \prod_{i=1}^{\psi(n)}(X - j \circ \alpha_i)$ *i anomenarem* $\Phi_n(X,j)$ *el* n*-èsim polinomi modular.*

Com que, per a tot $\gamma \in \Gamma(1)$, és $j = j \circ \gamma$, aquesta definició no depèn del sistema de representants elegit $\{\alpha_1, \ldots, \alpha_{\psi(n)}\}$.

Teorema 3.3.10. *Per a tot nombre enter* $n \geq 1$ *és* $\Phi_n(X,j) \in \mathbb{Z}[X,j]$. □

Proposició 3.3.11. *Per a tot* $n \geq 1$, *el polinomi* $\Phi_n(X,j)$ *és irreductible sobre el cos de les funcions racionals de* j *de coeficients complexos,* $\mathbb{C}(j)$. *És a dir,* $\Phi_n(X,j) \in \mathbb{C}(j)[X]$ *és irreductible.* □

Proposició 3.3.12. *Se satisfà que* $\Phi_1(X,j) = X - j = -\Phi_1(j,X)$. *D'altra banda, per a tot nombre enter* $n > 1$, *el polinomi* $\Phi_n(X,j)$ *és simètric; és a dir,* $\Phi_n(X,j) = \Phi_n(j,X)$. □

Proposició 3.3.13. *Si* n *no és un quadrat, aleshores* $\Phi_n(j,j)$ *és un polinomi en* j *de grau* > 1 *i coeficient dominant* ± 1. □

Corol·lari 3.3.14. *Per a tota matriu* $\alpha \in \mathbf{M}_2^+(\mathbb{Q})$, *la funció* $j \circ \alpha$ *és un element algebraic sobre el cos* $\mathbb{Q}(j)$, *enter sobre l'anell* $\mathbb{Z}[j]$.

DEMOSTRACIÓ. Podem suposar que els coeficients de la matriu α són nombres enters primers entre si; aleshores, si $n := \det\alpha$, resulta que $j \circ \alpha$ és una arrel del polinomi $\Phi_n(X,j) \in \mathbb{Z}[j][X] \subseteq \mathbb{Q}(j)[X]$, mònic. □

Les congruències de Kronecker. Establirem, ara, un resultat bàsic per a la demostració del **teorema 0.1**.

Teorema 3.3.15. *Per a tot nombre primer* p *se satisfà la relació*

$$\Phi_p(X,j) \equiv (X - j^p)(X^p - j) \pmod{p}.$$

DEMOSTRACIÓ. Podem prendre el sistema de representants de les òrbites en la forma usual

$$\alpha_i := \begin{bmatrix} 1 & i \\ 0 & p \end{bmatrix}, \quad i = 0, \ldots, p-1, \qquad \alpha_p := \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}.$$

Si escrivim $j(q) = \sum_{k \geq -1} c_k q^k$, obtenim de seguida que

$$j \circ \alpha_p(q) = j(q^p) = \sum_{k \geq -1} c_k q^{pk} \equiv j(q)^p \pmod{p},$$

ja que, per a tot $k \geq -1$, el coeficient c_k és enter i, per tant, $c_k^p \equiv c_k \pmod{p}$. D'altra banda, si $\zeta := \zeta_p$ és una arrel p-èsima primitiva de la unitat, aleshores $\zeta^{ik} \equiv 1 \pmod{(1-\zeta)}$ a l'anell $\mathbb{Z}[\zeta]$, d'on

$$j \circ \alpha_i(q) = \sum_{k \geq -1} c_k q^{k/p} \zeta^{ik} \equiv \sum_{k \geq -1} c_k q^{k/p} \pmod{(1-\zeta)};$$

això és dir que $j \circ \alpha_i(q) \equiv j(q^{1/p}) \pmod{(1-\zeta)}$.

Ara, de la definició dels polinomis modulars, obtenim que

$$\begin{aligned} \Phi_p(X, j(q)) &= (X - j \circ \alpha_p(q)) \textstyle\prod_{i=0}^{p-1} (X - j \circ \alpha_i(q)) \\ &\equiv (X - j(q)^p) \textstyle\prod_{i=0}^{p-1} \left(X - j(q^{1/p})\right) \\ &= (X - j(q)^p) \left(X - j(q^{1/p})\right)^p \\ &\equiv (X - j(q)^p) \left(X^p - j(q^{1/p})^p\right) \\ &\equiv (X - j(q)^p)(X^p - j(q)) \pmod{(1-\zeta)}, \end{aligned}$$

ja que $j\left(q^{1/p}\right)^p \equiv j(q) \pmod{p}$ i, per tant, $\pmod{(1-\zeta)}$.

Dit d'una altra manera, $\Phi_p(X, j) - (X - j^p)(X^p - j) = \sum_k P_k(j) X^k$, on els $P_k(j) \in p\mathbb{Z}[j]$ són polinomis, ja que el primer membre de la igualtat és de coeficients enters i és divisible per $1 - \zeta$ en $\mathbb{Z}[\zeta][X, j]$. Això demostra la propietat volguda. □

A fi de relacionar els polinomis modulars amb les xarxes de $\mathbb{C}$ i, en conseqüència, amb les corbes el·líptiques, encara cal establir un altre resultat. Comencem per estudiar les subxarxes $L' \subseteq L$ d'una xarxa $L := \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \in \mathbb{H}$, tals que el grup abelià quocient L/L' és cíclic.

Lema 3.3.16. *Siguin $n \in \mathbb{Z}$, $n \geq 1$, un nombre enter, $\tau \in \mathbb{H}$ un element qualsevol, i considerem la xarxa $L := \mathbb{Z} \oplus \mathbb{Z}\tau \subseteq \mathbb{C}$.*

a) Si $\gamma := \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(n)$ *és un dels representants de les òrbites* $\Gamma(1)\alpha$*, per a* $\alpha \in \Delta_n^*$*, llavors,* $L' := d(\mathbb{Z} \oplus \mathbb{Z}\gamma(\tau)) \subseteq L$ *és una subxarxa tal que el grup abelià quocient* L/L' *és cíclic d'ordre* n*.*

b) Si $L' \subseteq L$ *és una subxarxa tal que el grup abelià quocient* L/L' *és cíclic d'ordre* n*, existeix una única matriu* $\gamma \in C(n)$ *tal que* $L' = d(\mathbb{Z} \oplus \mathbb{Z}\gamma(\tau))$*.*

Demostració. Siguin $\tau \in \mathbb{H}$ i $L := \mathbb{Z} \oplus \mathbb{Z}\tau \subseteq \mathbb{C}$. Qualsevol subxarxa L' de L és un grup abelià lliure de dimensió 2, de manera que admet una $\mathbb{Z}$-base $\alpha, \beta \in L'$; si escrivim $\alpha = a\tau + b$, $\beta = c\tau + d$, amb $a, b, c, d \in \mathbb{Z}$, el teorema dels factors invariants ens proporciona l'índex $[L : L'] = |ad - bc|$; a més a més, el grup quocient és cíclic si, i només si, el primer factor invariant de la matriu $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ és 1; és a dir, si $\operatorname{mcd}(a, b, c, d) = 1$. Aquesta observació és la base de la demostració.

(a) En les hipòtesis de (a), sigui $\gamma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(n)$; llavors, $d\gamma(\tau) = a\tau + b$, de manera que $L' = \mathbb{Z}d \oplus \mathbb{Z}d\gamma(\tau) = \mathbb{Z}d \oplus \mathbb{Z}(a\tau + b)$; com que $\operatorname{mcd}(a, b, d) = 1$ i $|ad - bc| = ad = n$, $L' \subseteq L$ és una subxarxa tal que el grup abelià quocient L/L' és cíclic d'ordre n, com volíem veure.

(b) Recíprocament, suposem que $L' \subseteq L$ és una subxarxa tal que el grup abelià quocient L/L' és cíclic d'ordre n. En particular, tenim que $nL \subseteq L'$, de manera que $n = n \cdot 1 \in L'$. Per tant, té sentit considerar el nombre enter positiu més petit que pertany a L', posem d. Llavors, L' admet una $\mathbb{Z}$-base de la forma $d, a\tau + b$, amb $a, b \in \mathbb{Z}$, $a > 0$ (exercici sobre factors invariants). En conseqüència, és $ad = n$ i $\operatorname{mcd}(a, b, d) = 1$, i podem canviar b per $b - kd$, amb $k \in \mathbb{Z}$ apropiat, a fi que sigui $0 \leq b < d$. Amb tot això, obtenim que $\gamma := \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(n)$ i $L' = \mathbb{Z}d \oplus \mathbb{Z}(a\tau + b) = d(\mathbb{Z} \oplus \gamma(\tau))$. Això demostra l'existència de la matriu $\gamma \in C(n)$. La unicitat és immediata a partir del fet que d és el mínim nombre enter positiu que pertany a L' i de la definició de $C(n)$. $\square$

Proposició 3.3.17. *Sigui* $n \in \mathbb{Z}$*,* $n \geq 1$*, un nombre enter. Donats nombres complexos* $z, w \in \mathbb{C}$*, condició necessària i suficient perquè sigui* $\Phi_n(z, w) = 0$ *és que existeixin una xarxa* $L \subseteq \mathbb{C}$ *i una subxarxa* $L' \subseteq L$ *tals que* $j(L') = z$*,* $j(L) = w$*, i el grup abelià quocient* L/L' *sigui cíclic d'ordre* n*.*

Demostració. Acabem de veure que si L és una xarxa de la forma $\mathbb{Z} \oplus \mathbb{Z}\tau$, per a $\tau \in \mathbb{H}$, i $L' \subseteq L$ és una subxarxa tal que el grup abelià quocient L/L' és cíclic d'ordre n, llavors L' és de la forma $L' = d(\mathbb{Z} \oplus \mathbb{Z}\gamma(\tau))$, per

a $d \in \mathbb{Z}$, $d \geq 1$, i $\gamma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(n)$, única. En particular, com que L' i $\mathbb{Z} \oplus \mathbb{Z}\gamma(\tau)$ són xarxes homotètiques, tenim que $j(L') = j(\gamma(\tau))$.

Ara, la definició del polinomi modular ens diu que, en fixar el valor $j(\tau)$ com a segon component, és

$$\Phi_n(X, j(\tau)) = \prod_{\gamma \in C(n)} (X - j(\gamma(\tau))),$$

de manera que les arrels del polinomi $\Phi_n(X, j(\tau))$ són exactament els valors $j(\gamma(\tau))$, per a $\gamma \in C(n)$.

Si tenim en compte que la funció j és exhaustiva, donat $w \in \mathbb{C}$, existeix alguna xarxa $L \subseteq \mathbb{C}$ de la forma $L = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \in \mathbb{H}$, tal que $j(L) = j(\tau) = w$. Llavors, les arrels de $\Phi_n(X, w)$ són els valors $j(\gamma(\tau))$ per a $\gamma \in C(n)$; i aquests valors de j són els valors $j(L')$, per a les subxarxes $L' \subseteq L$ tals que el grup abelià quocient L/L' és cíclic d'ordre n. Així, si $z, w \in \mathbb{C}$ són tals que $\Phi_n(z, w) = 0$, la xarxa L admet una subxarxa L' com la que volem.

El recíproc és immediat a partir de l'observació que hem fet a l'inici de la demostració. Si $L' \subseteq L$ són xarxes tals que el grup abelià quocient L/L' és cíclic d'ordre n, podem canviar-les homotèticament, fet que no fa canviar els valors del seu invariant j, de manera que L sigui de la forma $L = \mathbb{Z} \oplus \mathbb{Z}\tau$, amb $\tau \in \mathbb{H}$. Llavors, $\Phi_n(j(L'), j(L)) = 0$, com volíem demostrar. □

Observació 3.3.18. *El* **teorema 3.10** *ens diu que, per a tot nombre enter $n \geq 1$, l'equació $\Phi_n(X, j) = 0$ ens proporciona una corba afí en el pla X, j definida sobre $\mathbb{Z}$; i la* **proposició 3.11** *ens diu que aquesta corba és absolutament irreductible; s'anomena la corba modular $Y_0(n)$. Llavors, les congruències de Kronecker (***teorema 3.16***) descriuen la reducció mòdul p de la corba modular $Y_0(p)$. I, finalment, la* **proposició 3.18** *ens diu que els punts complexos de la corba modular $Y_0(n)$ es corresponen bijectivament amb les classes d'isomorfisme d'isogènies cícliques de grau n, $E_z \to E_\omega$, on E_ω, E_z són corbes el·líptiques complexes d'invariants $j = \omega$ i $j = z$, respectivament.*

Corol·lari 3.3.19. *Siguin $\mathbb{C}/L$, $\mathbb{C}/L'$ corbes el·líptiques complexes. Existeix alguna isogènia $\mathbb{C}/L' \to \mathbb{C}/L$ cíclica de grau $n \geq 1$ si, i només si, $j(L')$ és una arrel del polinomi $\Phi_n(X, j(L)) \in \mathbb{C}[X]$.* □

3.4 Teoria de cossos de classes

En aquesta secció, enunciarem alguns conceptes i alguns resultats de teoria de cossos de classes que utilitzarem a la prova del **teorema 0.1**. Comença-

rem pel teorema de densitat de Txebotarev.

Definició 3.4.1. *Siguin K un cos de nombres i $\mathcal{P}_K$ el conjunt dels ideals primers del seu anell d'enters, $\mathcal{O}_K$. Donat un subconjunt qualsevol $\mathcal{S} \subseteq \mathcal{P}_\mathcal{K}$, es defineix la densitat de Dirichlet de S, si existeix, com el límit*

$$\delta(\mathcal{S}) := \lim_{\int \to \infty^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} \mathrm{N}(\mathfrak{p})^{-\int}}{-\log(\int - \infty)}.$$

Proposició 3.4.2. *Siguin K un cos de nombres i $\mathcal{S}, \mathcal{T} \subseteq \mathcal{P}_\mathcal{K}$ subconjunts qualssevol.*

a) $\delta(\mathcal{P}_K) = 1$.

b) Si $\mathcal{S} \subseteq \mathcal{T}$, i si $\delta(\mathcal{S})$ i $\delta(\mathcal{T})$ existeixen, llavors $\delta(\mathcal{S}) \leq \delta(\mathcal{T})$.

c) Si $\delta(\mathcal{S})$ existeix, llavors $0 \leq \delta(\mathcal{S}) \leq \infty$.

d) Si $\mathcal{S}$ i $\mathcal{T}$ són disjunts, i si $\delta(\mathcal{S})$ i $\delta(\mathcal{T})$ existeixen, llavors $\delta(\mathcal{S} \cup \mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T})$.

e) Si $\mathcal{S}$ és finit, llavors $\delta(\mathcal{S}) = 1$.

f) Si $\delta(\mathcal{S})$ existeix, i si $\mathcal{S}$ i $\mathcal{T}$ difereixen en una quantitat finita d'elements, llavors $\delta(\mathcal{T}) = \delta(\mathcal{S})$.

g) Sigui $\mathcal{P}_{\mathcal{K},\infty}$ el conjunt dels ideals primers $\mathfrak{p} \subseteq \mathcal{O}_K$ tals que $\mathrm{N}(\mathfrak{p})$ és primer. Llavors, si $\delta(\mathcal{S})$ existeix, també existeix $\delta(\mathcal{S} \cap \mathcal{P}_{\mathcal{K},\infty})$ i $\delta(\mathcal{S}) = \delta(\mathcal{S} \cap \mathcal{P}_{\mathcal{K},\infty})$. □

Sigui, ara, $L|K$ una extensió de Galois, no necessàriament abeliana, de cossos de nombres. Donat $\mathfrak{p} \in \mathcal{P}_K$ tal que $\mathfrak{p}$ és no ramificat en l'extensió $L|K$, els símbols d'Artin $\left(\frac{L|K}{\mathfrak{P}}\right)$, associats a tots els ideals primers $\mathfrak{P}$ de L que divideixen $\mathfrak{p}$, formen una classe de conjugació en $\mathrm{Gal}(L|K)$. Per tant, podem definir el símbol d'Artin $\left(\frac{L|K}{\mathfrak{p}}\right)$ com aquesta classe de conjugació.

Teorema 3.4.3. *De densitat de Txebotarev Siguin $L|K$ una extensió de Galois de cossos de nombres, $\sigma \in \mathrm{Gal}(L|K)$ un element qualsevol, i $\langle\sigma\rangle$ la classe de conjugació de σ en $\mathrm{Gal}(L|K)$. Llavors, el conjunt*

$$\left\{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ és no ramificat en } L \text{ i } \left(\frac{L|K}{\mathfrak{p}}\right) = \langle\sigma\rangle\right\}$$

té densitat de Dirichlet

$$\delta(\mathcal{S}) = \frac{\#\langle\sigma\rangle}{\#\mathrm{Gal}(\mathcal{L}|\mathcal{K})} = \frac{\#\langle\sigma\rangle}{[\mathcal{L} : \mathcal{K}]}. \ \square$$

Corol·lari 3.4.4. *Sigui $L|K$ una extensió de Galois de cossos de nombres. El conjunt dels primers $\mathfrak{p} \in \mathcal{P}_K$ tals que $\left(\frac{L|K}{\mathfrak{p}}\right) = 1$ té densitat $\frac{1}{[L:K]}$. En particular, el conjunt és infinit.* $\square$

Notem que aquest conjunt és el dels ideals primers $\mathfrak{p} \in \mathcal{P}_K$ que descomponen completament en L, ja que un primer $\mathfrak{p} \in \mathcal{P}_K$ descompon completament en L si, i només si, $\left(\frac{L|K}{\mathfrak{p}}\right) = 1$.

De fet, el conjunt dels ideals primers de K que descomponen completament en L caracteritzen unívocament l'extensió $L|K$.

Definició 3.4.5. *Donada una extensió de cossos de nombres $L|K$, no necessàriament de Galois, escriurem*

$$\mathcal{S}_{\mathcal{L}|\mathcal{K}} := \{\mathfrak{p} \in \mathcal{P}_{\mathcal{K}} : \mathfrak{p} \text{ descompon completament en } \mathcal{L}\}.$$

Teorema 3.4.6. *Siguin $L|K$, $M|K$ extensions de Galois de cossos de nombres. Llavors:*

a) $L \subseteq M$ si, i només si, existeix un conjunt finit $\mathcal{T} \subseteq \mathcal{P}_{\mathcal{K}}$ tal que $\mathcal{S}_{\mathcal{M}|\mathcal{K}} \subseteq \mathcal{S}_{\mathcal{L}|\mathcal{K}} \cup \mathcal{T}$.

b) $L = M$ si, i només si, existeixen conjunts finits $\mathcal{T}_\infty, \mathcal{T}_\in \subseteq \mathcal{P}_{\mathcal{K}}$ tals que $\mathcal{S}_{\mathcal{M}|\mathcal{K}} \cup \mathcal{T}_\infty = \mathcal{S}_{\mathcal{L}|\mathcal{K}} \cup \mathcal{T}_\in$.

Observem que l'afirmació (b) és una conseqüència immediata de (a). D'altra banda, l'afirmació (a) és un cas particular del resultat següent, on $f(\mathfrak{P}|\mathfrak{p})$ indica el grau residual.

Proposició 3.4.7. *Siguin $L|K$, $M|K$ extensions de cossos de nombres, no necessàriament de Galois.*

a) Si l'extensió $M|K$ és de Galois, llavors $L \subseteq M$ si, i només si, existeix un subconjunt finit $\mathcal{T} \subseteq \mathcal{P}_{\mathcal{K}}$ tal que $\mathcal{S}_{\mathcal{M}|\mathcal{K}} \subseteq \mathcal{S}_{\mathcal{L}|\mathcal{K}} \cup \mathcal{T}$.

b) Si l'extensió $L|K$ és de Galois, llavors $L \subseteq M$ si, i només si, existeix un subconjunt finit $\mathcal{T} \subseteq \mathcal{P}_{\mathcal{K}}$ tal que $\tilde{\mathcal{S}}_{M|K} \subseteq \mathcal{S}_{\mathcal{L}|\mathcal{K}} \cup \mathcal{T}$, on

$$\tilde{\mathcal{S}}_{M|K} := \{\mathfrak{p} \in \mathcal{P}_K : \ \mathfrak{p} \text{ és no ramificat en } M, \ \text{ i } f(\mathfrak{P}|\mathfrak{p}) = 1, \\ \text{per a algun primer } \mathfrak{P} \text{ de } M\}. \ \square$$

Notem que si $M|K$ és de Galois, llavors $\tilde{\mathcal{S}}_{M|K} := \mathcal{S}_{\mathcal{M}|\mathcal{K}}$; així, qualsevol de les dues afirmacions d'aquesta proposició implica el teorema anterior.

Per a acabar aquesta secció, introduirem el concepte i les propietats més generals dels cossos de classes dels ordres dels cossos quadràtics imaginaris. Siguin, doncs, K, un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ l'ordre de conductor f de K.

En el **teorema 1.24**, hem establert que el grup de classes d'ideals de l'ordre $\mathcal{O}$ es pot escriure en la forma

$$\mathbf{Cl}(\mathcal{O}) \simeq \frac{\mathbf{I}_K(f)}{\mathbf{P}_{K,\mathbb{Z}}(f)},$$

on $\mathbf{P}_{K,\mathbb{Z}}(f)$ és el subgrup de $\mathbf{I}_K(f)$ generat pels $\mathcal{O}_K$-ideals enters principals de la forma $\alpha\mathcal{O}_K$, on $\alpha \in \mathcal{O}_K$ és tal que $\alpha \equiv a \pmod{f}$, per a algun nombre enter $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a, f) = 1$.

Si denotem per $\mathbf{P}_{K,1}(f)$ el subgrup principal de congruència per al mòdul f; és a dir, el subgrup de $\mathbf{I}_K(f)$ generat pels $\mathcal{O}_K$-ideals enters principals de la forma $\alpha\mathcal{O}_K$, on $\alpha \in \mathcal{O}_K$ és tal que $\alpha \equiv 1 \pmod{f}$, és immediat que $\mathbf{P}_{K,1}(f) \subseteq \mathbf{P}_{K,\mathbb{Z}}(f) \subseteq \mathbf{I}_K(f)$, de manera que hi ha exactament un cos de classes per al subgrup $\mathbf{P}_{K,\mathbb{Z}}(f)$; aquest cos s'anomena el cos de classes de l'ordre $\mathcal{O}$. Si denotem per L aquest cos de classes, se satisfà que l'extensió $L|K$ és abeliana i que $\mathrm{Gal}(L|K) \simeq \mathbf{Cl}(\mathcal{O})$, l'isomorfisme donat pel símbol d'Artin.

Notem que, en particular, d'aquesta manera també obtenim la finitud del grup de classes $\mathbf{Cl}(\mathcal{O})$, ja que el grup quocient $\dfrac{\mathbf{I}_K(f)}{\mathbf{P}_{K,1}(f)}$ és finit. De fet, se satisfà el resultat següent.

Proposició 3.4.8. *Sigui L el cos de classes d'un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K. Llavors, l'extensió $L|\mathbb{Q}$ és de Galois, i el grup de Galois $\mathrm{Gal}(L|\mathbb{Q})$ és el producte semidirecte de $\mathrm{Gal}(L|K) \simeq \mathbf{Cl}(\mathcal{O})$ per un grup cíclic d'ordre 2, on l'element no trivial de C_2 actua en $\mathrm{Gal}(L|K)$ en la forma $\sigma \mapsto \sigma^{-1}$.* □

Recordem que un grup s'anomena diedral generalitzat si és extensió d'un grup cíclic d'ordre 2 per un grup abelià, no necessàriament cíclic. Com a conseqüència, disposem de la noció d'extensió diedral generalitzada.

Teorema 3.4.9. *Sigui K un cos quadràtic imaginari. Una extensió abeliana $L|K$ és diedral generalitzada sobre $\mathbb{Q}$ si, i només si, L és subcòs del cos de classes d'algun ordre de K.* □

Observació 3.4.10. *Donat un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K, el cos de classes de l'ordre $\mathcal{O}$ duu associat un conductor en el sentit de la teoria*

de cossos de classes; aquest conductor, $\mathfrak{f}(L|K)$ coincideix, gairebé sempre, amb el conductor f de l'ordre $\mathcal{O}$; però hi ha alguns casos en què això no és així. Més concretament:

$$\mathfrak{f}(L|K) = \begin{cases} \mathcal{O}_K, & \textit{si } f = 2, 3, \ \textit{i } K = \mathbb{Q}(\sqrt{-3}); \\ \mathcal{O}_K, & \textit{si } f = 2, \ \textit{i } K = \mathbb{Q}(\sqrt{-1}); \\ \dfrac{f}{2}\mathcal{O}_K, & \textit{si } f = 2f', \ f' \textit{ senar,} \\ & \textit{i } 2 \textit{ descompon completament en } \mathcal{O}_K; \\ f\mathcal{O}_K, & \textit{altrament.} \end{cases}$$

3.5 Demostració del teorema

Recordem l'enunciat del teorema que volem provar.

Teorema 3.5.1. *Siguin $\mathcal{O}$ un ordre d'un cos quadràtic imaginari K i $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionari invertible de K. Llavors, l'invariant j de $\mathfrak{a}$, $j(\mathfrak{a})$, és un nombre enter algebraic i el cos de classes de l'ordre $\mathcal{O}$ és el cos $K(j(\mathfrak{a}))$.*

Demostració. Començarem per veure que $j(\mathfrak{a})$ és un enter algebraic.
• Afirmem que existeix un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, primitiu de $\mathcal{O}$ i tal que $m := \mathrm{N}(\alpha)$ no és un quadrat (cf. la **definició 1.27**).

En efecte; siguin $\mathcal{O}_K$ l'anell dels enters de K, D el seu discriminant, $\omega_D := \dfrac{D+\sqrt{D}}{2}$, i f el conductor de l'ordre $\mathcal{O}$. Llavors, $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z} f\omega_D$ (cf. la **proposició 1.2**, (b)); a més a més, $\alpha := f\omega_D \in \mathcal{O}$ és un element primitiu de $\mathcal{O}$, perquè forma part d'una $\mathbb{Z}$-base de $\mathcal{O}$. Finalment, $m := \mathrm{N}(\alpha) = \mathrm{N}(f\omega_D)$ no és un quadrat, ja que, si designem per $x \mapsto x'$ l'automorfisme no trivial de K, el càlcul de la norma de $f\omega_D$ ens proporciona la igualtat

$$\mathrm{N}(f\omega_D) = f^2\omega_D\omega'_D = f^2\frac{D^2-D}{4} = f^2\frac{D(D-1)}{4};$$

i, com que $\mathrm{mcd}(D, D-1) = 1$ i D no és un quadrat, el producte $D(D-1)$ no pot ser un quadrat. •

Sigui, doncs, $\alpha \in \mathcal{O}$, $\alpha \neq 0$, un element primitiu de $\mathcal{O}$ tal que $m := \mathrm{N}(\alpha)$ no és un quadrat.

D'una banda, i com que m no és un quadrat, el polinomi $\Phi_m(X, X) \in \mathbb{Z}[X]$ és de grau > 1 i el seu coeficient dominant és ± 1 (cf. la **proposició 3.13**). D'altra banda, com que $\mathfrak{a}$ és un $\mathcal{O}$-ideal fraccionari propi de K i $\alpha \in \mathcal{O}$ és un element primitiu de $\mathcal{O}$, el grup abelià quocient $\dfrac{\mathfrak{a}}{\alpha\mathfrak{a}}$ és cíclic

d'ordre $\mathrm{N}(\alpha) = m$ (cf. el **corol·lari 1.29**). Com que $\mathfrak{a}$ i $\alpha\mathfrak{a}$ són xarxes de $\mathbb{C}$, la **proposició 3.18** ens ensenya que $\Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0$. A més a més, com que $\mathfrak{a}$ i $\alpha\mathfrak{a}$ són dues xarxes homotètiques, el **teorema 2.13** ens diu que és $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$, de manera que $\Phi_m(j(\mathfrak{a}), j(\mathfrak{a})) = 0$ i $j(\mathfrak{a})$ és un enter algebraic.

A continuació, i si L designa el cos de classes de l'ordre $\mathcal{O}$, i $M := K(j(\mathfrak{a}))$, cal veure que $L = M$.

Sigui $\mathcal{S}_{L|\mathbb{Q}}$ el conjunt dels primers de $\mathbb{Z}$ que descomponen completament en L (cf. la **definició 4.5**).

Una de les propietats principals dels cossos de classes dels ordres és que els primers de $\mathbb{Q}$ que hi descomponen completament són, llevat possiblement d'un conjunt finit d'excepcions, els primers representats per la forma nòrmica de l'ordre $\mathcal{O}$; és a dir, llevat d'un conjunt finit (en cada costat), el conjunt $\mathcal{S}_{L|\mathbb{Q}}$ coincideix amb el conjunt

$$\{p \text{ primer de } \mathbb{Z} : \ p = \mathrm{N}(\alpha), \ \text{ per a algun } \alpha \in \mathcal{O}\}. \tag{3.1}$$

Com que l'extensió $L|\mathbb{Q}$ és de Galois, i si tenim en compte la **proposició 4.7**, (a), per a demostrar que $M \subseteq L$ és suficient provar que tot element de $\mathcal{S}_{L|\mathbb{Q}}$, llevat potser d'un conjunt finit, pertany a $\mathcal{S}_{M|\mathbb{Q}}$; vegem, doncs, això.

Sigui $p \in \mathcal{S}_{L|\mathbb{Q}}$ qualsevol primer i suposem que p és no ramificat en $M|\mathbb{Q}$; com que la quantitat de primers que ramifiquen en qualsevol extensió és finita, això exclou, com a màxim, una quantitat finita d'elements de $\mathcal{S}_{L|\mathbb{Q}}$.

En virtut de (3.1), i llevat d'un conjunt finit de primers $p \in \mathcal{S}_{L|\mathbb{Q}}$, existeix $\alpha \in \mathcal{O}$, $\alpha \neq 0$, tal que $p = \mathrm{N}(\alpha)$. Llavors, el grup abelià quocient $\dfrac{\mathfrak{a}}{\alpha\mathfrak{a}}$ és finit d'ordre $p = \mathrm{N}(\alpha)$ i, en conseqüència, és cíclic. Per tant, tenim la igualtat

$$\Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0.$$

Ara, fem servir les congruències de Kronecker (cf. el **teorema 3.16**); existeix $\beta \in \mathcal{O}_M$ tal que

$$(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 = p\beta.$$

Si $\mathfrak{P} \subseteq \mathcal{O}_M$ és un primer de $\mathcal{O}_M$ que divideix p, obtenim que

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}.$$

• Afirmem que:

i) $\mathcal{O}_K[j(\mathfrak{a})] \subseteq \mathcal{O}_M$ i és un subgrup d'índex finit.

ii) Si p no divideix l'índex $[\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, la congruència $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$ implica que $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, per a tot element $\alpha \in \mathcal{O}_M$.

En efecte; com que $M = K(j(\mathfrak{a}))$ i $j(\mathfrak{a}) \in \mathcal{O}_M$, és clar que $\mathcal{O}_K[j(\mathfrak{a})] \subseteq \mathcal{O}_M$; i, a més a més, el grup abelià quocient és finit, perquè tots dos són grups abelians lliures de la mateixa dimensió $[M : \mathbb{Q}]$. Això demostra (i).

D'altra banda, com que p descompon completament en L, també descompon completament en K; si $\mathfrak{p} := \mathfrak{P} \cap K$, tenim que $\mathfrak{p}$ és un ideal de $\mathcal{O}_K$ de norma p, de manera que per a tot $\alpha \in \mathcal{O}_K$ és $\alpha^p \equiv \alpha \pmod{\mathfrak{p}}$. I, com que $\mathfrak{P}$ divideix $\mathfrak{p}$, és $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, per a tot $\alpha \in \mathcal{O}_K$. Com que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$, tenim que per a tot element $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$ és $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$.

L'extensió d'aquesta propietat a tot $\mathcal{O}_M$ és immediata a partir del fet que p no divideix $n := [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$. Com que $n\mathcal{O}_M \subseteq \mathcal{O}_K[j(\mathfrak{a})]$, tenim que per a tot $\alpha \in \mathcal{O}_M$ és $n\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$, de manera que $n^p\alpha^p \equiv n\alpha \pmod{\mathfrak{P}}$; i, com que $\mathfrak{P}$ divideix p i p no divideix n, és $n^p \equiv n \pmod{\mathfrak{P}}$; això fa que sigui $n\alpha^p \equiv n\alpha \pmod{\mathfrak{P}}$ i, com que n és invertible mòdul $\mathfrak{P}$, que sigui $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, per a tot $\alpha \in \mathcal{O}_M$, com volíem veure. •

Ara, de (ii) se segueix que, per a tot primer $\mathfrak{P} \subseteq \mathcal{O}_M$ que divideix p, i si $f(\mathfrak{P}|p)$ designa el grau residual, sigui $f(\mathfrak{P}|p) = 1$; i, com que p no ramifica en M, p descompon completament en $\mathcal{O}_M$. Així, obtenim que, llevat d'un conjunt finit, tots els primers de $\mathcal{S}_{L|\mathbb{Q}}$ pertanyen a $\mathcal{S}_{M|\mathbb{Q}}$ i, en conseqüència, és $M \subseteq L$.

Conèixer aquesta inclusió és important per a la resta de la prova. Efectivament, la inclusió $M = K(j(\mathfrak{a})) \subseteq L$ ens ensenya que el cos de classes L conté l'invariant $j(\mathfrak{a})$; i, com que $\mathfrak{a}$ és qualsevol $\mathcal{O}$-ideal fraccionari propi de K, L conté l'invariant $j(\mathfrak{b})$, per a tots els $\mathcal{O}$-ideals fraccionaris propis $\mathfrak{b}$ de K. Sigui $h := h(\mathcal{O})$ el nombre de classes de l'ordre $\mathcal{O}$, i siguin $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ representants de les classes de $\mathbf{Cl}(\mathcal{O})$. Llavors, $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ són diferents i, per a tot $\mathcal{O}$-ideal fraccionari propi $\mathfrak{b}$ de K, $j(\mathfrak{b})$ és un dels nombres $j(\mathfrak{a}_i)$ (cf. el **teorema 2.13** i el **corol·lari 2.16**). Com a conseqüència,

$$\Delta := \prod_{1 \le i < j \le h} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$$

és un element no nul de $\mathcal{O}_L$.

Ara, per a provar la inclusió contrària, $L \subseteq M$, usarem el criteri que, llevat d'un conjunt finit, $\tilde{\mathcal{S}}_{M|\mathbb{Q}} \subseteq \mathcal{S}_{L|\mathbb{Q}}$, on $\tilde{\mathcal{S}}_{M|\mathbb{Q}}$ és el conjunt dels primers p de $\mathbb{Q}$ no ramificats en $\mathcal{O}_M$ i que són divisibles per algun primer $\mathfrak{P}$ de M de grau residual 1 (cf. la **proposició 4.7**, (b)).

Sigui, doncs, $p \in \tilde{\mathcal{S}}_{M|\mathbb{Q}}$; és a dir, p és no ramificat en M i existeix algun primer $\mathfrak{P}$ de $\mathcal{O}_M$ que divideix p i tal que $f(\mathfrak{P}|p) = 1$. En particular, com

que $K|\mathbb{Q}$ és de Galois, p descompon completament en K i, en conseqüència, $p = \mathrm{N}(\mathfrak{p})$ per a algun ideal primer $\mathfrak{p} \subseteq \mathcal{O}_K$ que divideix p (podem prendre $\mathfrak{p} := \mathfrak{P} \cap K$). Si ens limitem a considerar els ideals p primers amb el conductor $f := [\mathcal{O}_K : \mathcal{O}]$, fet que exclou, com a màxim, una quantitat finita d'ideals primers de $\mathbb{Z}$ i, en conseqüència, un conjunt finit de primers de L, que podríem afegir a $\mathcal{S}_{L|\mathbb{Q}}$, obtenim que $\mathfrak{p} \cap \mathcal{O} \subseteq \mathcal{O}$ és un ideal primer de $\mathcal{O}$ primer amb f i que $\mathrm{N}(\mathfrak{p} \cap \mathcal{O}) = p$.

Ara, si podem demostrar que $\mathfrak{p} \cap \mathcal{O}$ és un ideal principal $\alpha\mathcal{O}$, llavors, $p = \mathrm{N}(\alpha)$ implica que $p \in \mathcal{S}_{L|\mathbb{Q}}$, en virtut del criteri (3.1) de més amunt, i haurem acabat.

Notem que, de nou, podem excloure de consideració una quantitat finita de primers; en particular, podem suposar que p és coprimer amb Δ. Posem $\mathfrak{a}' := (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. Com que $\mathrm{N}(\mathfrak{p} \cap \mathcal{O}) = p$, el grup abelià quocient $\dfrac{\mathfrak{a}}{\mathfrak{a}'}$ és cíclic d'ordre p. Per tant, tenim que $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$ (cf. la **proposició 3.18**). De nou, en virtut de la congruència de Kronecker, existeix un polinomi $Q(X,Y) \in \mathbb{Z}[X,Y]$ tal que

$$(j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a})) = 0.$$

Sigui $\tilde{\mathfrak{P}}$ un primer de L que divideix $\mathfrak{P}$. Com que $j(\mathfrak{a}')$ i $j(\mathfrak{a})$ pertanyen a $\mathcal{O}_L$, tenim que $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \tilde{\mathfrak{P}}$; en conseqüència, se satisfà almenys una de les congruències

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}, \qquad j(\mathfrak{a}') \equiv j(\mathfrak{a})^p \pmod{\tilde{\mathfrak{P}}}.$$

D'altra banda, com que $f(\mathfrak{P}|p) = 1$, tenim que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$; i, com que $\tilde{\mathfrak{P}}$ divideix $\mathfrak{P}$, obtenim que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}$. Ara, com que $\tilde{\mathfrak{P}}$ és de característica residual p, aquesta condició, juntament amb (2), ens ensenyen que $j(\mathfrak{a}') \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}$.

Si $\mathfrak{a}$ i $\mathfrak{a}'$ definissin classes diferents de $\mathbf{Cl}(\mathcal{O})$, llavors $j(\mathfrak{a}) - j(\mathfrak{a}')$ seria un dels factors de la definició de Δ i p no seria primer amb Δ, com hem suposat; per tant, $\mathfrak{a}$ i $\mathfrak{a}'$ pertanyen a la mateixa classe en $\mathbf{Cl}(\mathcal{O})$; és a dir, i com que $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$, l'ideal $\mathfrak{p} \cap \mathcal{O}$ és principal. Això acaba la demostració. □

3.6 Complements

En aquesta secció, enunciarem dos tipus de resultats que complementen el **teorema 0.1**. D'una banda, proporcionarem la llei de reciprocitat associada al cos de classes d'un ordre d'un cos quadràtic imaginari. D'altra banda, ens ocuparem dels cossos de classes radials de conductors enters dels cossos quadràtics imaginaris.

De manera semblant a com el teorema de Kronecker-Weber ens proporciona generadors de les extensions abelianes maximals de $\mathbb{Q}$ de conductors donats, el **teorema 0.1** ens proporciona un generador del cos de classes d'un ordre $\mathcal{O}$ d'un cos quadràtic imaginari. En el cas particular de l'ordre màxim, aquest cos és el cos de classes de Hilbert; doncs, obtenim el resultat següent.

Corol·lari 3.6.1. *Siguin K un cos quadràtic imaginari i $\mathcal{O}_K \subseteq K$ l'anell dels enters de K. El cos de classes de Hilbert de K és el cos $K(j(\mathcal{O}_K))$.* $\square$

A més a més, com a conseqüència del **teorema 0.1** i del **teorema 4.9**, obtenim el resultat següent.

Corol·lari 3.6.2. *Siguin K un cos quadràtic imaginari i $L|K$ una extensió finita. Llavors, $L|K$ és una extensió abeliana i $L|\mathbb{Q}$ és diedral generalitzada si, i només si, existeix un ordre $\mathcal{O} \subseteq K$ tal que $L \subseteq K(j(\mathcal{O}))$.* $\square$

Així com el teorema de Kronecker-Weber ens proporciona la llei de reciprocitat per a les extensions ciclotòmiques de $\mathbb{Q}$, és a dir, l'acció dels Frobenius sobre les arrels de la unitat, també es pot donar l'acció del grup de Galois del cos de classes de l'ordre $\mathcal{O}$ sobre el generador $j(\mathfrak{a})$ de l'extensió $L|K$; és donada per la llei de reciprocitat següent, sobre els generadors diferents $j(\mathfrak{a})$ del cos de classes.

Teorema 3.6.3. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i L el cos de classes de l'ordre $\mathcal{O}$. Si $\mathfrak{a} \subseteq K$ és un $\mathcal{O}$-ideal fraccionari propi i $\mathfrak{p} \subseteq \mathcal{O}_K$ és un $\mathcal{O}_K$-ideal enter primer, llavors*

$$\left(\frac{L|K}{\mathfrak{p}}\right)(j(\mathfrak{a})) = j((\overline{\mathfrak{p} \cap \mathcal{O}})\mathfrak{a}). \ \square$$

Aquest resultat es pot enunciar, en termes del grup de classes $\mathbf{Cl}(\mathcal{O})$, de la manera següent.

Corol·lari 3.6.4. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i L el cos de classes de l'ordre $\mathcal{O}$. Donats $\mathcal{O}$-ideals fraccionaris propis $\mathfrak{a}, \mathfrak{b} \subseteq K$, definim $\sigma_{\mathfrak{a}}(j(\mathfrak{b})) := j(\mathfrak{a}^{-1}\mathfrak{b})$. Llavors, $\sigma_{\mathfrak{a}}$ és un element de $\mathrm{Gal}(L|K)$ i l'assignació $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ indueix un isomorfisme $\mathbf{Cl}(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(L|K)$.* $\square$

Funcions de Weber. Un cop donats els cossos de classes dels ordres dels cossos quadràtics imaginaris, ens podem preguntar pels cossos de classes radials de K de conductor enter.

Donada una xarxa $L \subseteq \mathbb{C}$, la funció de Weber $\tau(z;L)$, associada a la xarxa L, és definida per

$$\tau(z;L) := \begin{cases} \dfrac{g_2(L)^2}{\Delta(L)}\wp(z;L)^2, & \text{si } g_3(L)=0; \\ \dfrac{g_3(L)}{\Delta(L)}\wp(z;L)^3, & \text{si } g_2(L)=0; \\ \dfrac{g_2(L)g_3(L)}{\Delta(L)}\wp(z;L) & \text{altrament.} \end{cases}$$

La propietat més important i, d'altra banda, immediata, de les funcions $\tau(z;L)$ de Weber és el seu comportament en les classes d'homotècia de xarxes.

Lema 3.6.5. *Siguin $L \subseteq \mathbb{C}$ una xarxa i $\lambda \in \mathbb{C}$, $\lambda \neq 0$ un nombre complex no nul, qualssevol. Llavors, $\tau(\lambda z;\lambda L) = \tau(z;L)$, per a tot $z \in \mathbb{C}$.* □

Teorema 3.6.6. *Siguin K un cos quadràtic imaginari, d_K el discriminant de K, i $N \in \mathbb{Z}$, $N > 0$, un nombre enter. Llavors:*

a) El cos $K(j(\mathcal{O}_K), \tau(1/N;\mathcal{O}_K))$ és el cos de classes radial per al mòdul $N\mathcal{O}_K$.

b) Si $\mathcal{O} \subseteq K$ és l'ordre de K de conductor N i posem, $\omega_K := \dfrac{d_K + \sqrt{d_K}}{2}$, el cos de classes radial per al mòdul $N\mathcal{O}_K$ és el cos $K(j(\mathcal{O}), \tau(\omega_K;\mathcal{O}_K))$. □

Així, el cos de classes radial de K per al mòdul $N > 0$ és generat, sobre el cos de classes de Hilbert de K, pel valor de la funció de Weber en un punt de N-divisió de la xarxa $\mathcal{O}_K$; o bé, sobre el cos de classes de l'ordre $\mathcal{O}$ de conductor N, pel valor de la funció de Weber en el generador ω_K de l'anell d'enters $\mathcal{O}_K$ de K.

Notem que, en qualsevol cas, obtenim el cos de classes radial de conductor N del cos quadràtic imaginari K en considerar la xarxa $\mathbb{Z} \oplus \mathbb{Z}\omega_K$ i afegir els valors de dues funcions en dos punts; la funció j en un generador de la xarxa i la funció de Weber en un punt de N-divisió (el punt $1/N$), en el primer cas; o bé a l'inrevés, el valor de la funció de Weber en un generador de la xarxa i el de la funció j en un punt de N-divisió de la xarxa $\mathcal{O}_K$ (notem que $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}N\omega_K$), en el segon.

3.7 L'equació de les classes

El **teorema 0.1** ens diu que si $\mathcal{O}$ és un ordre d'un cos quadràtic imaginari, el cos de classes de l'ordre $\mathcal{O}$ és $K(j(\mathfrak{a}))$, on $\mathfrak{a}$ és qualsevol $\mathcal{O}$-ideal fraccionari

propi de K; així, el teorema ens proporciona un generador del cos. Per exemple, podem prendre $\mathfrak{a} = \mathcal{O}$, de manera que el cos de classes de l'ordre $\mathcal{O}$ és el cos $K(j(\mathcal{O}))$. Es tracta d'estudiar una mica més els nombres algebraics $j(\mathfrak{a})$.

Lema 3.7.1. *Siguin K un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ un ordre de K. Llavors, $j(\mathcal{O})$ és un nombre real.*

DEMOSTRACIÓ. Com que la conjugació complexa és un automorfisme de $\mathcal{O}$, tenim que $\mathcal{O} \subseteq \mathbb{C}$ és una xarxa invariant per a la conjugació complexa. Ara bé, de les definicions de les funcions $g_2(L)$ i $g_3(L)$ (cf. la **proposició 2.5**), per a una xarxa arbitrària $L \subseteq \mathbb{C}$, tenim que, si L' denota la xarxa que s'obté de L en aplicar la conjugació complexa, $g_2(L')$ i $g_2(L)$ són nombres complexos conjugats i, anàlogament, $g_3(L')$ i $g_3(L)$ són nombres complexos conjugats; en conseqüència, $j(L')$ i $j(L)$ també són nombres complexos conjugats. Si apliquem això a la xarxa $L = \mathcal{O} = L'$, obtenim que $j(\mathcal{O})$ és invariant per a la conjugació complexa i, en conseqüència, $j(\mathcal{O}) \in \mathbb{R}$. □

A més a més, sabem que $j(\mathcal{O})$ és un nombre enter algebraic; per tant, el seu polinomi minimal sobre $\mathbb{Q}$ és de coeficients enters.

Definició 3.7.2. *Siguin K un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ un ordre qualsevol de K. Sigui $H_{\mathcal{O}}(X) \in \mathbb{Z}[X]$ el polinomi mònic irreductible que té $j(\mathcal{O})$ com a arrel; és a dir, el polinomi minimal de $j(\mathcal{O})$ sobre $\mathbb{Q}$. El polinomi $H_{\mathcal{O}}(X)$, o l'equació $H_{\mathcal{O}}(X) = 0$, s'anomena l'equació de les classes de $\mathcal{O}$. Com que $\mathcal{O} = \mathcal{O}_D$, on D és el discriminant de $\mathcal{O}$, sovint s'escriu $H_D(X)$ en lloc de $H_{\mathcal{O}}(X)$.*

Proposició 3.7.3. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K, $h := h(\mathcal{O}) := \#\mathbf{Cl}(\mathcal{O})$ el nombre de classes de $\mathcal{O}$, i $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ representants de les classes de $\mathbf{Cl}(\mathcal{O})$. Llavors,*

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)). \ \square$$

Corol·lari 3.7.4. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i $\mathfrak{a} \subseteq K$ un $\mathcal{O}$-ideal fraccionari propi de $\mathcal{O}$. Llavors, el polinomi minimal de $j(\mathfrak{a})$ sobre $\mathbb{Q}$ és $H_{\mathcal{O}}(X)$.* □

Les equacions de les classes ens permeten factoritzar els polinomis $\Phi_m(X, X)$. Per a això, tenim el resultat següent.

Lema 3.7.5. *Sigui $m \in \mathbb{Z}$, $m > 1$, i considerem el polinomi $\Phi_m(X, X)$.*

a) Si $q(X) \in \mathbb{Z}[X]$ és un polinomi mònic irreductible que divideix el polinomi $\Phi_m(X,X)$, existeixen un cos quadràtic imaginari K i un ordre $\mathcal{O} \subseteq K$ que conté un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, primitiu de norma $\mathrm{N}(\alpha) = m$, tals que $q(X) = H_{\mathcal{O}}(X)$.

b) Recíprocament, si K és un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ és un ordre per al qual existeix un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, primitiu de norma $\mathrm{N}(\alpha) = m$, llavors $H_{\mathcal{O}}(X)$ és un factor irreductible de $\Phi_m(X,X)$.

DEMOSTRACIÓ. Sigui β una arrel de $q(X)$; llavors, és $\Phi_m(\beta,\beta) = 0$. La **proposició 3.18** ens diu que existeixen xarxes $L' \subseteq L \subseteq \mathbb{C}$ tals que $j(L') = j(L) = \beta$ i que el grup abelià quocient L/L' és cíclic d'ordre m; el **teorema 2.13** ens diu, ara, que existeix $\alpha \in \mathbb{C}$, $\alpha \neq 0$, tal que $L' = \alpha L$; en particular, α pertany a l'anell de multiplicadors de la xarxa L, i $\alpha \notin \mathbb{Z}$, perquè L/L' és cíclic. En virtut del **teorema 2.15**, existeix un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K tal que $\alpha \in \mathcal{O}$, i, a més a més, les xarxes $L' \subseteq L$ són homotètiques a $\mathcal{O}$-ideals fraccionaris propis $\mathfrak{a}' \subseteq \mathfrak{a}$ de K; el fet que sigui $j(\mathfrak{a}) = j(L) = \beta$ ens diu que $q(X)$ és el polinomi minimal de $j(\mathfrak{a})$; és a dir, $q(X) = H_{\mathcal{O}}(X)$; això demostra la primera afirmació.

Recíprocament, sigui $\alpha \in \mathcal{O}$, $\alpha \neq 0$, un element primitiu de norma $\mathrm{N}(\alpha) = m$; llavors, $\mathcal{O}/\alpha\mathcal{O}$ és cíclic d'ordre m (cf. el **corol·lari 1.29**) i, en conseqüència, $\Phi_m(j(\mathcal{O}), j(\mathcal{O})) = \Phi_m(j(\alpha\mathcal{O}), j(\mathcal{O})) = 0$ (cf. la **proposició 3.18**). Així, $j(\mathcal{O})$ és una arrel del polinomi $\Phi_m(X,X)$, de manera que $H_{\mathcal{O}}(X) = \mathrm{Irr}(j(\mathcal{O}), K)$ divideix $\Phi_m(X,X)$. $\square$

A fi d'obtenir la factorització completa dels polinomis $\Phi_m(X,X)$, ens cal, encara, obtenir la multiplicitat de les equacions de les classes per a cada ordre $\mathcal{O}$ de cada cos quadràtic imaginari.

Definició 3.7.6. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre i $m > 1$ un nombre enter. Escriurem*

$$r(\mathcal{O}, m) := \#\frac{\{\alpha \in \mathcal{O} : \alpha \text{ és primitiu i } \mathrm{N}(\alpha) = m\}}{\mathcal{O}^*}.$$

Notem que el conjunt d'unitats de $\mathcal{O}$ és finit i que també ho és el conjunt d'elements de $\mathcal{O}$ de norma donada.

En efecte, les unitats són els elements de norma 1; i els elements de norma $m > 0$ són donats per les solucions (a,b) de l'equació diofantina

$$(a + bf\omega_K)(a + bf\omega'_K) = m,$$

on $x \mapsto x'$ indica la conjugació complexa o, equivalentment, l'automorfisme

no trivial de K. Aquesta equació es pot escriure en la forma

$$\begin{aligned} m &= (a+bf\omega_K)(a+bf\omega'_K) \\ &= a^2+b^2f^2\omega_K\omega'_K+abf(\omega_K+\omega'_K) \\ &= a^2+b^2f^2\frac{d_K(d_K-1)}{4}+abfd_K; \end{aligned}$$

és a dir, en la forma

$$4m=(2a+bfd_K)^2-d_K(bf)^2.$$

Ara, només cal tenir en compte que el discriminant d_K de K és un nombre enter negatiu, de manera que $|b|$ és fitat i, en conseqüència, només pot prendre una quantitat finita de valors enters; i, per tant, a només pot prendre una quantitat finita de valors enters.

Observació 3.7.7. *A més a més, si $r(\mathcal{O},m)\neq 0$; és a dir, si tenim un element primitiu de norma $m>1$, ha de ser $b\neq 0$, i la igualtat $4m=(2a+bfd_K)^2-d_K(bf)^2$ ens diu que el valor del discriminant d_K és fitat. Per tant, obtenim el resultat següent.*

Proposició 3.7.8. *Fixat un nombre $m>1$, la quantitat d'ordres $\mathcal{O}$ de cossos quadràtics imaginaris tals que $r(\mathcal{O},m)>0$ és finita.* □

Finalment, podem enunciar el resultat que ens proporciona la factorització dels polinomis $\Phi_m(X,X)$.

Teorema 3.7.9. *Sigui $m\in\mathbb{Z}$, $m>1$. Existeix un nombre complex $c_m\in\mathbb{C}$, $c_m\neq 0$, tal que*

$$\Phi_m(X,X)=c_m\prod_{\mathcal{O}}H_{\mathcal{O}}(X)^{r(\mathcal{O},m)},$$

on $\mathcal{O}$ recorre tots els ordres de tots els cossos quadràtics imaginaris. □

Això no és suficient, encara, per a obtenir l'equació de les classes per a un ordre donat. En efecte; donat l'ordre $\mathcal{O}$ o, equivalentment, el seu discriminant, un element primitiu qualsevol $\alpha\in\mathcal{O}$, $\alpha\neq 0$, ens proporciona un valor $m:=\mathrm{N}(\alpha)$ per al qual el polinomi $H_{\mathcal{O}}(X)$ és un divisor irreductible de $\Phi_m(X,X)$. Però, quin dels divisors irreductibles, si $\Phi_m(X,X)$ en té més d'un?

A fi de respondre aquesta darrera qüestió, s'introdueix el polinomi $\Phi_{m,1}(X,X)$ com el producte dels factors irreductibles de $\Phi_m(X,X)$ que són de multiplicitat 1; és a dir,

$$\Phi_{m,1}(X,X):=\prod_{r(D,m)=1}H_D(X).$$

Se satisfà la propietat següent.

Proposició 3.7.10. *Sigui $m > 1$ un nombre enter. Llavors,*

$$\Phi_{m,1}(X,X) = \begin{cases} H_{-4}(X)H_{-8}(X), & \textit{si } m = 2; \\ H_{-m}(X)H_{-4m}(X), & \textit{si } m \equiv 3 \pmod 4 \textit{ i } m \neq 3k^2, \\ & \textit{per a tot } k > 1; \\ H_{-4m}(X), & \textit{si } m > 2 \textit{ i } m \not\equiv 3 \pmod 4, \\ & \textit{o bé } m = 3k^2,\ k > 1. \square \end{cases}$$

El resultat anterior ens permet acabar el càlcul algorítmic de l'equació de les classes $H_D(X)$, per a gairebé tots els discriminants $D < 0$, però no per a tots (cf. [Co 89](p292–293).

Comencem per observar que, si posem $f(X) := \Phi_m(X,X)$, llavors el polinomi $g(X) := \dfrac{f(X)}{\mathrm{mcd}(f(X), f'(X))}$ és el producte de tots els factors irreductibles de $f(X)$, però tots apareixen, en $g(X)$, amb multiplicitat 1; llavors, tenim que $\Phi_{m,1}(X,X) = \dfrac{g(X)}{\mathrm{mcd}(g(X), f'(X))}$. Per tant, el càlcul de $\Phi_{m,1}(X,X)$ a partir del polinomi modular $\Phi_m(X,Y)$ no comporta cap problema.

Però, quin polinomi modular cal considerar? La proposició ens dóna una resposta parcial. Sigui $D < 0$ un discriminant negatiu qualsevol. Suposem, en primer lloc, que $D \equiv 0 \pmod 4$; això és, $D = -4m$, amb $m \geq 1$. Llavors,

$$H_D(X) = \begin{cases} H_{-4}(X) = X - 1728, & \text{si } m = 1, \\ H_{-8}(X) = X - 8000, & \text{si } m = 2, \\ H_{-12}(X) = X - 54000, & \text{si } m = 3, \\ H_{-4m}(X) = \Phi_{m,1}(X,X), & \text{si } m > 3 \text{ i } m \not\equiv 3 \pmod 4, \\ H_{-4m}(X) = \Phi_{m,1}(X,X), & \text{si } m > 3,\ m \equiv 3 \pmod 4 \\ & \text{i } m = 3k^2,\ k > 1. \end{cases}$$

Resten els casos en què és $m > 3$, $m \equiv 3 \pmod 4$, però $m \neq 3k^2$ per a tot nombre enter $k > 1$. En aquests casos, tenim que

$$\Phi_{m,1}(X,X) = H_{-m}(X)H_{-4m}(X) = H_{D/4}(X)H_D(X).$$

Per a distingir quin dels dos factors de $\Phi_{m,1}(X,X)$ és el factor que volem, observem que, si $m \equiv 3 \pmod 8$, la fórmula que relaciona els nombres de classes per a $D = -4m$ i $D = -m$ (cf. el **corol·lari 1.26**) ens diu que $h(-4m) = 3h(-m)$, de manera que els dos factors de $\Phi_{m,1}(X,X)$ són

de graus diferents. Però si $m \equiv 7 \pmod 8$, els dos nombres de classes coincideixen, de manera que no podem distingir els factors pel seu grau. En aquest cas, però, se satisfà que

$$H_{-m}(X) = \mathrm{mcd}(\Phi_{m,1}(X,X), \Phi_{(m+1)/4}(X,X)),$$

i això permet acabar el càlcul de $H_D(X)$ en el cas $m > 3$.

Estudiem, ara, el cas en què $D \equiv 1 \pmod 4$; això és, $D = -m$, amb $m \geq 3$, $m \equiv 3 \pmod 4$. Si $m = 3$, tenim que $H_D(X) = H_{-3}(X) = X$; i si $m > 3$, però $m \neq 3k^2$ per a tot nombre enter $k > 1$, tenim que

$$\Phi_{m,1}(X,X) = H_{-m}(X)H_{-4m}(X) = H_D(X)H_{4D}(X),$$

i es distingeix com més amunt.

Però els casos $m = 3k^2$, amb $k > 1$, senar, no són coberts per cap dels casos anteriors.

En efecte; suposem que $D = -3k^2$, amb $k > 1$, senar. Sigui $\alpha \in \mathcal{O} := \mathcal{O}_D$ un element primitiu de norma $\mathrm{N}(\alpha) =: m > 1$, i posem $\alpha = a + b\dfrac{k + k\sqrt{-3}}{2}$. Llavors, tenim que $4\,\mathrm{N}(\alpha) = (2a + kb)^2 + 3k^2b^2$. Si b dóna lloc a una solució α tal que $\alpha \in \mathcal{O}$ és un element primitiu, ha de ser $b \neq 0$. Si, a més a més, suposem que és $2a + kb \neq 0$, i posem $x \in \mathbb{Z}$ tal que $x^2 = 4\,\mathrm{N}(\alpha) - 3k^2b^2 = (2a + kb)^2 \neq 0$, obtenim les quatre solucions

$$(a,b) \in \left\{ \left(\frac{x - kb}{2}, b\right), \left(\frac{-x - kb}{2}, b\right), \left(\frac{-x + kb}{2}, -b\right), \left(\frac{x + kb}{2}, -b\right) \right\},$$

i totes elles donen lloc a valors primitius de α, perquè k és senar. Com que $\#\mathcal{O}_D^* = 2$, perquè $k > 1$, això produeix que $r(\mathcal{O}, m) \geq 2$.

D'altra banda, si existeix algun element $\alpha \in \mathcal{O}$ primitiu de norma $\mathrm{N}(\alpha) = m$, i tal que $b \neq 0$, però $2a + kb = 0$, llavors ha de ser $b = \pm 2$, $a = \mp k$, i $m = 3k^2$. Ara bé, per a $m = 3k^2$, hi ha exactament sis elements primitius de $\mathcal{O}$ de norma m; són els elements

$$\alpha = \pm k\sqrt{-3}, \quad \pm k\frac{3 + \sqrt{-3}}{2}, \quad \pm k\frac{-3 + \sqrt{-3}}{2};$$

de manera que $r(\mathcal{O}, 3k^2) = 3$.

Com a conseqüència, no hi ha cap valor de m tal que $H_D(X)$ sigui un divisor del polinomi $\Phi_{m,1}(X,X)$.

Observació 3.7.11. *Es pot provar de manera senzilla que, per a* $D = -3k^2$, $k > 1$, *senar, i* $m = \dfrac{3k^2+1}{4}$, *és* $r(\mathcal{O}, m) = 2$. *En efecte; els únics elements de* $\mathcal{O}$ *de norma* $\dfrac{3k^2+1}{4}$ *són els* $\alpha = a + b\dfrac{k+\sqrt{-3k^2}}{2}$, *amb*

$$(a,b) \in \left\{ \left(\frac{1-k}{2}, 1\right), \left(\frac{-1-k}{2}, 1\right), \left(\frac{1+k}{2}, -1\right), \left(\frac{-1+k}{2}, -1\right) \right\},$$

i tots ells són primitius. En particular, per a $k > 1$, *senar, el polinomi* $H_{-3k^2}(X)$ *és un factor irreductible de multiplicitat exactament* 2 *del polinomi* $\Phi_{\frac{1+3k^2}{4}}(X,X)$.

Anàlogament, els únics elements primitius de $\mathcal{O}$ *de norma* k^2 *són els elements*

$$\pm k\frac{1+\sqrt{-3}}{2}, \qquad \pm k\frac{-1+\sqrt{-3}}{2},$$

de manera que $r(\mathcal{O}, k^2) = 2$ *i el polinomi* $H_{-3k^2}(X)$ *és un factor de multiplicitat exactament* 2 *del polinomi* $\Phi_{k^2}(X,X)$; *així,* $H_{-3k^2}(X)$ *és un factor de multiplicitat exactament* 2 *del polinomi* $\operatorname{mcd}(\Phi_{\frac{1+3k^2}{4}}(X,X), \Phi_{k^2}(X,X))$.

En qualsevol cas, el resultat següent ens permet acabar de dissenyar un algoritme per al càlcul de totes les equacions de les classes.

Proposició 3.7.12. *Siguin* $k > 1$ *un nombre enter senar,* $D := -3k^2$, $d < 0$ *un discriminant negatiu qualsevol, i* $\mathcal{O} := \mathcal{O}_d$ *l'ordre quadràtic de discriminant* d. *Llavors:*

a) $r(\mathcal{O}_{-3k^2}, 3k^2) = 3$.

b) $r(\mathcal{O}_{-12k^2}, 3k^2) = 1$.

c) Per a $d \neq -3, -3k^2, -12k^2$, $r(\mathcal{O}_d, 3k^2)$ *és parell.*

Demostració. Considerem l'ordre $\mathcal{O} := \mathcal{O}_d$ de discriminant d, i suposem que $\alpha := a + b\dfrac{d+\sqrt{d}}{2} \in \mathcal{O}$, $a, b \in \mathbb{Z}$, és un element primitiu de norma $\mathrm{N}(\alpha) = 3k^2$. Observem que dir que α és primitiu equival a dir que $\operatorname{mcd}(a,b) = 1$; d'altra banda, si α és primitiu, i com que $3k^2 > 1$, ha de ser $b \neq 0$. L'equació que cal considerar és

$$12k^2 = 4\,\mathrm{N}(\alpha) = (2a+bd)^2 - b^2 d. \tag{3.2}$$

Suposem, en primer lloc, que l'equació (3.2) admet alguna solució (primitiva) amb $2a + bd = 0$. Llavors, b divideix $2a$ i, com que $\operatorname{mcd}(a,b) = 1$,

és $b = \pm 1, \pm 2$. En el cas $b = \pm 2$, obtenim que $d = -3k^2$; i ja hem vist més amunt que $r(\mathcal{O}_{-3k^2}, 3k^2) = 3$. En el cas $b = \pm 1$, obtenim que $d = -12k^2$; i com que els únics elements primitius de $\mathcal{O}_d$ de norma $-3k^2$ són els elements $\pm k\sqrt{-3}$, resulta que $r(\mathcal{O}_{-12k^2}, 3k^2) = 1$; això demostra (b).

Com a conseqüència, si $d \neq -3k^2, -12k^2$, per a totes les solucions primitives de (3.2) se satisfà que $2a + bd \neq 0$; posem $x := 2a + bd$. Podem escriure aquella equació en la forma equivalent

$$12k^2 + b^2 d = x^2,$$

on $x = 2a + bd \neq 0$, de manera que $12k^2 + b^2 d$ és un enter quadrat no nul. Observem que, per a $-b$, en lloc de b, els dos valors $\pm x$ no canvien, i podem calcular els corresponents valors de a; obtenim les solucions

$$(a, b) \in \left\{ \left(\frac{x - bd}{2}, b\right) \left(\frac{-x - bd}{2}, b\right) \left(\frac{x + bd}{2}, -b\right) \left(\frac{-x + bd}{2}, -b\right) \right\};$$

de manera equivalent, obtenim que els quatre elements

$$\alpha = \frac{\pm x \pm b\sqrt{d}}{2},$$

son primitius de norma $3k^2$; i tots quatre són diferents.

Ara, raonem de la manera següent: si $d \neq -3k^2, -12k^2$, podem agrupar els elements primitius de norma $-3k^2$ de quatre en quatre; com a conseqüència, si $\#\mathcal{O}_d^* = 2$, obtenim que $r(\mathcal{O}_d, 3k^2)$ és parell. Això només deixa fora de la discussió els casos dels discriminants $d = -3$ i $d = -4$, a part, és clar, dels casos $d = -3k^2, -12k^2$, exclosos des del començament.

Ara bé, si $d = -4$, l'equació (3.2) és $12k^2 = (2a - 4b)^2 + 4b^2$ que, en dividir per 4, és equivalent a $3k^2 = (a - 2b)^2 + b^2$; però aquesta equació no té solució, ja que k és senar i, per tant, $3k^2 \equiv 3 \pmod 4$, de manera que $3k^2$ no pot ser la suma de dos quadrats. Així, $r(\mathcal{O}_{-4}, 3k^2) = 0$ que, en particular, és parell. Això acaba la demostració. □

Observació 3.7.13. *Notem que la proposició no diu res del discriminant $d = -3$. En aquest cas, es pot provar que, si $k > 1$ és senar, i divisible per 3 o bé per algun nombre primer $p \equiv -1 \pmod 3$, llavors és $r(\mathcal{O}_{-3}, 3k^2) = 0$. Però si tots els primers p que divideixen k són tals que $p \equiv 1 \pmod 3$, pot ser $r(\mathcal{O}_{-3}, 3k^2) \neq 0$. En qualsevol cas, però, això no priva d'obtenir l'algoritme que se cerca, ja que el factor $H_{-3}(X) = X$ és molt senzill de detectar en $\Phi_{3k^2}(X, X)$.*

Corol·lari 3.7.14. *Siguin $k > 1$ un nombre enter senar i $g_k(X)$ el quocient del polinomi $\Phi_{3k^2}(X, X)$ per la potència de X que el divideix. Llavors, $H_{-3k^2}(X)$ és l'únic factor irreductible de multiplicitat exactament 3 del polinomi $g_k(X)$.* $\square$

Observació 3.7.15. *Podem descriure un altre algoritme per al càlcul dels polinomis de les classes, basat en la pròpia definició. De fet, el càlcul dels valors de la funció j és possible a partir, per exemple, del desenvolupament en sèrie (cf. la secció segona). D'altra banda, es pot calcular, via la teoria de la reducció de les formes quadràtiques binàries, representants de les formes primitives de discriminant donat D; això equival a calcular un sistema de representants de les classes dels $\mathcal{O}_D$-ideals fraccionaris propis $\mathfrak{a}$ de K; i els valors de la funció j en els zeros de les formes quadràtiques són les arrels del polinomi de les classes.*

Bibliografia

[B-Gro3] Buhler, J.P; Gross, B.H., *Arithmetic on elliptic curves with complex multiplication II*, Inventiones Math. **79**, 11–29 (1985).

[Co 89] Cox, D. A.: *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, New York, 1989.

[Ja] Janusz, G. J.: *Algebraic Number Fields*, Academic Press, New York, 1973,

[La] Lang, S.: *Elliptic Functions*, Addison-Wesley, Reading, MA, 1973,

[Ne] Neukirch, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999 Traducció de N. Schappacher. Edició original: Algebraische Zahlentheorie, 1992.

[Se] Serre, J-P.: *Cours d'Arithmètique*, Presses Universitaires de France, Paris, 1977; primera edició, 1970.

Capítol 4

CM-càlculs el·líptics

J.C. Lario
Dept. de Matemàtica Aplicada 2
Universitat Politècnica de Catalunya
Pau Gargallo 5,
E-08028 Barcelona

Introducció

Donat un cos de nombres K, la descripció de les seves extensions algebraiques segueix constituint un dels objectius importants de la teoria de nombres. En brut, si $\mathcal{O}_K$ denota l'anell d'enters de K, això significa estudiar els polinomis irreductibles de $\mathcal{O}_K[x]$ i conèixer les lleis que governen les factoritzacions de les seves reduccions mòdul els ideals primers $\mathfrak{p}$ de $\mathcal{O}_K$.

La teoria de Galois proporciona, en primera instància, un instrument útil en aquesta direcció; la clausura algebraica $\overline{K}$ s'obté com a límit projectiu de les extensions normals i finites L de K:

$$\mathrm{Gal}(\overline{K}/K) \simeq \lim \mathrm{Gal}(L/K)\,.$$

La teoria de cossos de classes fa un pas més enllà quan ens restringim a l'estudi d'extensions abelianes, donant lloc a un isomorfisme

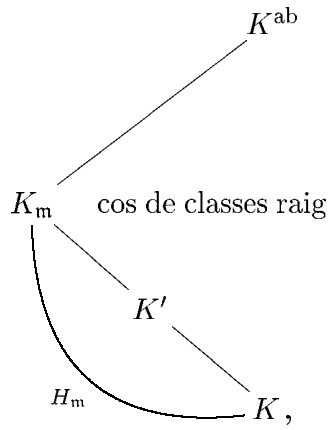
$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \lim \mathrm{Gal}(K_{\mathfrak{m}}/K)\,.$$

Els cossos $K_{\mathfrak{m}}$ s'anomenen cossos de classes raig i van associats a mòduls $\mathfrak{m}$ (essencialment ideals) del cos K. Per a cada $K_{\mathfrak{m}}$, disposem d'informació sobre la seva ramificació relativa a K, sobre descomposicions dels seus ideals

com a producte d'ideals primers, etc. Tot això es factible gràcies al morfisme d'Artin-Takagi, i s'obté així una parametrització de totes les extensions abelianes de K en termes de dades intrínseques del cos K: a cada subgrup de congruència mòdul $\mathfrak{m}$,

$$P_1(\mathfrak{m}) \subseteq H' \subseteq I(\mathfrak{m}),$$

li correspon una extensió abeliana K'/K. Recíprocament, tota extensió abeliana K'/K prové d'algun subgrup de congruència H' de manera que tenim un diagrama de cossos com segueix:



amb isomorfismes

$$\begin{aligned}
\mathrm{Gal}(K_{\mathfrak{m}}/K) &\simeq I(\mathfrak{m})/P_1(\mathfrak{m}) =: H_{\mathfrak{m}}\,;\\
\mathrm{Gal}(K'/K) &\simeq I(\mathfrak{m})/H'\,;\\
\mathrm{Gal}(K_{\mathfrak{m}}/K') &\simeq H'/P_1(\mathfrak{m})\,.
\end{aligned}$$

Per a les definicions i més detalls sobre aquesta correspondència podeu consultar les notes de P. Bayer en aquest volum. Com a casos particulars importants, destaquem:

$\mathfrak{m} = (1)$	$\mathfrak{m} = f\mathcal{O}_K$
$K_{(1)}$ cos de classes de Hilbert	K' cos de classes de l'ordre $\mathcal{O}_f$
$H_{(1)} = \mathrm{Pic}(\mathcal{O}_K)$	$\mathrm{Gal}(K'/K) = \mathrm{Pic}(\mathcal{O}_f)$

Dit això, hem d'afegir que la teoria de cossos de classes resulta insuficient si desitgem tenir informació efectiva des del punt de vista computacional sobre com construir cossos de classes raig (o cossos de classes d'ordres). En d'altres paraules, la teoria de cossos de classes no explica com construir polinomis definidors i/o elements primitius de les extensions abelianes

de K. Així com en el cas més senzill, $K = \mathbb{Q}$, tots els cossos de classes raig són extensions ciclotòmiques $K_{\mathfrak{m}} = \mathbb{Q}(\zeta)$, en general hom voldria realitzar els cossos de classes radials via valors especials de certes funcions analítiques o, alternativament, via punts especials de certes varietats algebraiques. Aquests plantejaments estan en la línia dels somnis de Kronecker, entre d'altres, i van quedar per escrit amb tota generalitat en el conegut Problema 12 de Hilbert.

D'aquesta manera és com la teoria de la multiplicació complexa entra en escena[1]. Fins al dia avui, a part del cas $K = \mathbb{Q}$, els resultats són totalment satisfactoris només per als cossos K que són quadràtics i imaginaris. Aquests resultats es deuen a Weber, Deuring i altres. Les corbes el·líptiques amb multiplicació complexa i llurs punts de divisió proporcionen l'anàleg del cas racional. Concretament, si $[K\colon \mathbb{Q}] = 2$ i K és imaginari, tenim que

$$K_{\mathfrak{m}} = K(j(\mathcal{O}_K), w(E[\mathfrak{m}]))\,,$$

on j denota la funció modular de Klein, w és la funció de Weber que normalitza les coordenades x's dels punts de $\mathfrak{m}$-divisió, i E és una corba el·líptica amb invariant $j(\mathcal{O}_K)$.

Posteriorment, Shimura, Taniyama i Weil van generalitzar la teoria de la multiplicació complexa obtenint resultats profunds, per bé que parcials, relatius a cossos de nombres de tipus CM i varietats abelianes amb multiplicació complexa en dimensió superior.

A banda d'interactuar amb la teoria de cossos de classes, una altra vessant no menys important de la teoria de la multiplicació complexa és l'aspecte modular. En efecte, l'estudi de Grössencharacters permet descriure la prolongació analítica i equacions funcionals per a les L-sèries de les varietats abelianes amb multiplicació complexa.

A continuació segueixen una sèrie de comentaris i càlculs a fi de posar èmfasi en els aspectes computacionals de la CM en el cas 1-dimensional.

4.1 Isogènies

En vista del que ens ocupa, ens restringirem a corbes el·líptiques definides sobre $\overline{\mathbb{Q}}$, encara que en algun moment haurem de considerar les seves reduccions en característica positiva. Per pensar les classes de $\overline{\mathbb{Q}}$-isogènia de corbes el·líptiques, a vegades resulta còmode pensar en el graf següent:

[1] En realitat, l'origen de la teoria de la multiplicació complexa es remunta als treballs d'Abel sobre la N-divisió de la lemniscata amb regla i compàs. En conseqüència, hem de situar la seva gènesi, ni que sigui en potència, a les Disquisitiones Arithmeticae de Gauss.

- **Vèrtexs**: Classes de $\overline{\mathbb{Q}}$-isomorfisme; és a dir, invariants j.

- **Arestes**: Isogènies cícliques.

Notem que si convé podem considerar les arestes com arcs (arestes orientades), tot i que cada isogènia té la seva isogènia dual. Donat un vèrtex $j \in \overline{\mathbb{Q}}$, per calcular els seus adjacents hem de resoldre les equacions $\Phi_N(j, X) = 0$ per a tot $N \geq 2$, on $\Phi_N(x, y)$ denota el N-èsim polinomi modular. En absència de multiplicació complexa, el component connex del graf resultant és un arbre.

Donades dues corbes el·líptiques E i E' sobre un cos arbitrari, sabem que $\mathrm{Hom}(E, E')$ és un $\mathbb{Z}$-mòdul lliure de rang ≤ 4. A més, si $0 \neq \varphi \in \mathrm{Hom}(E, E')$, aleshores

$$\mathrm{End}^0(E')\,\varphi = \mathrm{Hom}^0(E, E') = \varphi\,\mathrm{End}^0(E)\,.$$

En efecte, sigui $\varphi_1 \in \mathrm{Hom}(E, E')$ un altre morfisme. Aleshores, tenim que $\widehat{\varphi}\,\varphi_1 = [\alpha] \in \mathrm{End}(E)$. D'on s'obté la igualtat

$$\varphi_1 = \frac{1}{\deg(\varphi)}\,\varphi\,[\alpha]\,.$$

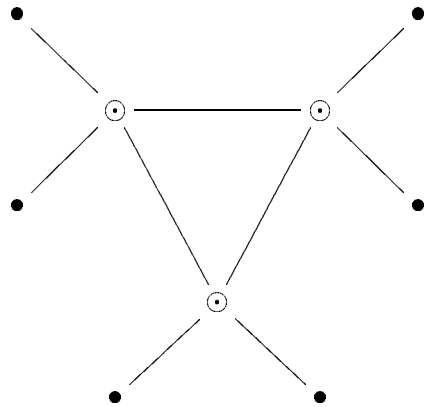
Així doncs, coneguda una isogènia (en cas d'existir) entre dues corbes el·líptiques, per conèixer totes les altres isogènies entre elles només ens cal estudiar llurs endomorfismes. En aquest sentit, es té que

$$\mathrm{End}(E) \simeq \begin{cases} \mathbb{Z}\,, \text{ o bé} \\ \mathcal{O}_f \text{ és un ordre quadràtic imaginari.} \end{cases}$$

Encara queda una tercera possibilitat, i és que $\mathrm{End}(E)$ sigui un ordre quaterniònic; però aquesta només es presenta quan treballem amb cossos de característica positiva. Tanmateix, notem que si $\varphi\colon E \to E'$ és una isogènia, aleshores $\mathrm{End}^0(E) = \mathrm{End}^0(E')$, però no necessàriament $\mathrm{End}(E) = \mathrm{End}(E')$.

Recordem que una corba el·líptica $E_{/\overline{\mathbb{Q}}}$ es diu que té multiplicació complexa si la seva àlgebra d'endomorfismes $\mathrm{End}(E)$ conté estrictament l'anell dels enters $\mathbb{Z}$. En tal cas, l'àlgebra $\mathrm{End}^0(E)$ és isomorfa a un cos quadràtic imaginari K. Per conveni, sempre triem l'isomorfisme compatible amb l'acció sobre les diferencials regulars de la corba E; és a dir, $[\alpha]^*(\omega) = \alpha\,\omega$ per a $\omega \in H^0(E, \Omega^1)$ i els corresponents α de l'ordre $\mathcal{O}_f$.

Associat a K, podem considerar el seu graf d'isogènies cícliques que té un aspecte com es mostra en la figura següent:



Aquí, $\odot$ indica els vèrtexs $j(\mathfrak{a})$ amb $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$, també anomenats vèrtexs principals. D'altra banda, $\bullet$ denota els vèrtexs $j(\mathfrak{a})$ amb $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_f)$. Notem que ara les arestes poden ser múltiples i també la presència de vèrtexs amb llaços.

Lema 4.1.1. *Siguin $E : y^2 = x^3 + a\,x + b$ i $E' : Y^2 = X^3 + A\,X + B$ corbes el·líptiques sobre $\overline{\mathbb{Q}}$. Suposem que existeix una isogènia $\varphi \in \mathrm{Hom}(E, E')$. Aleshores, tenim*

$$\varphi(x,y) = \left(R(x), \frac{1}{\lambda_\varphi}\, y\, \dot{R}(x) \right),$$

per a certa funció racional $R(x) \in \overline{\mathbb{Q}}(x)$ i $\lambda_\varphi \in \overline{\mathbb{Q}}$.

Prova. Escrivim $\varphi(x,y) = (R(x,y), Q(x,y))$, amb R, $Q \in \overline{\mathbb{Q}}(x,y)$. Atès que

$$\varphi^* \left(\frac{dX}{2Y} \right) = \frac{dR(x,y)}{2\,Q(x,y)} = \frac{\frac{\partial R}{\partial x}\, dx + \frac{\partial R}{\partial y}\, dy}{2\,Q(x,y)} = \lambda_\varphi\, \frac{dx}{2y}$$

per a cert $\lambda_\varphi \in \overline{\mathbb{Q}}$, se segueix que $\dfrac{\partial R}{\partial y} = 0$ i $Q(x,y) = \dfrac{1}{\lambda_\varphi}\, y\, \dfrac{\partial R}{\partial x}$. $\square$

És fàcil comprovar que si componem dues isogènies

$$E \xrightarrow{\varphi} E' \xrightarrow{\varphi'} E'' ,$$

aleshores se satisfà $\lambda_{\varphi'\varphi} = \lambda_{\varphi'}\, \lambda_\varphi$; i també que, si $E \xrightarrow{\varphi''} E'$ és una altra isogènia, aleshores tenim $\lambda_{\varphi+\varphi''} = \lambda_\varphi + \lambda_{\varphi''}$. En particular, es compleixen

les igualtats $\lambda_{[n]} = n$, i $\lambda_\varphi \lambda_{\widehat{\varphi}} = \deg \varphi \in \mathbb{Z}$, on $\widehat{\varphi}$ denota la isogènia dual de φ.

Exercici. Justifiqueu que el mètode següent permet calcular isogènies duals, si bé aquest només resulta eficient per a isogènies de graus petits. Siguin

$$E : y^2 = x^3 + a\,x + b \qquad E' : Y^2 = X^3 + A\,X + B$$

corbes el·líptiques sobre $\overline{\mathbb{Q}}$. Suposem donada una isogènia $E \xrightarrow{\varphi} E'$ per

$$\varphi(x,y) = \left(R(x), \frac{1}{\lambda_\varphi}\, y\, \frac{d}{dx} R(x) \right)$$

de grau N. Observem que $N-1$ és el grau del polinomi denominador reduït de $R(x)$. Considerem l'endomorfisme $[N]$ de E' que ve donat per

$$[N](X,Y) = \left(\frac{\phi_N(X)}{\psi_N(X)^2}, \frac{1}{N}\, Y\, \frac{d}{dX} \left(\frac{\phi_N(X)}{\psi_N(X)^2} \right) \right),$$

on els polinomis $\phi_N(X)$ i $\psi_N(X)$ poden ser calculats recurrentment com a [Sil1], pàgina 105. Volem descriure la isogènia dual $\widehat{\varphi}\colon E' \to E$ com

$$\widehat{\varphi}(X,Y) = \left(\widehat{R}(X), \frac{1}{\widehat{\lambda}_\varphi}\, Y\, \frac{d}{dx} \widehat{R}(X) \right).$$

Proveu que $T = \widehat{R}(X)$ s'obté com a factor lineal en factoritzar el polinomi sobre $\overline{\mathbb{Q}}(X)[T]$ obtingut de l'equació

$$R(T) = \frac{\phi_N(X)}{\psi_N(X)^2}.$$

Proveu que també se satisfà l'equació diferencial

$$\frac{N^2}{\lambda^2} \frac{T^3 + a\,T + b}{X^3 + A\,X + B} R'(T) = \frac{d}{dX} \left(\frac{\phi_N(X)}{\psi_N(X)^2} \right).$$

4.2 Cossos de definició

Siguin E i E' dues corbes el·líptiques definides sobre un mateix cos de nombres L. Suposem que existeix una isogènia

$$E_{/L} \xrightarrow{\varphi} E'_{/L}\,, \quad \varphi(x,y) = \left(R(x), \frac{1}{\lambda}\, y\, \dot{R}(x) \right).$$

Per a cada $\sigma \in \mathrm{Gal}(\overline{L}/L)$ podem considerar la isogènia conjugada

$$E_{/L} \xrightarrow{{}^{\sigma}\varphi} E'_{/L} \ .$$

Es presenten les situacions següents:

- **Cas sense CM.** Si $\mathrm{End}(E) \simeq \mathbb{Z}$, aleshores tenim ${}^{\sigma}\varphi = \pm\varphi$. D'on resulta que

  $$R(x) \in L[x]\,, \quad {}^{\sigma}\lambda = \pm\lambda\,.$$

  És immediat comprovar que l'aplicació

  $$\psi\colon \mathrm{Gal}(\overline{L}/L) \to \{\pm 1\}\,, \quad \sigma \mapsto \frac{\lambda}{{}^{\sigma}\lambda}$$

  és un 1-cocicle amb acció trivial; és a dir, ψ és un caràcter quadràtic. El seu cos fix L_ψ és $L(\lambda)$, el cos de definició de la isogènia φ, i satisfà $[L_\psi : L] \leq 2$.

- **Cas CM.** Si $\mathrm{End}(E) \simeq \mathcal{O} \subset K$, aleshores tenim

  $${}^{\sigma}\varphi = \frac{1}{\deg(\varphi)}\,[\alpha]\,\varphi\,, \quad \text{amb } [\alpha] \in \mathrm{End}(E')\,.$$

  A més, se satisfà $\deg(\varphi)^2 = \deg([\alpha]) = |\mathrm{Nor}_{K/\mathbb{Q}}(\alpha)|$, i

  $$\lambda/{}^{\sigma}\lambda = \overline{\alpha}/\deg(\varphi) \in K^*$$

  amb norma 1. Ara l'aplicació

  $$\psi\colon \mathrm{Gal}(\overline{L}/L) \to K^*\,, \quad \sigma \mapsto \frac{\lambda}{{}^{\sigma}\lambda}$$

  és un 1-cocicle que esdevé morfisme si ens restringim a $\mathrm{Gal}(\overline{L}/LK)$. Atès que la isogènia φ està definida sobre una extensió finita de L, notem que $\psi\colon \mathrm{Gal}(\overline{L}/LK) \to \mu(K)$ és un caràcter (quadràtic, llevat potser quan K sigui $\mathbb{Q}(i)$, o bé $\mathbb{Q}(\sqrt{-3})$). Ara, la isogènia φ queda definida sobre el cos fix LK_ψ. Remarquem també que $\mathrm{End}(E) = \mathrm{End}_{LK}(E)$, ja que $[\alpha]_E^{\sigma} = [{}^{\sigma}\alpha]_{{}^{\sigma}E}$.

4.3 L'exemple 23

En aquesta secció, ens proposem mostrar alguns càlculs senzills sobre cossos de Hilbert, cossos radials, cossos d'ordres i isogènies entre corbes el·líptiques amb CM que il·lustrin els resultats esmentats anteriorment. Per a la realització dels càlculs hem utilitzat una combinació de `PARI` i `Mathematica`.

Fixem el cos quadràtic imaginari $K = \mathbb{Q}(\sqrt{-23})$. El seu anell d'enters és $\mathcal{O}_K = \mathbb{Z}[\tau]$, on $\tau = (1+\sqrt{-23})/2$. El seu grup de classes d'ideals és

$$\mathrm{Pic}(\mathcal{O}_K) = \{[(1)], [\mathfrak{a}], [\mathfrak{b}]\} \simeq \mathbb{Z}/3\mathbb{Z},$$

on $2\,\mathcal{O}_K = \underbrace{(2,\tau)}_{\mathfrak{a}}\,\underbrace{(2,\tau+1)}_{\mathfrak{b}}$.

Com és costum, establim una bijecció entre representants de les classes d'ideals, classes de formes quadràtiques i elements del semi-pla superior $\mathbb{H}$ en el domini fonamental clàssic del grup modular $\mathrm{SL}_2(\mathbb{Z})$:

$$\begin{aligned}
(1) &\longleftrightarrow (1,1,6) &&\longleftrightarrow \tau_1 = \tau \\
\mathfrak{a} &\longleftrightarrow (2,-1,3) &&\longleftrightarrow \tau_3 = \tau/2 \\
\mathfrak{b} &\longleftrightarrow (2,1,3) &&\longleftrightarrow \tau_2 = (\tau+1)/2\,.
\end{aligned}$$

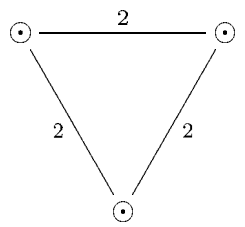
Aleshores podem calcular els invariants j associats a les corbes el·líptiques *principals* amb CM sobre K; és a dir, aquelles que tenen àlgebra d'endomorfismes isomorfa a l'ordre maximal $\mathcal{O}_K$:

$$\begin{aligned}
j(\tau_1) &= -349225.699699333682... \\
j(\tau_2) &= 737.84998496684... + 1764.0189...\,i \\
j(\tau_3) &= 737.84998496684... - 1764.0189...\,i\,.
\end{aligned}$$

Així trobem que

$$\mathrm{Irr}(j(\tau_i), \mathbb{Q}; X) = X^3 + 3491750\,X^2 - 5151296875\,X + 5^9\,.\,11^3\,.\,17^3\,.$$

De la relació que lliga les τ's podem desduir que el graf de les isogènies principals té l'aspecte següent



En qualsevol cas, en presència de CM, cal fer notar que el grau 2 en el diagrama anterior pot ser substituït per qualsevol enter positiu que sigui norma d'elements de K; com per exemple, 3, 13, 23, 29, 31, ...

Cos de classes de Hilbert. Es tracta del cos radial associat al mòdul trivial i ve donat per $K_{(1)} = K(j(\mathcal{O}_K))$. El cos de Hilbert $K_{(1)}$ és la màxima extensió abeliana i no-ramificada de K. Recordem també que l'invariant j avaluat en qualsevol ordre de tot cos quadràtic imaginari és sempre un nombre real.

En l'exemple que ens ocupa, tenim el diagrama de cossos següent:

$$\begin{tikzcd}
 & K_{(1)} = \mathbb{Q}(\beta) \arrow[dl, dash, "C_3"'] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{-23}) \arrow[dr, dash] & & \mathbb{Q}(j(\tau_i)) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Amb l'ajuda de `PARI`, podem trobar polinomis definidors/elements primitius més senzills. Concretament, trobem

$$\mathbb{Q}(j(\tau_i)) \simeq \mathbb{Q}[\alpha]/(\alpha^3 - \alpha - 1)$$

i

$$\mathrm{Irr}(\beta, \mathbb{Q}; X) = X^6 - 3X^5 + 5X^4 - 5X^3 + 5X^2 - 3X + 1\,.$$

Els conjugats de β són: β_i, $-\beta_i + 1$, amb

$$\begin{aligned}
\beta_1 &= \beta\,;\\
\beta_2 &= -\beta^5 + 2\beta^4 - 3\beta^3 + 2\beta^2 - 3\beta + 1\,;\\
\beta_3 &= -\beta^5 + 3\beta^4 - 5\beta^3 + 5\beta^2 - 5\beta + 3\,.
\end{aligned}$$

Es té que $\mathrm{Gal}(K_{(1)}/\mathbb{Q}) \simeq D_{2.3} \simeq \mathcal{S}_3$, amb generadors σ i τ donats per

$$\begin{cases}
\sigma\colon \beta \mapsto -\beta + 1 & \text{conjugació complexa;}\\
\tau\colon \beta \mapsto -\beta_2 + 1 & \text{automorfisme d'ordre 3.}
\end{cases}$$

També tenim $\mathrm{disc}(K_{(1)}/\mathbb{Q}) = -23^3$, i l'anell d'enters és $\mathcal{O}_{K_{(1)}} = \mathbb{Z}[\beta]$. Donem la descomposició de l'únic primer ramificat de $K_{(1)}/\mathbb{Q}$: $23\,\mathcal{O}_{K_{(1)}} = \mathfrak{P}_1^2\mathfrak{P}_2^2\mathfrak{P}_3^2$. Finalment, si fixem l'arrel $\beta = 0.5+0.42445224584391...\,i$, trobem les relacions

$$\begin{aligned}\alpha_1 &= \beta^4 - 2\beta^3 + 3\beta^2 - 2\beta + 2\,;\\ \alpha_2 &= \beta^5 - 3\beta^4 + 5\beta^3 - 5\beta^2 + 4\beta - 2\,;\\ \alpha_3 &= -\beta^5 + 2\beta^4 - 3\beta^3 + 2\beta^2 - 2\beta\,,\end{aligned}$$

on α_i són les arrels de $\alpha^3 - \alpha + 1 = 0$ de manera que es compleix

$$\begin{aligned}j(\tau_i) &= -820750\,\alpha_i^2 - 1084125\,\alpha_i - 616750\,;\\ \sqrt{-23} &= 4\beta^5 - 10\beta^4 + 16\beta^3 - 14\beta^2 + 18\beta - 7\,.\end{aligned}$$

Cos de classes radial. Venen donats per $K_{\mathfrak{m}} = K(j(\mathcal{O}_K), w(E[\mathfrak{m}]))$, on $w(E[\mathfrak{m}])$ són els valors que pren la funció de Weber en els punts de $\mathfrak{m}$-divisió d'una corba el·líptica E amb invariant igual a $j(\mathcal{O}_K)$. Considerarem el cas $\mathfrak{m} = 3\,\mathcal{O}_K$. Posem $j = j(\mathcal{O}_K)$. La corba $E\colon y^2 = x^3 + Ax + B$ amb

$$A = -27\,j\,(j - 1728)\,, \quad B = 54\,j\,(j - 1728)^2$$

té invariant $j(E) = j$. Les x's de $E[\mathfrak{m}] = E[3]$ són les arrels de

$$3\,x^4 + 6\,A\,x^2 + 12\,B\,x - A^2\,.$$

Si $P = (x,y) \leftrightarrow (\wp(z,\Lambda), \wp'(z,\Lambda)) \in E[\mathfrak{m}]$, aleshores

$$w(P) = \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda) = \frac{729}{32}\frac{c_4c_6}{\Delta}\,x\,.$$

La successió exacta $1 \to \{\pm 1\} \to (\mathcal{O}_K/\mathfrak{m})^* \to \mathrm{Gal}(K_{\mathfrak{m}}/K) \to \mathrm{Pic}(\mathcal{O}_K) \to 1$ imposa que

$$[K_{\mathfrak{m}} : K] = \frac{1}{2}\,h(K)\,\#(\mathcal{O}_K/\mathfrak{m})^* = 6\,.$$

Posposem per uns moments el càlcul de polinomis definidors per al cos radial $K_{\mathfrak{m}}$.

Cos de classes d'un ordre. Venen donats per $K_{\mathcal{O}_f} = K(j(\mathcal{O}_f))$. Examinem el cas de conductor $f = 3$. Recordem que, en general, si tenim

$$\mathfrak{m} = f\,\mathcal{O}_K\,, \quad \mathcal{O}_f = \mathbb{Z} + f\,\mathcal{O}_K$$

aleshores

$$K \subseteq K_{\mathcal{O}_f} \subseteq K_{\mathfrak{m}}\,.$$

L'extensió $K_{\mathcal{O}_3}/K$ té grau $\#\operatorname{Pic}(\mathcal{O}_3) = 6$. Representants de formes quadràtiques de discriminant $-3^2 \cdot 23$ i les corresponents arrels a $\mathbb{H}$ són:

$$\begin{array}{ll}
\mathbf{f} = (2,-1,26) & \tau_1 = (3\tau - 1)/2 \\
\mathbf{f}^2 = (4,-1,13) & \tau_2 = (3\tau - 1)/4 \\
\mathbf{f}^3 = (8,7,8) & \tau_3 = (3\tau - 5)/8 \\
\mathbf{f}^4 = (4,1,13) & \tau_4 = (3\tau - 2)/4 \\
\mathbf{f}^5 = (2,1,26) & \tau_5 = (3\tau - 2)/2 \\
\mathbf{f}^6 = \mathrm{id} = (1,1,52) & \tau_6 = 3\tau - 2
\end{array}$$

El cos $K_{\mathcal{O}_3}$ té polinomi definidor sobre $\mathbb{Q}$:

$$\begin{array}{l}
X^{12} - 3X^{11} + 4X^{10} - 5X^9 + 5X^8 + 2X^7 - \\
7X^6 + 2X^5 + 5X^4 - 5X^3 + 4X^2 - 3X + 1\,.
\end{array}$$

Observem que en aquest exemple tenim $K_{\mathcal{O}_3} = K_{(3)}$, i també $\mathbb{Q}(\sqrt{-3}) \subset K_{\mathcal{O}_3}$. És cert que si el cos de l'ordre de conductor f conté les arrels f-èsimes de la unitat, aleshores $K_{\mathcal{O}_f} = K_{(f)}$? Resposta, no sempre. En general, se sap que $\operatorname{Gal}(K_{(f)}/K_{\mathcal{O}_f}(\zeta_f))$ és un 2-grup elemental (Hasse, [Ko] pàgina 110).

Càlcul d'isogènies. Amb les notacions d'abans, podem escriure

$$j_1 = \frac{256(t-3)^3}{t-4}\,, \quad j_2 = \frac{16(t+12)^3}{(t-4)^2} = {}^{\sigma}j_1\,, \quad j_3 = {}^{\tau}j_1\,,$$

on

$$t = \frac{1}{16}\,(455\,\beta^5 - 1025\,\beta^4 + 1070\,\beta^3 - 1230\,\beta^2 + 870\,\beta - 317) \in K_{(1)}\,.$$

Fent ús de les fórmules de Velú, trobem que les corbes el·líptiques

$$E_1\colon y^2 = x^3 + x^2 + \frac{1}{t}\,x\,, \qquad E_2\colon y^2 = x^3 - 2\,x^2 + \left(1 - \frac{4}{t}\right)\,x\,,$$

amb invariants j_1 i j_2 respectivament, admeten una isogènia $\varphi\colon E_1 \to E_2$ definida sobre $K_{(1)}$ de grau 2 que ve donada per

$$\varphi(x,y) = \left(x + 1 + \frac{1}{t\,x}\,,\, y\,\left(1 - \frac{1}{t\,x^2}\right)\right)\,.$$

Per translacions sobre $\mathbb{Q}$, fixem equacions de Weierstrass per a E_1 i E_2 com segueix:

$$E_{j_1} : y^2 = x^3 + \frac{3-t}{3\,t}\,x + \frac{2\,t-9}{27\,t}\,,$$

$$E_{j_2} : y^2 = x^3 - \frac{12+t}{3\,t}\,x + \frac{2\,(t-36)}{27\,t}\,.$$

Notem que es té un isomorfisme $\psi\colon E_{j_2} \to {}^{\sigma}E_{j_1}$. Ara bé, aquest isomorfisme està definit sobre $K_{(1)}(\sqrt{-2})$. En efecte, és fàcil comprovar que

$$\left(-\frac{12+t}{3\,t}\right)\left(\frac{1}{\sqrt{-2}}\right)^4 = \left(\frac{3-t}{3\,t}\right)^{\sigma},$$

$$\left(\frac{2\,(t-36)}{27\,t}\right)\left(\frac{1}{\sqrt{-2}}\right)^6 = \left(\frac{2\,t-9}{27\,t}\right)^{\sigma}.$$

Així, en aquests models, la isogènia $\mu_\sigma\colon E_{j_1} \to {}^{\sigma}E_{j_1}$ s'escriu

$$\mu_\sigma(x,y) = \left(\frac{-3\,t\,x^2+t\,x-3}{2\,t\,(3\,x-1)}\,,\ \frac{1}{\sqrt{-2}}\,y\,\frac{-9\,t\,x^2+6\,t\,x-t+9}{2\,t\,(3\,x-1)^2}\right).$$

Observem que si modifiquéssim E_{j_1} per $K_{(1)}$-isomorfismes, les corresponents isogènies μ_σ quedarien definides sobre $K_{(1)}(\sqrt{-2\,\gamma^\sigma\gamma})$ amb $\gamma \neq 0$ de $K_{(1)}$. Procedint de manera anàloga, ara amb l'automorfisme $\tau \in \mathrm{Gal}(K_{(1)}/\mathbb{Q})$, trobem que $\mu_\tau\colon E_{j_1} \to {}^{\tau}E_{j_1}$ està definida sobre $K_{(1)}(\sqrt{u})$ on

$$u = \frac{1}{308}\left(62 + 75\,\beta - 333\,\beta^2 + 384\,\beta^3 - 183\,\beta^4 + 54\,\beta^5\right).$$

És cert que per torçaments de E_{j_1} sobre el cos de Hilbert $K_{(1)}$ és possible definir μ_σ i μ_τ sobre $K_{(1)}$? La resposta a aquesta pregunta és afirmativa. La raó és que $\mathbb{Q}(\sqrt{-23})$ té discriminant primer (llevat signe) i Gross ha estudiat minuciosament les corbes el·líptiques reals $A(p)$ amb CM corresponents a cossos quadràtics imaginaris $\mathbb{Q}(\sqrt{-p})$ amb $p \equiv 3 \pmod 4$. Així, el millor model de Weierstrass que podem considerar en el nostre cas és

$$A(23)\colon Y^2 = X^3 - \frac{115}{48}\left(7 + 11\,\alpha + 5\,\alpha^2\right)X - \frac{161}{864}\left(240 + 379\,\alpha + 307\,\alpha^2\right),$$

on α és l'arrel real de $x^3 - x - 1$. Fins i tot, $A(23)$ admet model global minimal sobre $K_{(1)}^{+} = K_{(1)} \cap \mathbf{R}$ (confronteu amb [Gr2]).

4.4 Modularitat

Passem a recordar els resultats més importants sobre modularitat de corbes el·líptiques amb CM. Comencem per recordar la definició de L-sèries associades a corbes el·líptiques arbitràries.

L-sèries de Hasse-Weil. Sigui E una corba el·líptica definida sobre un cos de nombres L. Per a cada ideal primer $\mathfrak{p}$ de L tal que E tingui bona reducció en $\mathfrak{p}$, posem

$$\begin{cases} \mathbf{F}_{\mathfrak{p}} = \mathcal{O}_L/\mathfrak{p}\,, \\ q_{\mathfrak{p}} = \mathrm{Nor}_{L/\mathbb{Q}}(\mathfrak{p}) = \#\mathbf{F}_{\mathfrak{p}}\,, \\ a_{\mathfrak{p}} = q_{\mathfrak{p}} + 1 - \#\widetilde{E}(\mathbf{F}_{\mathfrak{p}}). \end{cases}$$

La L-sèrie de Hasse-Weil associada a $E_{/L}$ es defineix per

$$\begin{aligned} L(E_{/L}, s) = & \prod_{\mathfrak{p}\ \mathrm{br}} (1 - a_{\mathfrak{p}}\, q_{\mathfrak{p}}^{-s} + q_{\mathfrak{p}}^{1-2s})^{-1} \times \\ & \prod_{\mathfrak{p}\ \mathrm{rms}} (1 - q_{\mathfrak{p}}^{-s})^{-1} \prod_{\mathfrak{p}\ \mathrm{rmns}} (1 + q_{\mathfrak{p}}^{-s})^{-1} \end{aligned}$$

(br = bona reducció, rms = reducció multiplicativa split, rmns = reducció multiplicativa no-split.)

Recordem que $\det(1 - \varphi_{\mathfrak{p},\ell} T) = 1 - a_{\mathfrak{p}} T + q_{\mathfrak{p}} T^2 = (1 - \alpha_{\mathfrak{p}} T)(1 - \overline{\alpha}_{\mathfrak{p}} T)$, on $\varphi_{\mathfrak{p},\ell}\colon T_\ell(\widetilde{E}) \to T_\ell(\widetilde{E})$ denota l'endomorfisme de Frobenius actuant sobre el mòdul de Tate $T_\ell(\widetilde{E})$ de la reducció de E mòdul $\mathfrak{p}$.

Super-conjectura. $L(E_{/L}, s)$ admet prologanció analítica a tot $\mathbb{C}$ i satisfà equació funcional per $s \mapsto 2 - s$.

Aquesta conjectura és certa per al cas $L = \mathbb{Q}$ (Wiles et al.) i per a les corbes el·líptiques amb CM (Hecke-Deuring).

Grössencharacters i L-sèries de Hecke. Per als detalls i definicions precises consulteu [Sil2], [Lang]. Sigui L un cos de nombres. Considerem el grup topològic $\mathbf{A}_L^* = \prod_v' L_v^*$ de les ideles de L. Recordem que donat un $x \in \prod_v L_v^*$, es té

$$x \in \mathbf{A}_L^* \Leftrightarrow x_v \in R_v^* \ \text{ q.p.t } v\,,$$

on R_v denota l'anell de la valoració v de L. Tenim les inclusions naturals

$$L^* \hookrightarrow \mathbf{A}_L^*, \qquad \alpha \mapsto (\dots, \alpha, \alpha, \alpha, \dots)$$

$$L_v^* \hookrightarrow \mathbf{A}_L^*, \qquad t \longmapsto (\dots, 1, \underset{\substack{\uparrow \\ v\text{-component.}}}{t}, 1, \dots)$$

Definició. Un Grössencharacter (o caràcter de Hecke) és un morfisme continu $\psi\colon \mathbf{A}_L^* \to \mathbb{C}^*$ tal que $\psi(L^*) = 1$. Diem que ψ és no ramificat en $\mathfrak{p}$ si $\psi(R_\mathfrak{p}^*) = 1$. En tal cas, escrivim $\psi(\mathfrak{p}) = \psi(\dots, 1, 1, \pi, 1, 1, \dots)$; altrament, escrivim $\psi(\mathfrak{p}) = 0$.

Com a conseqüència del Teorema 5 [Lang], capítol X, tenim que és el mateix donar:

- $\psi\colon \mathbf{A}_L^* \to \mathbb{C}^*$ un Grössencharacter de L no-ramificat fora d'un conjunt finit de primers;
- Una extensió abeliana L' de L;
- Un morfisme $\psi\colon I_L(\mathfrak{m}) \to \mathbb{C}^*$ tal que $\psi((a)) = a$ per a tot $a \equiv 1 \pmod{\mathfrak{m}}$.

Per veure això, s'usa que $L' \subseteq L_\mathfrak{m}$ per a cert mòdul $\mathfrak{m}$, i també els isomorfismes

$$\mathrm{Gal}(L_\mathfrak{m}/L) \simeq \mathbf{A}_L^*/L^* U_\mathfrak{m} \simeq I_L(\mathfrak{m})/P_{L,1}(\mathfrak{m}).$$

Definició. La L-sèrie de Hecke associada a ψ és

$$L(s, \psi) = \prod_\mathfrak{p} \left(1 - \psi(\mathfrak{p}) q_\mathfrak{p}^{-s}\right)^{-1}.$$

Teorema (Hecke). $L(s, \psi)$ admet prolongació analítica a tot $\mathbb{C}$ i satisfà equació funcional per $s \mapsto N(\psi) - s$, on $N(\psi)$ és cert nombre complex.

Grössencharacters el·líptics. Sigui $E_{/L}$ una corba el·líptica amb CM i tal que $\mathrm{End}(E) = \mathcal{O}_K$. Si $K \subseteq L$, es defineix $\psi_{E/L}\colon \mathbf{A}_L^* \longrightarrow K^* \subseteq \mathbb{C}^*$ per

$$\psi_{E/L}(x) = (\mathrm{Nor}_{L/K}((x)))\, \mathrm{Nor}_{L/K}(x^{-1})_\infty$$

i es comprova que $\psi_{E/L}$ és un Grössencharacter de L (cf. [Sil2]). No obstant, per tal de calcular la L-sèrie de Hecke associada a E, només ens interessa conèixer els valors $\psi_{E/L}(\mathfrak{p})$ per als ideals primers $\mathfrak{p}$ de bona reducció. Així, resulta que $\psi_{E/L}(\mathfrak{p}) \in \mathcal{O}_K$ es correspon amb l'endomorfisme aixecament del Frobenius $\varphi_{\mathfrak{p}}$ mòdul $\mathfrak{p}$,

$$\begin{tikzcd} E \arrow[r, "\psi_{E/L}(\mathfrak{p})"] \arrow[d] & E \arrow[d] \\ \widetilde{E} \arrow[r, "\varphi_{\mathfrak{p}}"] & \widetilde{E}. \end{tikzcd}$$

De manera que es satisfan les igualtats:

$$q_{\mathfrak{p}} = \mathrm{Nor}_{L/K}(\mathfrak{p}) = \mathrm{Nor}_{K/\mathbb{Q}}(\psi_{E/L}(\mathfrak{p})),$$

$$a_{\mathfrak{p}} = \psi_{E/L}(\mathfrak{p}) + \overline{\psi_{E/L}(\mathfrak{p})}.$$

Teorema (Deuring). (i) Si $K \subseteq L$, aleshores

$$L(E_{/L}, s) = L(s, \psi_{E/L})\, L(s, \overline{\psi}_{E/L});$$

(ii) Si $K \not\subseteq L$, aleshores $L(E_{/L}, s) = L(s, \psi_{E/LK})$.

CM i modularitat. Donat un Grössencharacter de K mòdul $\mathfrak{m}$, és a dir

$$\psi_K \colon I_K(\mathfrak{m}) \longrightarrow \mathbb{C}^*$$

amb $\psi_K((a)) = a$ per a tot $a \in K^*$ tal que $a \equiv 1 \mod {}^*\mathfrak{m}$, considerem els tres caràcters de Dirichlet següents:

χ: $(\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$, caràcter de Dirichlet associat a K;

η: $(\mathbb{Z}/M\mathbb{Z})^* \to \mathbb{C}^*$, caràcter de Dirichlet definit per $\eta(a) = \psi_K((a))/a$;

ε: $(\mathbb{Z}/MD\mathbb{Z})^* \to \mathbb{C}^*$, el producte $\varepsilon = \eta\chi$.

Aqui, D és el valor absolut del discriminant de K i M és la norma del mòdul $\mathfrak{m}$.

Teorema (Hecke, Shimura). La sèrie

$$g(q) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \psi_K(\mathfrak{a})\, q^{N(\mathfrak{a})} \in S_2(MD,\varepsilon)$$

és una e-forma (vector propi per l'àlgebra de Hecke).

Posem $f(q) = \sum a_n q^n$ la forma nova associada. Se satisfà que $f = f \otimes \chi$. En particular, si $\chi(p) = -1$ aleshores $a_p = 0$. (Aquesta és la manera pràctica de reconèixer una e-forma modular amb CM: l'abundància de coeficients a_p nuls).

Optimalitat i restricció de Weil. Si partim d'un Grössencharacter mòdul $\mathfrak{m}$,

$$\psi_K \colon I_K(\mathfrak{m}) \to \mathbb{C}^*,$$

com abans, podem construir la forma nova associada

$$f(q) = \sum a_n q^n \in S_2(N,\varepsilon), \quad E_f = \mathbb{Q}(\{a_n\}).$$

Ara considerem el quocient optimal $J_1(N) \to A_f$ que correspon a la forma nova f. Se satisfà

$$L(A_f/\mathbb{Q},s) = \prod_\sigma L({}^\sigma f, s) = \begin{cases} \prod_\tau L(s, {}^\tau\psi_K)\, L(s, \overline{{}^\tau\psi_K}) & \text{si } K \subseteq E_f; \\ \prod_\tau L(s, {}^\tau\psi_K) & \text{si } K \nsubseteq E_f, \end{cases}$$

on $\sigma \colon E_f \hookrightarrow \overline{\mathbb{Q}}$ i $\tau \colon \operatorname{Im}\psi_K \hookrightarrow \overline{\mathbb{Q}}$ recorren les respectives immersions. És clar que $E_f \subseteq \operatorname{Im}\psi_K$ i també que $K \subseteq \operatorname{Im}\psi_K$. A més, tenim una $\overline{\mathbb{Q}}$-isogènia $A_f \sim E^m$ per a certa corba el·líptica $E_{/\overline{\mathbb{Q}}}$ amb CM. En realitat, $E_{/\overline{\mathbb{Q}}}$ també pot ser obtinguda com a quocient optimal de $J_1(N)$.

Qüestió 1. És cert que el quocient optimal $E_{/\overline{\mathbb{Q}}}$ de $J_1(N)$ és sempre principal?

Qüestió 2. Sobre quin cos de nombres L queda definit aquest quocient optimal? Quina relació hi ha entre $L(s,\psi_K)$ i $L(E_{/L},s)$?

Qüestió 3. Existeix algun cos de nombres L' tal que la restricció de Weil $\operatorname{Res}_{L'/\mathbb{Q}}(E)$ és producte de varietats abelianes modulars?

4.5 L'exemple 23 (de nou)

Ara reprenem l'exemple $K = \mathbb{Q}(\sqrt{-23})$ des del punt de vista modular. Aquesta vegada, per realitzar els càlculs hem utilitzat `PARI`, `Mathematica`, i també els paquets modulars `M1-Symbols` de J. Quer i `Hecke` de W. Stein.

Considerem la forma nova $f(q) = \sum a_n q^n \in S_2(69, (\frac{\cdot}{69}))$ tal que té per cos de coeficients $E_f = \mathbb{Q}(t)$ amb $t^6 + 12\,t^4 + 36\,t^2 + 23 = 0$. Es té que $[E_f^{\mathrm{gal}} : \mathbb{Q}] = 12$ i els conjugats de t dins E_f són $\{\pm t\}$. Tenim el diagrama de cossos

$$\begin{tikzcd}
 & E_f \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(t^2) \arrow[dr, dash, "\mathrm{tr}"'] & & \mathbb{Q}(t^3+6\,t) = \mathbb{Q}(\sqrt{-23}) \arrow[dl, dash] \\
 & \mathbb{Q}\,. &
\end{tikzcd}$$

En executar els paquets modulars, trobem els primers p-coeficients de Fourier de la q-expansió de f:

$$\begin{aligned}
a_2 &= t \\
a_3 &= -t^5/6 + t^4/6 - 5t^3/3 + 7t^2/6 - 19t/6 + 2/3 \\
a_5 &= 0 \\
a_7 &= 0 \\
a_{11} &= 0 \\
a_{13} &= -t^4 - 9\,t^2 - 12 \\
a_{17} &= 0 \\
a_{19} &= 0 \\
a_{23} &= -\sqrt{-23} \\
a_{29} &= t^5 + 10\,t^3 + 17\,t \\
a_{31} &= t^4 + 11\,t^2 + 20\,, \ \ldots\ , a_{59} = 2\sqrt{-23}\,.
\end{aligned}$$

Procedim a construir de manera artesanal un Grössencharacter ψ_K tal que proporciona aquesta forma nova f. Per tal motiu, triem el mòdul $\mathfrak{m} = \mathfrak{p}_3$ determinat per les condicions

$$3\,\mathcal{O}_K = \mathfrak{p}_3\,\overline{\mathfrak{p}}_3\,, \qquad \tau \equiv 1 \pmod{\mathfrak{p}_3}\,.$$

Considerem el Grössencharacter ψ_K associat a $\mathfrak{m}$. Volem construir el vector propi per l'àlgebra de Hecke corresponent; és a dir,

$$f(q) = \sum a_n q^n\,, \quad \text{amb } a_p = \sum_{\mathfrak{p}|p} \psi_K(\mathfrak{p})$$

sempre que p descompongui completament a K o bé $p = 23$; altrament fem $a_p = 0$. Notem que $\psi_K(\mathfrak{p}_3) = 0$, però $\psi_K(\overline{\mathfrak{p}}_3)$ és no-nul. Recordem que

$$2\,\mathcal{O}_K = \underbrace{(2,\tau)}_{\mathfrak{a}}\,\underbrace{(2,\tau+1)}_{\mathfrak{b}}\,.$$

Donat un primer $p \in \mathbb{Z}$ i un ideal primer $\mathfrak{p}$ de K amb $\mathfrak{p} \mid p$, es presenten tres possibilitats:

$$\mathfrak{p} = \begin{cases} (\alpha)\,, \\ \mathfrak{a}\,(\alpha)\,, \\ \mathfrak{b}\,(\alpha)\,, \end{cases}$$

per a cert $\alpha \in K^*$. A més, podem triar α de manera que –*bien entendu*– es tingui $\alpha \equiv 1 \pmod{\mathfrak{p}_3}$. Per a tot $p \neq 3, 23$, tenim

$$\pm p = \psi_K((p)) = \begin{cases} \psi_K(\mathfrak{p})\,\psi_K(\mathfrak{p}') & \text{, si } p = \mathfrak{p}\,\mathfrak{p}'; \\ \psi_K(\mathfrak{p}) & \text{, si } p = \mathfrak{p}, \end{cases}$$

on el signe $\pm$ s'adapta segons el de la congruència $p \equiv \pm 1 \pmod 3$.

Un cop decidit el valor $\psi_K(\mathfrak{a})$, tots els coeficients de la forma parabòlica $f(q)$ queden únivocament determinats. A la vista de la igualtat

$$\mathfrak{a}^3 = (2-\tau)\,,$$

posem $\gamma := \sqrt[3]{2-\tau}$ (un càlcul senzill mostra que γ és arrel de $x^6 - 3\,x^3 + 8$). D'aquesta manera, queden fixats els valors

$$\psi_K((1)) = 1\,, \quad \psi_K(\mathfrak{a}) = \gamma\,, \quad \psi_K(\mathfrak{b}) = -2/\gamma\,.$$

En particular, si fem $t := \gamma - 2/\gamma$, tenim $a_2 = t$.

Per a cada primer $p \neq 3, 23$ que descompongui a K, escrivim $p = \mathfrak{p}\,\mathfrak{p}'$ amb $\mathfrak{p} = (p, *)$ per a cert element $*$ de $\mathcal{O}_K$. Localitzem $[\mathfrak{p}] = [\mathfrak{c}] \in \{[(1)], [\mathfrak{a}], [\mathfrak{b}]\}$, i trobem $\alpha \in K$ amb $\alpha \equiv 1 \bmod \mathfrak{p}_3$ tal que $\mathfrak{p} = \mathfrak{c}\,(\alpha)$. Aleshores, tindrem

$$\psi_K(\mathfrak{p}) = \alpha\,\psi_K(\mathfrak{c})\,.$$

I, per tant, trobem el coeficient

$$a_p = \psi_K(\mathfrak{p}) + \frac{\pm p}{\psi_K(\mathfrak{p})} \quad \text{(amb signe + sii } p \equiv 1 \bmod 3\text{)}.$$

La taula següent mostra els resultats per a primers petits que descomponen completament a K:

p	$*$	$[\mathfrak{p}]$	α	a_p
13	$3+2\tau$	$\mathfrak{a}$	$\frac{-5+\tau}{2}$	$-t^4-9t^2-12$
29	$7+2\tau$	$\mathfrak{b}$	$\frac{-4+3\tau}{2}$	t^5+10t^3+17t
31	$-16+2\tau$	$\mathfrak{b}$	$\frac{-8+\tau}{2}$	t^4+11t^2+20
47	$19+2\tau$	$\mathfrak{a}$	$\frac{5+3\tau}{2}$	...
59	$-7+2\tau$	(1)	$-7+2\tau$	$2\sqrt{-23}$

Càlcul de quocients optimals. La q-expansió $\sum a_n q^n$ de f comença

$$f(q) = \quad q + t\,q^2 + \left(-t^5/6 + t^4/6 - 5\,t^3/3 + 7\,t^2/6 - 19\,t/6 + 2/3\right) q^3$$

$$+(t^2 \quad +2)\,q^5 + \left(t^5/6 + t^4/3 + 7\,t^3/6 + 17\,t^2/6 + 2\,t/3 + 23/6\right) q^6 + \ldots$$

Recordem que t satisfà $t^6 + 12\,t^4 + 36\,t^2 + 23 = 0$. Una base racional de $H^0(A_f, \Omega^1_{/\mathbb{Q}})$ s'obté a partir de les formes parabòliques:

$$g_1(q) = q + \tfrac{2}{3}\,q^3 + 2\,q^4 + \tfrac{23}{6}\,q^6 - \tfrac{14}{3}\,q^9 - \tfrac{5}{2}\,q^{12} - 12\,q^{13} + 4\,q^{16} - \tfrac{23}{6}\,q^{18} \ldots$$

$$g_2(q) = q^2 - \tfrac{19}{6}\,q^3 + \tfrac{2}{3}\,q^6 + 4\,q^8 + \tfrac{13}{6}\,q^9 - \tfrac{5}{2}\,q^{12} - \tfrac{14}{3}\,q^{18} + \ldots$$

$$g_3(q) = \tfrac{7}{6}\,q^3 + q^4 + \tfrac{17}{6}\,q^6 - \tfrac{13}{6}\,q^9 - 3\,q^{12} - 9\,q^{13} + 6\,q^{16} - \tfrac{23}{6}\,q^{18} + \ldots$$

$$g_4(q) = -\tfrac{5}{3}\,q^3 + \tfrac{7}{6}\,q^6 + q^8 + \tfrac{5}{3}\,q^9 - \tfrac{1}{2}\,q^{12} - \tfrac{13}{6}\,q^{18} + \dots$$

$$g_5(q) = \tfrac{1}{6}\,q^3 + \tfrac{1}{3}\,q^6 - \tfrac{1}{6}\,q^9 - \tfrac{1}{2}\,q^{12} - q^{13} + q^{16} - \tfrac{1}{3}\,q^{18} + \dots$$

$$g_6(q) = -\tfrac{1}{6}\,q^3 + \tfrac{1}{6}\,q^6 + \tfrac{1}{6}\,q^9 - \tfrac{1}{6}\,q^{18} + \dots$$

Tenim la igualtat $f = g_1 + t\,g_2 + t^2\,g_3 + t^3\,g_4 + t^4\,g_5 + t^5\,g_6$. És fàcil comprovar que les formes cuspidals Galois conjugades de f s'obtenen pel procediment següent:

$$^{\sigma}f = \sum \psi_K(\mathfrak{a})\,\varepsilon(\mathfrak{a})\,q^{\mathrm{N}(\mathfrak{a})}\,,$$

on ε recorre el grup de caràcters $\widehat{\mathrm{Pic}(\mathcal{O}_3)}$. Si apliquem els operadors d'Atkin-Li, obtenim:

$$f \mid W_3 = \lambda_3\,f \otimes \chi_3 = \lambda_3\,\overline{f}\,;$$

$$f \mid W_{23} = \lambda_{23}\,f \otimes \chi_{23} = -f\,;$$

$$f \mid W_{69} = \lambda_{69}\,f \otimes \chi_{69} = -\lambda_3\,f \otimes \chi_3\,,$$

on

$$\lambda_3 = \frac{\sqrt{-3}}{a_3}\,, \quad \lambda_{23} = \frac{\sqrt{-23}}{a_{23}}\,, \quad \lambda_{69} = \lambda_3\,\lambda_{23}\,,$$

i $\chi_3 = \left(\frac{\ }{3}\right)$, $\chi_{23} = \left(\frac{\ }{23}\right)$, $\chi_{69} = \chi_3\,\chi_{23}$.

Nota. Recordem que tots els ideals de $K = \mathbb{Q}(\sqrt{-23})$ capitulen sobre el cos de Hilbert $K_{(1)}$. Així, per exemple, $2 = \mathfrak{a}\,\mathfrak{b}$ sobre K i

$$\mathfrak{a}\,\mathcal{O}_{K_{(1)}} = \left(-3\,\beta + 3\,\beta^2 - 3\,\beta^3 + 2\,\beta^4 - \beta^5\right)\,,$$

$$\mathfrak{b}\,\mathcal{O}_{K_{(1)}} = \left(-3 + 4\,\beta - 4\,\beta^2 + 4\,\beta^3 - 3\,\beta^4 + \beta^5\right)\,,$$

on, com abans, β és una arrel de $x^6 - 3\,x^5 + 5\,x^4 - 5\,x^3 + 5\,x^2 - 3\,x + 1$. Notem que un sistema d'unitats fonamentals del cos $K_{(1)}$ ve donat per: $\varepsilon_1 = 1 - \beta + 2\,\beta^2 - 2\,\beta^3 + \beta^4$ i $\varepsilon_2 = 2\,\beta - 2\,\beta^2 + 3\,\beta^3 - 2\,\beta^4 + \beta^5$.

Qüestió. Com podem utilitzar la informació anterior per determinar una forma parabòlica $h(z) \in S_2(\Gamma_1(69))$ tal que la diferencial regular $h(q)\,dq/q \in$

$H^0(A_f, \Omega^1)$ proporcioni els quocients optimals el·líptics amb CM associats. En d'altres paraules, per tal que

$$\Lambda = \left\{ 2\pi i \int_\eta h(z)\, dz \colon \eta \in H_1(X_1(69); \mathbb{Z}) \right\} \subset \mathbb{C}$$

sigui una ret. Llevat d'un factor transcendent calculat a partir de la funció Γ d'Euler, Λ serà proporcional a un ideal d'algun ordre de $K = \mathbb{Q}(\sqrt{-23})$.

Bibliografia

[B-Gro3] Buhler, J.P; Gross, B.H., *Arithmetic on elliptic curves with complex multiplication II*, Inventiones Math. **79**, 11–29 (1985).

[Deu] Deuring, M., *Die Klassenkörper er Komplexen Multiplication*, Ency. der Math. Wiss. Band I, 2. Teil. Heft 10, Teil II (1958).

[Gro1] Gross, B.H., *Arithmetic on elliptic curves with complex multiplication*, Lectures Notes in Mathematics, Vol. 776. Berlin-Heidelberg-New York: Springer (1980).

[Gro2] Gross, B.H., *Minimal models for elliptic curves with complex multiplication*, Compositio Math. **45**, 155–164 (1970).

[Lang] Lang, S., *Algebraic Number Theory*, Addison-Wesley Pub. Co., (1970).

[Ko] Koch, H., *Algebraic Number Theory*, Springer, (1997).

[Ne 86] Neukirch, J., *Class field theory*, Grundlehren der Matematischen Wissenschaft, 280 (1986).

[Sil1] Silverman, J.H., *The arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, (1992).

[Sil2] Silverman, J.H., *Advanced Topics on the Arithmetic of Elliptic Curves* , GTM 151, Springer-Verlag, (1994).

[Vla] Vladut, S.G., *Kronecker's Jugendtraum and Modular Functions*, Studies in the Development of Modern Mathematics, Vol. 2, Gordon and Breach Publishers (1991).

Capítol 5

Construcció de varietats abelianes amb CM

J. Fernández
Dept. de Matemàtica Aplicada 2
Universitat Politècnica de Catalunya
Pau Gargallo 5,
E-08028 Barcelona

Introducció

Sobre un cos de característica 0, les corbes el·líptiques amb multiplicació complexa es caracteritzen pel fet que la seva àlgebra d'endomorfismes és un cos quadràtic (que resulta ser imaginari). El nostre objectiu és generalitzar aquest concepte per a varietats abelianes de dimensió qualsevol.

Només considerarem varietats abelianes definides sobre $\mathbb{C}$. De fet, aquesta simplificació equival a *abandonar* la característica positiva, perquè tota varietat algebraica sobre un cos de característica 0 està definida sobre una extensió de $\mathbb{Q}$ finitament generada, la qual es pot veure com a subcòs de $\mathbb{C}$.

Tenint en compte el cas de les corbes el·líptiques, semblaria plausible considerar com a varietats abelianes amb multiplicació complexa (CM, per abreujar) aquelles tals que la seva àlgebra d'endomorfismes sigui un cos de nombres de grau igual a dues vegades la dimensió de la varietat. Si féssim això, estaríem forçant que les varietats abelianes amb CM fossin simples. Per poder considerar varietats no necessàriament simples, hem d'afeblir la

condició anterior, tal i com es fa a la següent definició de *varietat abeliana amb CM.*

Definició 5.0.1. *Sigui A una varietat abeliana (definida sobre $\mathbb{C}$) i suposem que existeix una immersió $\iota : F \hookrightarrow \mathrm{End}^0(A)$, on F és un cos de nombres de grau $2\dim(A)$. Es diu aleshores que (A, ι) és una* varietat abeliana de tipus F.

Observació 5.0.2. Com veurem més endavant, és important especificar quina és la immersió ι en cada cas.

Observació 5.0.3. Si F és un subcòs de l'àlgebra d'endomorfismes d'una varietat abeliana de dimensió n, es pot demostrar que el grau $[F : \mathbb{Q}]$ divideix $2n$. Les varietats abelianes amb CM, per tant, són aquelles tals que la seva àlgebra d'endomorfismes conté un cos de nombres de grau màxim.

Una condició necessària perquè (A, ι) sigui una varietat abeliana de tipus F és la que lliga, a la pròpia definició, la dimensió de la varietat amb el grau del cos de nombres; però n'hi ha més. Això és el que tractem a la secció 5.1, on també introduïm la noció de *CM-tipus.* A la secció 5.2, veurem com són els tors complexos associats a les varietats abelianes amb CM, i això ens conduirà al *teorema de construcció* de varietats abelianes amb CM (secció 5.3). A la secció 5.4, parlarem de morfismes entre varietats abelianes amb CM. Finalment, l'objectiu principal de la secció 5.5 serà la definició del *reflex* d'un CM-tipus.

5.1 Varietats abelianes amb CM

Sigui (A, ι) una varietat abeliana de tipus F. La varietat A i el cos F satisfan una colla de propietats que recollim a continuació en forma de proposicions. La majoria de resultats que es fan servir (p.e., a [Sh 98], pàgs. 35–40) per demostrar aquestes propietats són de teoria general d'àlgebres simples i de teoria de representacions de $\mathbb{Q}$-àlgebres.

Proposició 5.1.1. *El centralitzador de $\iota(F)$ a $\mathrm{End}^0(A)$ és $\iota(F)$.*

Proposició 5.1.2. *La varietat abeliana A és isògina a un producte B^h, on B és una varietat abeliana simple (determinada llevat d'isogènia).*

Proposició 5.1.3. *L'àlgebra d'endomorfismes del factor simple B de la varietat abeliana A és isomorfa, via la immersió natural* $\mathrm{End}^0(B) \hookrightarrow \mathrm{End}^0(A)$,

a un subcòs K de F amb $[K:\mathbb{Q}] = 2m$, on m és la dimensió de B. En particular, B és una varietat abeliana amb CM: si posem ι' per designar l'isomorfisme de K en $\mathrm{End}^0(B)$, tenim que (B,ι') és una varietat abeliana de tipus K.

Observació 5.1.4. La varietat abeliana B és simple. El cos K, per tant, ha de ser *totalment real* o bé un *cos CM* (és a dir, una extensió quadràtica totalment imaginària d'un cos totalment real).

Observació 5.1.5. L'àlgebra d'endomorfismes de la varietat abeliana A és isomorfa a l'àlgebra de matrius $\mathrm{M}_h(K)$. En particular, A és simple si, i només si, $\mathrm{End}^0(A)$ és un cos.

Proposició 5.1.6. *El cos F és totalment imaginari, i existeixen $n = \dim A$ $\mathbb{Q}$-immersions $\varphi_1,\ldots,\varphi_n$ de F en $\mathbb{C}$ tals que*

$$\rho_a^A\,\iota \;\simeq\; \varphi_1 \oplus \cdots \oplus \varphi_n\,,$$

on ρ_a^A és una representació analítica de $\mathrm{End}^0(A)$. A més, necessàriament, es té que

$$\overline{\varphi_i} \neq \varphi_j \quad \forall i,j \in \{1,\ldots,n\}.$$

Així doncs, de les $2n$ $\mathbb{Q}$-immersions del cos F en els complexos, n'hi ha la meitat de *distingides*, en el sentit que la seva suma directa és equivalent a la restricció a $\iota(F)$ d'una representació analítica (qualsevol) de $\mathrm{End}^0(A)$. Especificarem aquestes n immersions $\varphi_1,\ldots,\varphi_n$ dient que (A,ι) és una *varietat abeliana de tipus* $(F,\{\varphi_i\})$.

Podem aplicar la proposició 5.1.6 a la varietat abeliana B i el cos K. Només cal tenir present llavors l'observació 5.1.4, així com el fet que qualsevol representació analítica de $\mathrm{End}^0(A)$, restringida a $\iota'(K) = \mathrm{End}^0(B)$ via la immersió natural $\mathrm{End}^0(B) \hookrightarrow \mathrm{End}^0(A)$, és equivalent a la suma directa d'una representació analítica de $\mathrm{End}^0(B)$ amb ella mateixa h vegades, per obtenir la darrera de les propietats que ens interessen.

Proposició 5.1.7. *El cos K és un cos CM, i existeixen m $\mathbb{Q}$-immersions $\psi_1,\ldots,\psi_m$ de K en $\mathbb{C}$, amb $\overline{\psi_i} \neq \psi_j$ $\forall i,j \in \{1,\ldots,m\}$, tals que*

$$\rho_a^B\,\iota' \;\simeq\; \psi_1 \oplus \cdots \oplus \psi_m\,,$$

on ρ_a^B és una representació analítica de $\mathrm{End}^0(B)$. A més, les immersions $\psi_1,\ldots,\psi_m$ són precisament les $\mathbb{Q}$-immersions de K en $\mathbb{C}$ induïdes per les immersions $\varphi_1,\ldots,\varphi_n$ de la proposició 5.1.6.

Observació 5.1.8. És clar que $[F : K] = h$. En particular, si la varietat abeliana A no és simple, aleshores la inclusió del cos CM K en el cos totalment imaginari F és estricta.

La situació que acabem de descriure ens porta a la definició de *CM-tipus*. Suposem que tenim un cos de nombres F de grau $2n$ i que triem la meitat de les seves $\mathbb{Q}$-immersions en els complexos, $\varphi_1, \ldots, \varphi_n$.

Definició 5.1.9. *Es diu que el parell* $(F, \{\varphi_1, \ldots, \varphi_n\})$, *o bé simplement* $(F, \{\varphi_i\})$, *és un* CM-tipus *si existeixen una varietat abeliana* A *(de dimensió* n*) i una immersió* $\iota : F \hookrightarrow \mathrm{End}^0(A)$ *de forma que* (A, ι) *és de tipus* $(F, \{\varphi_i\})$, *és a dir, de forma que* $\rho_a^A \iota \simeq \varphi_1 \oplus \cdots \oplus \varphi_n$, *on* ρ_a^A *és una representació analítica de* $\mathrm{End}^0(A)$.

Perquè $(F, \{\varphi_i\})$ pugui ser un CM-tipus, és necessari que el cos F sigui totalment imaginari i que la conjugació complexa de cada immersió φ_i no coincideixi amb cap de les altres immersions (cf. proposició 5.1.6). Hi ha una altra condició necessària (cf. proposició 5.1.7) que ja implica aquestes dues (cf. observació 5.1.11) i que destaquem ara en forma de teorema. Necessitem abans la següent definició.

Definició 5.1.10. *Donat el parell* $(F, \{\varphi_i\})$, *sigui* K *un subcòs de* F *i siguin* $\psi_1, \ldots, \psi_m$ *les* $\mathbb{Q}$*-immersions de* K *en* $\mathbb{C}$ *induïdes per* $\varphi_1, \ldots, \varphi_n$. *Direm que* $(K, \{\psi_j\})$ *és un* CM-subcòs *de* $(F, \{\varphi_i\})$ *si* K *és un cos CM i*

$$\overline{\psi_i} \neq \psi_j \quad \forall i, j \in \{1, \ldots, m\}.$$

Observació 5.1.11. La darrera condició de la definició implica automàticament que

$$\overline{\varphi_i} \neq \varphi_j \quad \forall i, j \in \{1, \ldots, n\}.$$

En particular, el cos F és totalment imaginari, i el grau del cos de nombres K és $2m$ (perquè les seves $\mathbb{Q}$-immersions en $\mathbb{C}$ són $\psi_1, \ldots, \psi_m, \overline{\psi_1}, \ldots, \overline{\psi_m}$).

Teorema 5.1.12. *Si* $(F, \{\varphi_i\})$ *és un CM-tipus, aleshores té un CM-subcòs* $(K, \{\psi_j\})$.

El primer dels objectius que perseguim és demostrar que aquesta condició ja és suficient; això és el que fem al teorema 5.3.1. L'existència de varietats abelianes de tipus $(F, \{\varphi_i\})$, per tant, serà equivalent a l'existència d'un CM-subcòs del parell $(F, \{\varphi_i\})$.

5.2 Tors complexos amb CM

Per demostrar el recíproc del teorema 5.1.12, necessitem més informació sobre les varietats abelianes amb CM. Volem veure ara com són els tors complexos associats a aquestes varietats.

Suposem que (A, ι) és una varietat abeliana de tipus $(F, \{\varphi_1, \ldots, \varphi_n\})$. El grup de punts complexos de la varietat abeliana A és analíticament isomorf a un tor complex $\mathbb{C}^n/D$. La xarxa D ha de poder expressar-se en termes del cos F i les immersions $\varphi_1, \ldots, \varphi_n$. Vegem com (cf. [Sh 98], pàgs. 40–41).

El conjunt $\mathcal{O}$ format pels elements de F *que són endomorfismes de* A,

$$\iota(\mathcal{O}) = \iota(F) \cap \mathrm{End}(A),$$

és un ordre del cos F. Direm que $\mathcal{O}$ és l'*ordre* de (A, ι). Si designem per ρ_a la representació analítica de $\mathrm{End}^0(A)$ relativa al tor complex $\mathbb{C}^n/D$, és clar que

$$\mathcal{O} = \left\{\alpha \in F \;\middle|\; \rho_a(\iota(\alpha))\, D \subset D\right\}.$$

En particular, D és un $\mathcal{O}$-mòdul. De fet, es pot veure que és isomorf a un ideal $\mathfrak{m}$ de l'anell $\mathcal{O}$; concretament, $D = \rho_a(\iota(\mathfrak{m}))\, x$ per a algun $x \in \mathbb{C}^n$. D'aquí es dedueix immediatament que l'ordre de (A, ι) coincideix amb l'ordre de l'ideal $\mathfrak{m}$:

$$\mathcal{O} = \left\{\alpha \in F \;\middle|\; \alpha\, \mathfrak{m} \subset \mathfrak{m}\right\}.$$

Recordem que el *tipus* de la varietat (A, ι) ve determinat pel fet que

$$\rho_a \iota \;\simeq\; \varphi_1 \oplus \cdots \oplus \varphi_n.$$

Això vol dir que, en alguna base $(v_1, \ldots, v_n)$ de $\mathbb{C}^n$, per a tot $\alpha \in F$ la matriu de l'aplicació lineal $\rho_a(\iota(\alpha))$ és

$$S_\varphi(\alpha) := \mathrm{diag}(\alpha^{\varphi_1}, \ldots, \alpha^{\varphi_n}).$$

Si $(x_1, \ldots, x_n)$ són les coordenades del punt x en aquesta base, aleshores les dels punts de la xarxa D són

$$\left\{(x_1\alpha^{\varphi_1}, \ldots, x_n\alpha^{\varphi_n}) \;\middle|\; \alpha \in \mathfrak{m}\right\}.$$

En particular, totes les coordenades x_i són diferents de 0 (altrament, tindríem la xarxa D continguda en un subespai propi de $\mathbb{C}^n$). Per tant, podem

fer el canvi de base $v_i \mapsto u_i := x_i v_i$. En la nova base $(u_1, \ldots, u_n)$, la representació matricial dels endomorfismes $\rho_a(\iota(\alpha))$ continua sent la mateixa, mentre que la xarxa D ve donada per $\varphi(\mathfrak{m})$, on, per a tot $\alpha \in F$,

$$\varphi(\alpha) := (\alpha^{\varphi_1}, \ldots, \alpha^{\varphi_n}).$$

Observació 5.2.1. Acabem d'introduir una aplicació $\mathbb{Q}$-lineal $\varphi : F \hookrightarrow \mathbb{C}^n$ i una immersió de $\mathbb{Q}$-àlgebres $S_\varphi : F \hookrightarrow \mathrm{M}_n(\mathbb{C})$ que farem servir constantment a partir d'ara, identificant sovint les matrius $S_\varphi(\alpha)$ amb els endomorfismes de $\mathbb{C}^n$ que defineixen de forma canònica.

Finalment, el canvi de base $u_i \mapsto e_i$, on $(e_1, \ldots, e_n)$ és la base canònica de $\mathbb{C}^n$, dóna un isomorfisme de tors complexos

$$\mathbb{C}^n/D \xrightarrow{\simeq} \mathbb{C}^n/\varphi(\mathfrak{m}).$$

A més, si $\widetilde{\rho}_a$ és la representació analítica de $\mathrm{End}^0(A)$ relativa al tor complex $\mathbb{C}^n/\varphi(\mathfrak{m})$, per a tot $\alpha \in F$ es té que $\widetilde{\rho}_a(\iota(\alpha)) = S_\varphi(\alpha)$. Hem arribat així al següent resultat.

Teorema 5.2.2. *Si (A, ι) és una varietat abeliana de tipus $(F, \{\varphi_i\})$, aleshores existeixen un $\mathbb{Z}$-mòdul lliure $\mathfrak{m} \subset F$ de rang $2n$ i un isomorfisme*

$$\theta : A \xrightarrow{\simeq} \mathbb{C}^n/\varphi(\mathfrak{m})$$

tals que:

1. *L'ordre de (A, ι) és $\mathcal{O} = \{\alpha \in F \mid \alpha\mathfrak{m} \subset \mathfrak{m}\}$.*
2. *Per a tot $\alpha \in \mathcal{O}$, es té el diagrama commutatiu*

$$\begin{tikzcd} A \arrow[r, "\theta"] \arrow[d, "\iota(\alpha)"'] & \mathbb{C}^n/\varphi(\mathfrak{m}) \arrow[d, "S_\varphi(\alpha)"] \\ A \arrow[r, "\theta"] & \mathbb{C}^n/\varphi(\mathfrak{m}). \end{tikzcd}$$

Resumirem l'enunciat d'aquest teorema dient que (A, ι) és una *varietat abeliana de tipus* $(F, \{\varphi_i\}, \mathfrak{m})$. Sembla natural fer-se la següent pregunta: si prenem qualsevol $\mathbb{Z}$-mòdul lliure $\mathfrak{m} \subset F$ de rang màxim, és llavors $\mathbb{C}^n/\varphi(\mathfrak{m})$ una varietat abeliana de tipus $(F, \{\varphi_i\})$? El resultat de la propera secció ens dóna una resposta afirmativa, sempre i quan el parell $(F, \{\varphi_i\})$ tingui un CM-subcòs (cf. teorema 5.1.12).

Abans d'arribar al *teorema de construcció* de varietats abelianes amb CM, aprofitem el resultat anterior per deduir-ne la següent conseqüència.

Corol·lari 5.2.3. *Si (A,ι) i (A',ι') són varietats abelianes del mateix CM-tipus $(F,\{\varphi_i\})$, aleshores són isògines.*

Demostració. Pel teorema 5.2.2, existeixen isomorfismes

$$\theta : A \to \mathbb{C}^n/\varphi(\mathfrak{m}) \qquad \text{i} \qquad \theta' : A' \to \mathbb{C}^n/\varphi(\mathfrak{m}'),$$

amb $\mathfrak{m}$ i $\mathfrak{m}'$ $\mathbb{Z}$-submòduls lliures de F de rang $2n$. Només cal veure llavors que els tors complexos $\mathbb{C}^n/\varphi(\mathfrak{m})$ i $\mathbb{C}^n/\varphi(\mathfrak{m}')$ són isògins.

En efecte, com que el rang de $\mathfrak{m}$ i $\mathfrak{m}'$ és màxim, existeix algun enter no-nul g tal que $g\,\mathfrak{m} \subset \mathfrak{m}'$. L'automorfisme de $\mathbb{C}^n$ obtingut per multiplicació per l'enter g defineix, per tant, una isogènia

$$g : \mathbb{C}^n/\varphi(\mathfrak{m}) \longrightarrow \mathbb{C}^n/\varphi(\mathfrak{m}'),$$

i $\lambda := (\theta')^{-1} g\theta$ és llavors una isogènia $A \to A'$. □

Observació 5.2.4. Amb les notacions de la demostració del corol·lari, és clar que $S_\varphi(\alpha)\,g = g\,S_\varphi(\alpha) \quad \forall \alpha \in F$. Per tant, tornant a fer servir el teorema 5.2.2, tenim que la isogènia λ *commuta amb l'operació de* F:

$$\iota'(\alpha)\,\lambda = \lambda\,\iota(\alpha) \quad \forall \alpha \in F.$$

5.3 El teorema de construcció

Considerem un cos de nombres F de grau $2n$, i siguin $\varphi_1,\ldots,\varphi_n$ la meitat de les seves $\mathbb{Q}$-immersions en els complexos. El següent resultat, en combinació amb el teorema 5.1.12, dóna una condició necessària i suficient perquè el parell $(F,\{\varphi_i\})$ sigui un CM-tipus. A més, en aquest cas, diu com construir varietats abelianes de tipus $(F,\{\varphi_i\})$; el teorema 5.2.2 ens assegura llavors que aquestes seran, llevat d'isomorfisme, totes les varietats abelianes d'aquest tipus.

Teorema 5.3.1. *Suposem que $(F,\{\varphi_i\})$ admet $(K,\{\psi_1,\ldots,\psi_m\})$ com a CM-subcòs. Sigui $\mathfrak{m} \subset F$ un $\mathbb{Z}$-mòdul lliure de rang $2n$, i considerem el seu ordre, $\mathcal{O} = \{\alpha \in F \mid \alpha\,\mathfrak{m} \subset \mathfrak{m}\}$. Aleshores, $\mathfrak{m}$ defineix una varietat abeliana amb CM d'ordre $\mathcal{O}$:*

1. *$\mathbb{C}^n/\varphi(\mathfrak{m})$ és una varietat abeliana.*

2. *Es té una immersió d'anells* $S_\varphi : \mathcal{O} \hookrightarrow \mathrm{End}\,(\mathbb{C}^n/\varphi(\mathfrak{m}))$ *definida, per a tot* $\alpha \in \mathcal{O}$*, pel diagrama commutatiu*

$$\begin{array}{ccc} \mathbb{C}^n & \xrightarrow{S_\varphi(\alpha)} & \mathbb{C}^n \\ \downarrow & & \downarrow \\ \mathbb{C}^n/\varphi(\mathfrak{m}) & \xrightarrow{S_\varphi(\alpha)} & \mathbb{C}^n/\varphi(\mathfrak{m}). \end{array}$$

Per tant, és té una immersió de $\mathbb{Q}$*-àlgebres* $S_\varphi : F \hookrightarrow \mathrm{End}^0\,(\mathbb{C}^n/\varphi(\mathfrak{m}))$*, i* $(\mathbb{C}^n/\varphi(\mathfrak{m}), S_\varphi)$ *és una varietat abeliana de tipus* $(F, \{\varphi_i\})$*.*

Demostració. Dels dos punts de l'enunciat del teorema, el realment important és el primer. El segon és immediat; només cal tenir presents els següents fets:

- La representació analítica de $\mathrm{End}^0\,(\mathbb{C}^n/\varphi(\mathfrak{m}))$ estableix un isomorfisme entre l'anell $\mathrm{End}\,(\mathbb{C}^n/\varphi(\mathfrak{m}))$ i el següent subanell de $\mathrm{End}(\mathbb{C}^n)$:

$$\left\{ f \in \mathrm{End}(\mathbb{C}^n) \;\middle|\; f\,\varphi(\mathfrak{m}) \subset \varphi(\mathfrak{m}) \right\}.$$

- La imatge de la immersió $S_\varphi : F \hookrightarrow \mathrm{End}(\mathbb{C}^n)$ restringida a $\mathcal{O}$ està inclosa en el subanell anterior:

$$S_\varphi(\alpha)\,\varphi(\mathfrak{m}) \subset \varphi(\mathfrak{m}) \quad \forall \alpha \in \mathcal{O}.$$

Quant a la demostració del primer punt, vegem primer que $\mathbb{C}^n/\varphi(\mathfrak{m})$ és un tor complex. Si suposem que $\mathfrak{m} = \langle \alpha_1, \ldots, \alpha_{2n} \rangle_{\mathbb{Z}}$, aleshores

$$\varphi(\mathfrak{m}) = \langle \varphi(\alpha_1), \ldots, \varphi(\alpha_{2n}) \rangle_{\mathbb{Z}}.$$

Per demostrar que $\varphi(\mathfrak{m})$ és una xarxa a $\mathbb{C}^n$, només cal veure que els vectors $\varphi(\alpha_1), \ldots, \varphi(\alpha_{2n})$ de $\mathbb{C}^n$ són linealment independents sobre $\mathbb{R}$, és a dir, que la matriu

$$\begin{pmatrix} \varphi(\alpha_1) & \overline{\varphi(\alpha_1)} \\ \vdots & \\ \vdots & \\ \varphi(\alpha_{2n}) & \overline{\varphi(\alpha_{2n})} \end{pmatrix} = \begin{pmatrix} \alpha_1^{\varphi_1} & \cdots & \alpha_1^{\varphi_n} & \alpha_1^{\overline{\varphi_1}} & \cdots & \alpha_1^{\overline{\varphi_n}} \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{2n}^{\varphi_1} & \cdots & \alpha_{2n}^{\varphi_n} & \alpha_{2n}^{\overline{\varphi_1}} & \cdots & \alpha_{2n}^{\overline{\varphi_n}} \end{pmatrix}$$

és invertible. En efecte: $\varphi_1, \ldots, \varphi_n, \overline{\varphi_1}, \ldots, \overline{\varphi_n}$ són totes les $\mathbb{Q}$-immersions de F en $\mathbb{C}$, i $\{\alpha_1, \ldots, \alpha_{2n}\}$ és una $\mathbb{Q}$-base de F (de forma que el determinant de la matriu anterior és precisament el discriminant d'aquesta base).

La demostració que el tor complex $\mathbb{C}^n/\varphi(\mathfrak{m})$ és una varietat abeliana consta de dues parts (cf. [Sh 98], pàgs. 42–44):

(A) Primer es demostra que $\mathbb{C}^n/\varphi(\mathfrak{m})$ és isògin a $(\mathbb{C}^m/\Delta)^h$ per a alguna xarxa Δ de $\mathbb{C}^m$, on $2m = [K : \mathbb{Q}]$ (cf. observació 5.1.11) i $h := [F : K]$.

(B) Aleshores, es demostra que $\mathbb{C}^m/\Delta$ és una varietat abeliana (és a dir, que admet una forma de Riemann); fent servir (A), es té llavors que $\mathbb{C}^n/\varphi(\mathfrak{m})$ també ho és.

Observació 5.3.2. En particular, si la inclusió del cos CM K en F és estricta, aleshores la varietat abeliana $\mathbb{C}^n/\varphi(\mathfrak{m})$ no és simple.

Vegem la demostració de (A). Fixem al cos K un $\mathbb{Z}$-mòdul lliure de rang màxim, $\mathfrak{n} = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_{2m}\mathbb{Z}$, i al cos F una K-base $\{\gamma_1, \ldots, \gamma_h\}$. Aleshores,

$$\mathfrak{m}' \;:=\; \gamma_1\mathfrak{n} \oplus \cdots \oplus \gamma_h\mathfrak{n} \;=\; \bigoplus_{k,j} \gamma_k\beta_j\mathbb{Z}$$

és un $\mathbb{Z}$-submòdul lliure de F de rang $2n$. Tal com hem vist a la demostració del corol·lari 5.2.3, els tors complexos $\mathbb{C}^n/\varphi(\mathfrak{m})$ i $\mathbb{C}^n/\varphi(\mathfrak{m}')$ són isògins. Tenim que

$$\varphi(\mathfrak{m}') \;=\; \Delta_1 \oplus \cdots \oplus \Delta_h\,,$$

on, per a tot $k \in \{1, \ldots, h\}$,

$$\Delta_k \;:=\; \varphi(\gamma_k\mathfrak{n}) \;=\; \langle \varphi(\gamma_k\beta_1), \ldots, \varphi(\gamma_k\beta_{2m}) \rangle_{\mathbb{Z}}\,.$$

Donat que $\varphi(\mathfrak{m}')$ és una xarxa a $\mathbb{C}^n$, els $2n$ vectors $\varphi(\gamma_k\beta_j)$ són linealment independents sobre $\mathbb{R}$; si, associat a cada grup Δ_k, definim

$$V_k \;:=\; \varphi(\gamma_k\beta_1)\mathbb{R} \oplus \cdots \oplus \varphi(\gamma_k\beta_{2m})\mathbb{R}\,,$$

aleshores és clar que, com a $\mathbb{R}$-espais vectorials,

$$\mathbb{C}^n \;=\; V_1 \oplus \cdots \oplus V_h\,.$$

Lema 5.3.3. *V_k és un $\mathbb{C}$-espai vectorial de $\mathbb{C}^n$, és a dir, $\sqrt{-1}\,V_k \subset V_k$.*

Per tant, la darrera igualtat és vàlida com a $\mathbb{C}$-espais vectorials. A més, per a cada $k \in \{1, \ldots, h\}$, el quocient V_k/Δ_k és un tor complex; i el producte directe $(V_1/\Delta_1) \times \cdots \times (V_h/\Delta_h)$ és isomorf a

$$(V_1 \oplus \cdots \oplus V_h)/(\Delta_1 \oplus \cdots \oplus \Delta_h) \;=\; \mathbb{C}^n/\varphi(\mathfrak{m}').$$

Siguin ara ψ i S_ψ les immersions del cos K (en $\mathbb{C}^m$ i en $\mathrm{M}_m(\mathbb{C})$, respectivament) definides a partir de $\psi_1, \ldots, \psi_m$, de forma anàloga a φ i S_φ. Aplicant a $\mathfrak{n}$ el que hem demostrat més amunt per a $\mathfrak{m}$, tenim que

$$\Delta \;:=\; \psi(\mathfrak{n}) \;=\; \langle \psi(\beta_1), \ldots, \psi(\beta_{2m}) \rangle_{\mathbb{Z}}$$

és una xarxa a $\mathbb{C}^m$. El següent lema ens diu que cada tor complex V_k/Δ_k és isomorf a $\mathbb{C}^m/\Delta$. Així doncs, el tor complex de partida, $\mathbb{C}^n/\varphi(\mathfrak{m})$, és isògin a $(\mathbb{C}^m/\Delta)^h$.

Lema 5.3.4. *L'isomorfisme de $\mathbb{R}$-espais vectorials*

$$\begin{array}{rccc} \delta_k : & \mathbb{C}^m & \longrightarrow & V_k \\ & \psi(\beta_j) & \longmapsto & \varphi(\gamma_k \beta_j) \end{array}$$

és $\mathbb{C}$-lineal, és a dir, $\delta_k(\sqrt{-1}\,x) = \sqrt{-1}\,\delta_k(x) \;\; \forall x \in \mathbb{C}^m$.
A més és clar que $\delta_k(\Delta) = \Delta_k$.

Finalment, vegem la demostració de (B). Volem construir una forma hermítica i definida positiva $H : \mathbb{C}^m \times \mathbb{C}^m \longrightarrow \mathbb{C}$ tal que $\operatorname{Im} H(\Delta \times \Delta) \subset \mathbb{Z}$. Recordem que el cos K és una extensió quadràtica totalment imaginària d'un cos totalment real K_0. Les m immersions de K_0 en $\mathbb{R}$ són precisament les induïdes per $\psi_1, \ldots, \psi_m$. Del teorema d'aproximació aplicat a K_0 se segueix immediatament el següent lema.

Lema 5.3.5. *Existeix $\zeta \in K$ amb $K = K_0(\zeta)$ i $\zeta^2 \in K_0$ (en particular, ζ és totalment imaginari pur i ζ^2 és totalment negatiu) tal que*

$$\operatorname{Im}(\zeta^{\psi_j}) > 0 \quad \forall j \in \{1, \ldots, m\}.$$

Podem considerar llavors la forma hermítica H definida per la matriu diagonal $2\operatorname{diag}\big(\operatorname{Im}(\zeta^{\psi_1}), \ldots, \operatorname{Im}(\zeta^{\psi_m})\big)$: donats dos vectors $x = (x_1, \ldots, x_m)$ i $y = (y_1, \ldots, y_m)$ de $\mathbb{C}^m$,

$$H(x,y) \;:=\; 2\sum_{j=1}^{m} \operatorname{Im}(\zeta^{\psi_j})\, x_j\, \overline{y_j} \;=\; -2\sqrt{-1}\sum_{j=1}^{m} \zeta^{\psi_j}\, x_j\, \overline{y_j}.$$

És clar que H és definida positiva. La seva part imaginària es calcula fàcilment:

$$\operatorname{Im} H(x,y) \;=\; \sum_{j=1}^{m} \zeta^{\psi_j}\,(\overline{x_j}\,y_j \;-\; x_j\,\overline{y_j})\,.$$

Volem veure què passa en restringir-la a $\Delta \times \Delta$. Fent servir que l'automorfisme no-trivial de K sobre K_0 és la conjugació complexa (a qualsevol $\mathbb{Q}$-immersió de K en $\mathbb{C}$), obtenim que, per a $\alpha, \beta \in K$,

$$\operatorname{Im} H\,(\psi(\alpha), \psi(\beta)) \;=\; \operatorname{tr}_{K/\mathbb{Q}}(\zeta\,\overline{\alpha}\,\beta)\,.$$

Com que $\Delta = \psi(\mathfrak{n})$, tenim doncs que $\operatorname{Im} H(\Delta \times \Delta) \subset \operatorname{tr}_{K/\mathbb{Q}}(\zeta\,\overline{\mathfrak{n}}\,\mathfrak{n})$. Ara bé, com que el $\mathbb{Z}$-mòdul $\mathfrak{n}$ és finitament generat, existeix algun enter positiu g tal que $g(\zeta\,\overline{\mathfrak{n}}\,\mathfrak{n})$ està contingut a l'anell d'enters del cos K. Aleshores,

$$g \operatorname{Im} H(\Delta \times \Delta) \;\subset\; \mathbb{Z}\,,$$

i gH és una forma de Riemann a $\mathbb{C}^m/\Delta$. □

Amb les notacions de la demostració, és fàcil veure que

$$H\,(x,\, S_\psi(\beta)\,y) \;=\; H\,\big(S_\psi(\overline{\beta})\,x,\, y\big) \qquad \forall \beta \in K\,. \tag{5.1}$$

Es té de fet el següent resultat (cf. [Sh 98], pàgs. 44–45).

Teorema 5.3.6. *Siguin K, K_0, $\psi_1, \ldots, \psi_m$ i Δ com al teorema 5.3.1 i a la seva demostració.*

1. *Si la varietat abeliana $\mathbb{C}^m/\Delta$ és simple, aleshores tota forma de Riemann H a $\mathbb{C}^m/\Delta$ satisfà la propietat (5.1).*

2. *Si H és una forma de Riemann a $\mathbb{C}^m/\Delta$ que satisfà (5.1), aleshores*

$$H(x,y) \;=\; 2\sum_{j=1}^{m} \operatorname{Im}(\zeta^{\psi_j})\,x_j\,\overline{y_j}$$

per a algun $\zeta \in K$ amb $\zeta^2 \in K_0$ totalment negatiu i tal que

$$\operatorname{Im}(\zeta^{\psi_j}) > 0 \quad \forall j \in \{1, \ldots, m\}\,.$$

5.4 Isogènies i grup de classes d'ideals

Fixem un CM-tipus $(F, \{\varphi_1, \ldots, \varphi_n\})$. A la secció 5.2, hem vist que totes les varietats abelianes d'aquest tipus són isògenes. El que ens demanem ara és el següent: si ens restringim al subconjunt format per les varietats d'un determinat ordre $\mathcal{O}$ del cos F, quantes classes d'isomorfisme n'hi ha? Donarem resposta a aquesta qüestió en el cas que l'ordre $\mathcal{O}$ sigui el maximal: llevat que s'indiqui el contrari, totes les varietats abelianes (A, ι) de tipus F en aquesta secció seran *principals*, és a dir, tals que

$$\iota(\mathcal{O}_F) \;=\; \iota(F) \cap \mathrm{End}(A)\,,$$

on $\mathcal{O}_F$ és l'anell d'enters del cos F.

Inspirem-nos en el cas de dimensió 1 (cf. [Si 94], pàgs. 96–103). Donat un cos quadràtic imaginari K, podem considerar el conjunt $\mathcal{ELL}(\mathcal{O}_K)$ de les classes d'isomorfisme de corbes el·líptiques E (definides sobre $\mathbb{C}$) amb CM per l'anell d'enters del cos K, és a dir, tals que $\mathrm{End}(E) \simeq \mathcal{O}_K$ (on aquest isomorfisme es considera *normalitzat*, en el sentit que fa correspondre cada endomorfisme de E amb la seva representació analítica i no pas amb el conjugat complex d'aquesta). El conjunt $\mathcal{ELL}(\mathcal{O}_K)$ està en bijecció amb el grup H_K de classes d'ideals del cos K, i una forma d'obtenir aquesta bijecció és la següent: fixada una corba el·líptica $\mathbb{C}/\Lambda$ de $\mathcal{ELL}(\mathcal{O}_K)$, cada ideal $\mathfrak{a}$ de K defineix un element $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ de $\mathcal{ELL}(\mathcal{O}_K)$ que només depèn de la classe de l'ideal $\mathfrak{a}$ a H_K. Considerem un parell d'observacions al respecte:

- Que la (classe d'isomorfisme de la) corba el·líptica $\mathbb{C}/\Lambda$ sigui un element de $\mathcal{ELL}(\mathcal{O}_K)$ és equivalent a dir que $\mathcal{O}_K = \{\alpha \in \mathbb{C} \,|\, \alpha\,\Lambda \subset \Lambda\}$. Per tant, si l'ideal $\mathfrak{a}$ es pren enter, aleshores l'endomorfisme identitat de $\mathbb{C}$ indueix una isogènia natural

  $$\pi_{\mathfrak{a}} : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\mathfrak{a}^{-1}\Lambda\,.$$

  El seu nucli, $\mathfrak{a}^{-1}\Lambda/\Lambda$, es podria pensar com el conjunt de punts de $\mathbb{C}/\Lambda$ que s'anul·len en *multiplicar-los per l'ideal* $\mathfrak{a}$. Aquesta isogènia és el precedent en dimensió 1 del concepte de $\mathfrak{a}$-*multiplicació*, que és el que farem servir per generalitzar la bijecció anterior per al cas de varietats abelianes (principals) de tipus $(F, \{\varphi_i\})$.

- Donades $E_1, E_2 \in \mathcal{ELL}(\mathcal{O}_K)$ i una isogènia $\lambda : E_1 \to E_2$, no és difícil demostrar que λ *commuta amb l'operació de* K, és a dir, que, per a

tot $\alpha \in \mathcal{O}_K$, es té el diagrama commutatiu

$$\begin{array}{ccc} E_1 & \xrightarrow{\lambda} & E_2 \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ E_1 & \xrightarrow{\lambda} & E_2\,. \end{array}$$

La definició *correcta* d'isomorfisme entre varietats abelianes amb CM haurà d'incloure aquesta propietat. Això ens condueix al concepte de *F-morfisme.*

Definició 5.4.1. *Siguin (A_1, ι_1) i (A_2, ι_2) varietats abelianes de tipus F, i considerem un morfisme $\lambda : A_1 \to A_2$. Direm que λ és un F-*morfisme*, o també un* morfisme de (A_1, ι_1) en (A_2, ι_2), *i escriurem*

$$\lambda : (A_1, \iota_1) \longrightarrow (A_2, \iota_2)\,,$$

si, per a tot $\alpha \in \mathcal{O}_F$, el següent diagrama commuta:

$$\begin{array}{ccc} A_1 & \xrightarrow{\lambda} & A_2 \\ {\scriptstyle\iota_1(\alpha)}\downarrow & & \downarrow{\scriptstyle\iota_2(\alpha)} \\ A_1 & \xrightarrow{\lambda} & A_2\,. \end{array}$$

*Es defineixen anàlogament els conceptes de F-*isomorfisme *i F-*endomorfisme.

En el que segueix, és important la proposició 5.1.1. Una altra forma d'enunciar-la és aquesta.

Lema 5.4.2. *Si (A, ι) és una varietat abeliana de tipus F i ordre $\mathcal{O}$, aleshores tot endomorfisme de (A, ι) és de la forma $\iota(\alpha)$ per a algun $\alpha \in \mathcal{O}$.*

Fixem ara, fins al final de la secció, una varietat abeliana (A, ι) de tipus $(F, \{\varphi_i\}, \mathfrak{m})$. Fent servir la definició 5.4.1, i tenint en compte la hipòtesi de principalitat, això vol dir (cf. teorema 5.2.2) que $\mathfrak{m}$ és un ideal (fraccionari) de F i que existeix un isomorfisme

$$\theta : (A, \iota) \longrightarrow (\mathbb{C}^n/\varphi(\mathfrak{m}), S_\varphi)\,.$$

Sigui $\mathfrak{a}$ un ideal enter (no-nul) de F. Donat que $\mathfrak{m} \subset \mathfrak{a}^{-1}\mathfrak{m}$, el morfisme identitat a $\mathbb{C}^n$ indueix una isogènia natural

$$\pi_{\mathfrak{a}} : (\mathbb{C}^n/\varphi(\mathfrak{m}), S_\varphi) \longrightarrow \left(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}), S_\varphi\right)\,.$$

A més, del fet que $\mathfrak{m}$ és un ideal de F, es dedueix que la varietat abeliana $\big(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}), S_\varphi\big)$ també és principal. Mòdul isomorfisme, això és el que entendrem per una $\mathfrak{a}$-*transformació* (cf. [La 83], pàgs. 55–60).

Definició 5.4.3. *Siguin (A', ι') una varietat abeliana (principal) de tipus F i λ un morfisme de (A, ι) en (A', ι'). Direm que λ és una* $\mathfrak{a}$-multiplicació, *i que (A', ι') és una* $\mathfrak{a}$-transformació de (A, ι), *si $\lambda \simeq \pi_\mathfrak{a}$, és a dir, si existeix un isomorfisme de (A', ι') en $\big(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}), S_\varphi\big)$ que faci commutatiu el diagrama següent:*

$$\begin{array}{ccc} (A, \iota) & \xrightarrow{\theta} & (\mathbb{C}^n/\varphi(\mathfrak{m}), S_\varphi) \\ {\scriptstyle\lambda}\big\downarrow & & \big\downarrow{\scriptstyle\pi_\mathfrak{a}} \\ (A', \iota') & \xrightarrow{\simeq} & \big(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}), S_\varphi\big) \end{array} .$$

En particular, (A', ι') és una varietat abeliana de tipus $(F, \{\varphi_i\}, \mathfrak{a}^{-1}\mathfrak{m})$.

Observació 5.4.4. La definició anterior no depèn de l'ideal $\mathfrak{m}$ que representi la varietat abeliana (A, ι).

Per al nostre objectiu, necessitem veure que la classe de F-isomorfisme d'una $\mathfrak{a}$-transformació de (A, ι) està unívocament determinada per la classe de l'ideal $\mathfrak{a}$ al grup H_F. Només cal comprovar el següent resultat.

Proposició 5.4.5. *Donats $\mathfrak{a}$ i $\mathfrak{b}$ ideals enters (no-nuls) de F, les varietats abelianes $\big(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}), S_\varphi\big)$ i $\big(\mathbb{C}^n/\varphi(\mathfrak{b}^{-1}\mathfrak{m}), S_\varphi\big)$ són isomorfes si, i només si, existeix algun $\alpha \in F$ tal que $\mathfrak{a} = \alpha\,\mathfrak{b}$.*

Demostració. Si $\mathfrak{a} = \alpha\,\mathfrak{b}$ per a algun $\alpha \in F$, aleshores és clar que $S_\varphi(\alpha)$ indueix un isomorfisme de $\big(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}), S_\varphi\big)$ en $\big(\mathbb{C}^n/\varphi(\mathfrak{b}^{-1}\mathfrak{m}), S_\varphi\big)$. Recíprocament, donat un isomorfisme ϑ, tenim que $\pi_\mathfrak{b}^{-1}\vartheta\,\pi_\mathfrak{a}$ és un element de l'àlgebra d'endomorfismes de $(\mathbb{C}^n/\varphi(\mathfrak{m}), S_\varphi)$; pel lema 5.4.2, ha de ser de la forma $S_\varphi(\alpha)$ per a algun $\alpha \in F$. En particular, la representació analítica de ϑ és precisament $S_\varphi(\alpha)$. Donat que ϑ és un isomorfisme, tenim que

$$\varphi(\alpha\,\mathfrak{a}^{-1}\mathfrak{m}) \;=\; S_\varphi(\alpha)\,\varphi(\mathfrak{a}^{-1}\mathfrak{m}) \;=\; \varphi(\mathfrak{b}^{-1}\mathfrak{m}),$$

d'on $\mathfrak{a} = \alpha\,\mathfrak{b}$. □

Finalment, vegem que qualsevol varietat abeliana (principal) de tipus $(F, \{\varphi_i\})$ es pot obtenir a partir de (A, ι) fent alguna $\mathfrak{a}$-multiplicació.

Proposició 5.4.6. *Si (A_1, ι_1) i (A_2, ι_2) són varietats abelianes de tipus $(F, \{\varphi_i\})$, aleshores (A_2, ι_2) és una $\mathfrak{a}$-transformació de (A_1, ι_1) per a algun ideal enter (no-nul) $\mathfrak{a}$ de F.*

Demostració. Suposem que cada (A_j, ι_j) és de tipus $(F, \{\varphi_i\}, \mathfrak{m}_j)$. Només cal veure llavors que $(\mathbb{C}^n/\varphi(\mathfrak{m}_2), S_\varphi)$ és una $\mathfrak{a}$-transformació de $(\mathbb{C}^n/\varphi(\mathfrak{m}_1), S_\varphi)$ per a algun ideal $\mathfrak{a} \subset \mathcal{O}_F$, és a dir, que existeixen una isogènia

$$\lambda : (\mathbb{C}^n/\varphi(\mathfrak{m}_1), S_\varphi) \longrightarrow (\mathbb{C}^n/\varphi(\mathfrak{m}_2), S_\varphi)$$

i un isomorfisme

$$(\mathbb{C}^n/\varphi(\mathfrak{m}_2), S_\varphi) \xrightarrow{\simeq} \left(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}_1), S_\varphi\right)$$

tals que el diagrama següent sigui commutatiu:

$$\begin{tikzcd}
 & (\mathbb{C}^n/\varphi(\mathfrak{m}_1), S_\varphi) \arrow[dl, "\lambda"'] \arrow[d, "\pi_{\mathfrak{a}}"] \\
(\mathbb{C}^n/\varphi(\mathfrak{m}_2), S_\varphi) \arrow[r, "\simeq"] & \left(\mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m}_1), S_\varphi\right) .
\end{tikzcd}$$

Com a isogènia λ, podem prendre $S_\varphi(\alpha)$ per a qualsevol element α no-nul de $\mathfrak{m}_1^{-1}\mathfrak{m}_2$; si volem llavors que el seu nucli,

$$S_\varphi(\alpha)^{-1}\,\varphi(\mathfrak{m}_2)/\varphi(\mathfrak{m}_1) \;=\; \varphi(\alpha^{-1}\mathfrak{m}_2)/\varphi(\mathfrak{m}_1)\,,$$

coincideixi amb el de $\pi_{\mathfrak{a}}$, l'ideal $\mathfrak{a}$ que cal prendre és $\alpha\,\mathfrak{m}_1\mathfrak{m}_2^{-1}$. Tenim aleshores que $\mathfrak{a}^{-1}\mathfrak{m}_1 = \alpha^{-1}\mathfrak{m}_2$, i l'isomorfisme

$$S_\varphi(\alpha^{-1}) : (\mathbb{C}^n/\varphi(\mathfrak{m}_2), S_\varphi) \xrightarrow{\simeq} \left(\mathbb{C}^n/\varphi(\alpha^{-1}\mathfrak{m}_2), S_\varphi\right)$$

tanca el diagrama. □

Corol·lari 5.4.7. *Hi ha una bijecció entre el conjunt de classes de F-isomorfisme de varietats abelianes (principals) de tipus $(F, \{\varphi_i\})$ i el grup de classes d'ideals de F.*

5.5 CM-tipus i teoria de Galois

Què se'n pot dir, dels cossos de definició de les varietats abelianes amb CM? Un dels resultats clàssics al respecte (cf. [Sh 98], pàgs. 65–66) ens relaciona aquests cossos de definició amb els dels endomorfismes de l'ordre de la varietat.

Teorema 5.5.1. *Sigui (A, ι) una varietat abeliana de tipus $(F, \{\varphi_i\})$ i d'ordre $\mathcal{O}$, i sigui $\widetilde{K}$ el cos reflex del CM-tipus $(F, \{\varphi_i\})$. Suposem que k és un cos de definició per a la varietat A. Si els endomorfismes de $\iota(\mathcal{O})$ estan definits sobre k, aleshores $\widetilde{K} \subset k$. Recíprocament, si el CM-tipus $(F, \{\varphi_i\})$ és primitiu i $\widetilde{K} \subset k$, aleshores tots els endomorfismes de A estan definits sobre k.*

Per entendre, com a mínim, l'enunciat d'aquest teorema, necessitem introduir els conceptes de *CM-tipus primitiu* i de *reflex d'un CM-tipus.* Això és el que pretenem fer en aquesta darrera secció (cf. [Sh 98], pàgs. 59–64).

Fixem un CM-tipus $(F, \{\varphi_1, \ldots, \varphi_n\})$. Pel teorema 5.1.12, sabem que té un CM-subcòs $(K, \{\psi_1, \ldots, \psi_m\})$. Sigui $L/\mathbb{Q}$ una extensió de Galois finita amb $F \subset L$ i amb grup de Galois G. Si posem S per designar el conjunt dels elements de G que indueixen les immersions $\varphi_1, \ldots, \varphi_n$, és clar que $S\sigma = S$ per a tot $\sigma \in \mathrm{Gal}(L/K)$. En altres paraules, el subcòs K' de L fix pel subgrup

$$H' := \{\, \sigma \in G \mid S\sigma = S \,\}$$

està inclòs en K; per tant, si ${\psi_1}', \ldots, {\psi_r}'$ són les $\mathbb{Q}$-immersions de K' en $\mathbb{C}$ induïdes pel conjunt S, el següent resultat ens diu que $(K', \{{\psi_l}'\})$ és el *mínim CM-subcòs* de $(F, \{\varphi_i\})$.

Proposició 5.5.2. *K' és un cos CM, i $\overline{{\psi_i}'} \neq {\psi_j}'$ $\forall i, j \in \{1, \ldots, r\}$.*

Si recuperem ara les observacions 5.1.8 i 5.3.2, podem donar la següent *triple* caracterització dels anomenats *CM-tipus primitius.*

Corol·lari 5.5.3. *Amb les notacions anteriors, són equivalents:*

1. *Les varietats abelianes de tipus $(F, \{\varphi_i\})$ són simples.*
2. *El CM-tipus $(F, \{\varphi_i\})$ no té cap CM-subcòs propi.*
3. $\mathrm{Gal}(L/F) = H'$.

Considerem, per exemple, el *CM-tipus ciclotòmic clàssic.* Donat un primer senar p, la p-èsima extensió ciclotòmica $\mathbb{Q}(\zeta_p)$ és una extensió abeliana de $\mathbb{Q}$ amb grup de Galois G_p isomorf a $(\mathbb{Z}/p\mathbb{Z})^*$: per a cada $j \in \{1, \ldots, p-1\}$, sigui φ_j l'element de G_p definit per $\varphi_j(\zeta_p) = {\zeta_p}^j$. Donat que $\mathbb{Q}(\zeta_p)$ és un cos CM, és clar que el parell $(\mathbb{Q}(\zeta_p), \{\varphi_1, \ldots, \varphi_t\})$, on $t = (p-1)/2$, és un

CM-tipus. A més, és primitiu. En efecte, només cal aplicar el corol·lari amb $L = \mathbb{Q}(\zeta_p)$: en aquest cas, $S = \{\varphi_1, \ldots, \varphi_t\}$, i si $S\,\varphi_k = S$, és a dir, si

$$\{k, \ldots, t\,k\} \;\equiv\; \{1, \ldots, t\} \pmod{p},$$

aleshores φ_k és l'automorfisme identitat, perquè

$$k\,\frac{p^2-1}{8} \;=\; k + \cdots + t\,k \;\equiv\; 1 + \cdots + t \;=\; \frac{p^2-1}{8} \pmod{p},$$

d'on $k \equiv 1 \pmod{p}$.

Amb les mateixes notacions d'abans, posem ara $\widetilde{S} := \{\sigma^{-1} | \sigma \in S\}$. Considerem el subgrup

$$\widetilde{H} \;:=\; \left\{ \sigma \in G \;\middle|\; \widetilde{S}\sigma = \widetilde{S} \right\},$$

i siguin $\widetilde{K}$ el subcòs de L fix per $\widetilde{H}$ i $\{\chi_k\}$ les $\mathbb{Q}$-immersions de $\widetilde{K}$ en $\mathbb{C}$ induïdes pels elements de $\widetilde{S}$.

Proposició 5.5.4. $(\widetilde{K}, \{\chi_k\})$ *és un CM-tipus primitiu, anomenat* reflex *del CM-tipus* $(F, \{\varphi_i\})$.

Observació 5.5.5. Es pot demostrar que $\widetilde{K} = \mathbb{Q}(\mathrm{tr}_\varphi(F))$, on $\mathrm{tr}_\varphi(\alpha) = \sum_{i=1}^{n} \alpha^{\varphi_i}$ per a tot $\alpha \in F$. Les immersions χ_k tampoc no depenen de la clausura L.

Observació 5.5.6. Per la mateixa definició, és clar que el reflex del CM-subcòs $(K, \{\psi_j\})$ també és $(\widetilde{K}, \{\chi_k\})$. A més, el reflex de $(\widetilde{K}, \{\chi_k\})$ és precisament el mínim CM-subcòs $(K', \{\psi_l{}'\})$, que coincideix amb el CM-tipus $(F, \{\varphi_i\})$ si aquest és primitiu.

En el cas particular que l'extensió $F/\mathbb{Q}$ sigui de Galois, podem prendre $L = F$, i llavors $S = \{\varphi_1, \ldots, \varphi_n\}$ i

$$G \;=\; \mathrm{Gal}(F/\mathbb{Q}) \;=\; S \sqcup \{\overline{\varphi_1}, \ldots, \overline{\varphi_n}\}.$$

Si l'extensió és abeliana, aleshores $H' = \widetilde{H}$, i els cossos del CM-tipus reflex i del mínim CM-subcòs coincideixen. Si, a més, el CM-tipus $(F, \{\varphi_i\})$ és primitiu, aleshores el seu reflex és $(F, \{\varphi_i{}^{-1}\})$. Així, per exemple, el reflex del CM-tipus ciclotòmic clàssic $(\mathbb{Q}(\zeta_p), \{\varphi_i\})$ és $(\mathbb{Q}(\zeta_p), \{\overline{\varphi_i}\})$, mentre que els CM-tipus associats a les corbes el·líptiques amb CM són *autoreflexos*.

Bibliografia

[La 83] S. Lang. *Complex multiplication.* Grundlehren der mathematischen Wissenschaften, 255. Springer-Verlag, 1983.

[Sh 98] G. Shimura. *Abelian varieties with complex multiplication and modular forms.* Princeton University Press, 1998.

[Si 94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, 1994.

Capítol 6

Series L de variedades abelianas con CM

L. Dieulefait [1]
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

6.1 Reducción de variedades algebraicas

Sea V_k variedad afín definida sobre un cuerpo k. Sea su anillo de funciones $R_k = k[x_1, ..., x_n]$. Sea $\mathfrak{O}$ anillo de valoración discreta de k con ideal maximal $\mathfrak{P}$. Vemos $R = \mathfrak{O}[x_1, ..., x_n]$ como anillo afín sobre $\mathfrak{O}$. $V = \text{Spec } R$. Todo homomorfismo $R \to R'$ será un punto de V sobre R'. Definimos V módulo $\mathfrak{P}$, que denotamos $V(\mathfrak{P})$ como Spec $(R/\mathfrak{P}R)$.
Sea $k(\mathfrak{P}) = \mathfrak{O}/\mathfrak{P}$ cuerpo residual, también denotado $\tilde{k}$, y $\tilde{R} = R/\mathfrak{P}R$. Tenemos que $\tilde{R} = \tilde{k}[\tilde{x}_1, ..., \tilde{x}_n]$.
Si $\mathfrak{P}R$ es primo en R, R se ve como anillo afín de la variedad afín V sobre k (o $V(\mathfrak{P})$ sobre $k(\mathfrak{P})$).
Un punto de $V(\mathfrak{P})$ es un homomorfismo.

$$R(\mathfrak{P}) \to K(\mathfrak{P})$$

[1] con el apoyo de TMR - Marie Curie beca ERB4001GT974451

donde $K(\mathfrak{P})$ es algún cuerpo que contiene a $k(\mathfrak{P})$.
Componiendo con la aplicación canónica:

$$R \to R(\mathfrak{P}) \to K(\mathfrak{P})$$

obtenemos un punto de V.
Para variedades proyectivas, se define reducción mediante cubrimientos por cartas afines y verificando las compatibilidades pertinentes.
El grafo de la ley de grupo de una variedad abeliana es una variedad. Sea A variedad abeliana definida sobre $\mathfrak{O}$, es decir que tanto las ecuaciones que definen A como las que expresan la ley de grupo tienen coeficientes en $\mathfrak{O}$, diremos que A tiene buena reducción en $\mathfrak{P}$ si $A(\mathfrak{P})$ es variedad no singular y si la reducción de la ley de grupo módulo $\mathfrak{P}$ es el grafo de una ley de grupo en $A(\mathfrak{P})$. En tal caso $A(\mathfrak{P})$ es una variedad abeliana. Si un primo no es de buena reducción se dirá de mala reducción.
Si extendemos la valoración discreta $(\mathfrak{O}, \mathfrak{P})$ a un anillo de valoración con ideal maximal $(\mathfrak{D}, \mathfrak{B})$ de k^{alg} (que induce anillos de valoración discreta en las subextensiones finitas), los puntos de orden m de A, conjunto que denotamos $A[n]$, son racionales sobre $\mathfrak{D}$, luego podemos reducirlos módulo $\mathfrak{B}$ y obtenemos un homomorfismo:

$$A[m] \to A[m](\mathfrak{B}) \subseteq A(\mathfrak{P}).$$

Más aún, si m y $\mathfrak{P}$ son coprimos tenemos un isomorfismo:

$$A[m] \to A[m](\mathfrak{B}) = A(\mathfrak{B})[m]$$

entre $A[m]$ y los puntos de orden m en la reducción $A(\mathfrak{B})$. La demostración de este hecho es inmediata si se asume compatibilidad de las operaciones algebraicas de A con la reducción módulo $\mathfrak{B}$. Resumamos este resultado y otros en el siguiente teorema:

Teorema 6.1.1. *Sea A variedad abeliana sobre un cuerpo de números k. Para casi todo (todos salvo un número finito) ideal primo $\mathfrak{P}$ de k, $A(\mathfrak{P}) = \tilde{A}$ es variedad abeliana y $a \to \tilde{a}$ es un homomorfismo de A en $\tilde{A}$. Este homomorfismo induce isomorfismo entre los grupos de puntos de orden finito coprimo con la característica de $\tilde{k}$ de A y $\tilde{A}$.*
Sean A, B variedades abelianas sobre k, entonces, para casi todo $\mathfrak{P}$ ideal primo de k se tiene lo siguiente:
Para todo $\lambda \in \mathrm{Hom}(A, B)$, $\tilde{\lambda}$ es homomorfismo de $\tilde{A}$ en $\tilde{B}$ y la reducción $\lambda \to \tilde{\lambda}$ es un homomorfismo inyectivo:

$$\mathrm{Hom}(A, B) \to \mathrm{Hom}(A(\mathfrak{P}), B(\mathfrak{P})).$$

En particular, si $A = B$ tenemos un homomorfismo inyectivo de $\mathrm{End}(A)$ *en* $\mathrm{End}(A(\mathfrak{P}))$.

La reducción de A módulo $\mathfrak{P}$ está definida sobre el cuerpo finito $k(\mathfrak{P})$, lo cual permite definir los siguientes homomorfismos:

Definición 6.1.2. *Sea A variedad abeliana sobre un cuerpo k de característica $p > 0$. Sea $q = p^f$ una potencia de p ($f > 0$). El morfismo $z \to z^q$ aplicado a los puntos de A nos da un homomorfismo de A en A^q que denotaremos π y llamaremos homomorfismo "elevar a la q". Notemos que A^q es variedad abeliana pues en general, para cada isomorfismo σ del cuerpo de definición k en un cuerpo k^σ, A^σ nos da una variedad abeliana sobre k^σ, donde el origen de A^σ será la imagen O^σ del origen O de A.*
Si el cuerpo de definición es el cuerpo de q elementos, entonces $A^q = A$ y por lo tanto π es un endomorfismo de A, que llamaremos el endomorfismo de Frobenius o "elevar a la q" de A.

6.2 Descomposición del Frobenius

Sea (A, ι) variedad abeliana con multiplicación compleja de tipo $(F, \{\varphi_i\})$ definida sobre k, principal. Sea $(K^*, \{\psi_\alpha\})$ el reflejo de $(F, \{\varphi_i\})$. Sabemos que $k \supseteq K^*$, y por lo tanto podemos extender los morfismos ψ_α a k, extensión que denotaremos de igual forma por abuso de notación.

Teorema 6.2.1. *Sea $\pi_{\mathfrak{P}}$ el homomorfismo "elevar a la $N(\mathfrak{P})$" de $\tilde{A}$ en $\tilde{A}^{N(\mathfrak{P})}$, y sea π el endomorfismo de $\tilde{A}$ "elevar a la $N(\mathfrak{B})$", donde:*
$\mathfrak{P}$ es un primo de K^* que divide al primo racional p, $\mathfrak{B}$ es un primo de k que divide a $\mathfrak{P}$ y $\tilde{A}$ denota la reducción de A módulo $\mathfrak{B}$. Suponemos que estamos en un caso de buena reducción y además que p no ramifica en F. Bajo estas condiciones se tiene que:
(1) $\prod_\alpha \mathfrak{P}^{\psi_\alpha}$ es un ideal de F y $(\tilde{A}^{N(\mathfrak{P})}, \tilde{\iota}^{N(\mathfrak{P})}, \pi_{\mathfrak{P}})$ es una $\prod_\alpha \mathfrak{P}^{\psi_\alpha}$-transformada de $(\tilde{A}, \tilde{\iota})$.
(2) Existe π_0 en F tal que $\tilde{\iota}(\pi_0) = \pi$ y se tiene:

$$(\pi_0) = \prod_\alpha N_{k/K^*}(\mathfrak{B})^{\psi_\alpha}.$$

Demostración: Sea $\dim A = n$, $\quad \mathfrak{O} = \mathfrak{O}_F$.
Existen n formas diferenciales invariantes ω_i en A tal que:

$$\delta_\iota(\mu)\omega_i = \mu_{\varphi_i}\omega_i \qquad i = 1, ..., n$$

para todo $\mu \in \mathfrak{O}$. Podemos asumirlas definidas en una extensión algebraica finita de k. Sea k_1 extensión de Galois de $\mathbb{Q}$ que contenga a k y a F en la que las formas diferenciales ω_i estén definidas. Sea $\mathfrak{B}_1 \mid \mathfrak{B}$ un primo de k_1. Denotemos con $\tilde{}$ la reducción módulo $\mathfrak{B}_1$. Podemos asumir que las ω_i son $\mathfrak{B}_1$-finitas y $\tilde{\omega}_i \neq 0$ para todo i.
Veamos que las $\tilde{\omega}_i$ son linealmente independientes sobre el cuerpo residual $\tilde{k}_1$. Sea $\{\beta_1, \ldots, \beta_{2n}\}$ base de $\mathfrak{O}$ sobre $\mathbb{Z}$. Llamando θ_i al conjugado complejo de φ_i, el determinante de la matriz:

$$M = \begin{pmatrix} \beta_1^{\varphi_1} & \ldots & \beta_1^{\varphi_n} & \beta_1^{\theta_1} & \ldots & \beta_1^{\theta_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{2n}^{\varphi_1} & \ldots & \beta_{2n}^{\varphi_n} & \beta_{2n}^{\theta_1} & \ldots & \beta_{2n}^{\theta_n} \end{pmatrix}$$

no es divisible por $\mathfrak{B}_1$, pues p no ramifica en F.
Por lo tanto, la matriz formada por las primeras n columnas de M tiene rango n módulo $\mathfrak{B}_1$, con lo que ciertas n filas son linealmente independientes módulo $\mathfrak{B}_1$. Luego, existen n elementos en $\mathfrak{O}$, que denotamos $\mu_1, ..., \mu_n$, tales que:

$$\det\,(\mu_j^{\varphi_i}) \not\equiv 0 \pmod{\mathfrak{B}_1}. \tag{2.1}$$

Supongamos que $\sum_{i=1}^n \xi_i \tilde{\omega}_i = 0$ para ciertos elementos ξ_i de $\tilde{k}_1$. Multiplicando por $\delta_\iota(\tilde{\mu}_j)$ obtenemos, para cada j:

$$\sum_i \delta_\iota(\tilde{\mu}_j)\xi_i\tilde{\omega}_i = \sum_i \xi_i \tilde{\mu}_j^{\varphi_i}\tilde{\omega}_i = 0.$$

Aplicando (2.1) deducimos que $\xi_i\tilde{\omega}_i = 0$ para todo i, de donde: $\xi_i = 0$ para todo i, y por lo tanto las formas diferenciales $\tilde{\omega}_i$ son linealmente independientes sobre $\tilde{k}_1$, y base de las diferenciales invariantes de $\tilde{A}$.
$(\tilde{A}, \tilde{\iota})$ es una variedad abeliana de tipo $(F, \{\varphi_i\})$ sobre el cuerpo de $N(\mathfrak{B})$ elementos. Existe un elemento π_0 de $\mathfrak{O}$ tal que: $\tilde{\iota}(\pi_0) = \pi$. Además $N(\pi_0) = \text{grado}(\pi) = N(\mathfrak{B})^n$. Sea:

$$(\pi_0) = \mathfrak{P}_1^{e_1}.....\mathfrak{P}_s^{e_s}$$

la descomposición del ideal principal (π_0) en ideales primos de F. Para cada i, sea σ_i automorfismo de k_1 que extiende a φ_i^{-1}. Para cada t, sea d_t el cardinal del conjunto: $\{i : \mathfrak{B}_1^{\sigma_i} \mid \mathfrak{P}_t\}$. Sea h el número de clases de ideales de F. Luego, $\mathfrak{P}_t^{he_t} = \gamma_t\mathfrak{O}$ para algún $\gamma_t \in \mathfrak{O}$. Es fácil ver que d_t es el número de i tales que $\gamma_t^{\varphi_i} \in \mathfrak{B}_1$. Reduciendo módulo $\mathfrak{B}_1$:

$$\delta_{\tilde{\iota}}(\gamma_t)\tilde{\omega}_i = \tilde{\gamma}_t^{\varphi_i}\tilde{\omega}_i \qquad i = 1, ..., n.$$

Como las $\tilde{\omega}_i$ son base del espacio $\mathfrak{D}_0(\tilde{A})$ de formas diferenciales invariantes de $\tilde{A}$, vemos que la aplicación lineal $\delta_{\tilde{\iota}}(\gamma_t)$ de $\mathfrak{D}_0(\tilde{A})$ en sí mismo tiene rango $n - d_t$.
Si $\tilde{x}$ es un punto genérico de $\tilde{A}$ sobre $\tilde{k}$ tenemos:

$$\tilde{k}(\tilde{\iota}(\gamma_t)\tilde{x}) \supseteq \tilde{k}(\pi^h\tilde{x}) = \tilde{k}(\tilde{x}^{N(\mathfrak{B})^h})$$

pues $\pi_0^h \in \mathfrak{P}_t^{e_t h} = (\gamma_t)$.
Luego:

$$N(\mathfrak{P}_t^{he_t}) = N(\gamma_t) = grado(\tilde{\iota}(\gamma_t)) \leq N(\mathfrak{B})^{h(n-rango(\delta_{\tilde{\iota}}(\gamma_t)))} = N(\mathfrak{B})^{hd_t}$$

Se sigue que:

$$N(\mathfrak{P}_t)^{e_t} \leq N(\mathfrak{B})^{d_t}. \qquad (2.2)$$

Poniendo $N_{k_1/k}(\mathfrak{B}_1) = \mathfrak{B}^r$ obtenemos:

$$N(\mathfrak{P}_t)^{e_t r} \leq N(\mathfrak{B})^{d_t r} = \prod{}' N(\mathfrak{B}_1^{\sigma_i}) \qquad (2.3)$$

donde el producto es sólo sobre aquellos i tales que $\mathfrak{B}_1^{\sigma_i} \mid \mathfrak{P}_t$. Cada $\mathfrak{B}_1^{\sigma_i}$ divide a lo sumo a un $\mathfrak{P}_t$, luego de (2.3) y la descomposición de (π_0) se tiene que:

$$N(\pi_0)^r \leq \prod_{i=1}^{n} N(\mathfrak{B}_1^{\sigma_i}). \qquad (2.4).$$

Esta desigualdad es en realidad igualdad, pues ambos lados valen $N(\mathfrak{B})^{nr}$, por lo tanto (2.2) y (2.3) son igualdades. Vemos en particular que de las igualdades (2.3) y (2.4) se sigue que cada $\mathfrak{B}_1^{\sigma_i}$ divide exactamente a un $\mathfrak{P}_t$ (y no a ninguno).
Pongamos $N_{k_1/F}(\mathfrak{B}_1^{\sigma_i}) = \mathfrak{P}_t^{u_t}$ donde $\mathfrak{B}_1^{\sigma_i}$ divide a $\mathfrak{P}_t$. Como k_1/F es una extensión de Galois, u_t no depende de i, y por lo tanto, partiendo de $N(\mathfrak{B}_1^{\sigma_i}) = N(\mathfrak{P}_t)^{u_t}$ y aplicando la igualdad (2.3) obtenemos :

$$N(\mathfrak{P}_t)^{re_t} = N(\mathfrak{P}_t)^{u_t d_t}.$$

De donde: $re_t = u_t d_t$. Entonces:

$$\mathfrak{P}_t^{e_t r} = (\mathfrak{P}_t^{u_t})^{d_t} = \prod{}' N_{k_1/F}(\mathfrak{B}_1^{\sigma_i})$$

donde el producto es sobre aquellos i tales que $\mathfrak{B}_1^{\sigma_i} \mid \mathfrak{P}_t$. De aquí se obtiene la descomposición:

$$(\pi_0)^r = \mathfrak{P}_1^{re_1} \ldots \mathfrak{P}_s^{re_s} = N_{k_1/F}(\prod_{i=1}^{n} \mathfrak{B}_1^{\sigma_i}) \qquad (2.5).$$

Sea σ automorfismo de Frobenius de $\mathfrak{B}_1$ sobre K^*, es decir, un automorfismo de k_1/K^* tal que $\mathfrak{B}_1^\sigma = \mathfrak{B}_1$ y $z^\sigma \equiv z^{N(\mathfrak{P})} \pmod{\mathfrak{B}_1}$ para todo z entero de k_1.
Sea $N(\mathfrak{P}) = q$. Como $\mathfrak{B}_1^\sigma = \mathfrak{B}_1$, A^σ tiene buena reducción en $\mathfrak{B}_1$ y $(\tilde{A^\sigma}, \tilde{\iota^\sigma}) \cong (\tilde{A}^q, \tilde{\iota}^q)$. Sabemos que (A^σ, ι^σ) es una C-transformada de (A, ι) para alguna C clase de ideales de F, y lo mismo $(\tilde{A}^q, \tilde{\iota}^q)$ lo es de $(\tilde{A}, \tilde{\iota})$.
$\pi_{\mathfrak{P}}$ es un homomorfismo de $(\tilde{A}, \tilde{\iota})$ en $(\tilde{A}^q, \tilde{\iota}^q)$, luego es una $\mathfrak{W}$-multiplicación para algún ideal $\mathfrak{W}$ de $\mathfrak{O}$. Sea $N_{k/K^*}(\mathfrak{B}) = \mathfrak{P}^v$, luego $N(\mathfrak{B}) = q^v$.
Consideremos el homomorfismo π_a "elevar a la q" , de $\tilde{A}^{q^{a-1}}$ en $\tilde{A}^{q^a}$ para cada a entero positivo. Como $(\tilde{A}^{q^{a-1}}, \tilde{A}^{q^a}, \pi_a)$ es imagen isomorfa de $(\tilde{A}, \tilde{A}^q, \pi_{\mathfrak{P}})$ vemos que $(\tilde{A}^{q^a}, \tilde{\iota}^{q^a}, \pi_a)$ es una $\mathfrak{W}$-transformada de $(\tilde{A}^{q^{a-1}}, \tilde{\iota}^{q^{a-1}})$. Luego $\pi_v \ldots \pi_2 \pi_1$ es una $\mathfrak{W}^v$-multiplicación de $\tilde{A}$ en $\tilde{A}^{N(\mathfrak{B})} = \tilde{A}$. Por otro lado $(\pi_v \ldots \pi_1)\tilde{x} = \tilde{x}^{q^v} = \tilde{x}^{N(\mathfrak{B})} = \pi\tilde{x}$, de donde $\pi = \pi_v \ldots \pi_1$. Como π es una (π_0)-multiplicación, tenemos que $(\pi_0) = \mathfrak{W}^v$. De (2.5) se sigue que:

$$\mathfrak{W}^{vr} = (\pi_0)^r = \prod_{i=1}^{n} N_{k_1/F}(\mathfrak{B}_1^{\sigma_i}). \qquad (2.6)$$

Sea $G = \mathrm{Gal}(k_1/\mathbb{Q})$, $S^* = \{g \in G : g = \psi_\alpha \text{ en } K^*, \text{ para algún } \alpha\}$.
Sea H (resp. H^*) subgrupo de G correspondiente a F (resp. K^*). Por definición de reflejo: $S^* = \bigcup_i \sigma_i H = \bigcup_\alpha H^* \psi_\alpha$. Aplicando (2.6):

$$\mathfrak{W}^{vr} \sim \prod_{\tau \in S^*} \mathfrak{B}_1^\tau \sim \prod_\alpha \prod_{\gamma \in H^*} \mathfrak{B}_1^{\gamma\psi_\alpha} \sim \prod_\alpha N_{k_1/K^*}(\mathfrak{B}_1)^{\psi_\alpha} \sim \prod_\alpha (\mathfrak{P}^{rv})^{\psi_\alpha}$$

donde la relación $\sim$ significa que se tiene ideales de subcuerpos de k_1 que coinciden al extenderlos a k_1. Concluimos entonces que: $\mathfrak{W} = \prod_\alpha \mathfrak{P}^{\psi_\alpha}$ y esto prueba (1) del teorema.
Como $(\pi_0) = \mathfrak{W}^v$ y $\mathfrak{P}^v = N_{k/K^*}(\mathfrak{B})$ queda probado también (2).

6.3 Series L de variedades abelianas con CM

6.3.1 Grössencharacteres

Sea k cuerpo de números, $\mathfrak{M}$ ideal entero de k. Denotemos por $I_k(\mathfrak{M})$ al conjunto de los ideales de k coprimos con $\mathfrak{M}$, enteros o no. Diremos que un

homomorfismo:

$$\chi : I_k(\mathfrak{M}) \to \{x \in \mathbb{C} : |x| = 1\}$$

es un Grössencharacter si existen enteros f_σ y números reales ξ_σ, con σ recorriendo las inmersiones $k \cong \mathbb{C}$ no conjugadas complejas entre sí, tales que para todo $\mathfrak{A} = (\alpha)$ ideal principal con $\alpha \equiv 1 \pmod{\mathfrak{M}}$:

$$\chi(\mathfrak{A}) = \prod_\sigma (\alpha^\sigma/|\alpha^\sigma|)^{f_\sigma} \prod_\sigma |\alpha^\sigma|^{i\xi_\sigma}.$$

Diremos que $\mathfrak{M}$ es un ideal de definición de χ.
Dos Grössencharacteres χ_1 y χ_2 se dicen equivalentes si coinciden allí donde están definidos. Dado un Grössencharacter χ, llamaremos conductor al ideal de definición minimal de entre los de todos los Grössencharacteres equivalentes a χ. Por último, se dice que χ es primitivo cuando su ideal de definición coincide con su conductor.
La función L de variable compleja asociada a un Grössencharacter χ viene dada por:

$$L(s,\chi) = \sum{}' \chi(\mathfrak{A}) N(\mathfrak{A})^{-s} = \prod{}' (1 - \chi(\mathfrak{P}) N(\mathfrak{P})^{-s})^{-1}$$

donde la suma es sobre los ideales enteros en $I_k(\mathfrak{M})$, y el producto sobre los ideales primos en $I_k(\mathfrak{M})$.
L es holomorfa en todo $\mathbb{C}$ si $\chi \neq 1$.
Sea $\bar{\chi}(\mathfrak{A}) = \chi(\bar{\mathfrak{A}})$. Si se define la función $\xi(s,\chi)$ como el producto de $L(s,\chi)$ por un adecuado factor Γ, se tiene la ecuación funcional:

$$\xi(s,\chi) = W(\chi)\xi(1-s,\bar{\chi})$$

para una constante $W(\chi)$.

6.3.2 Funciones Z de variedades abelianas

Sea κ cuerpo de q elementos, V variedad algebraica completa no singular sobre κ. Para cada entero positivo m, sea N_m la cantidad de puntos de V sobre una extensión de κ de grado m. Asociamos a V/κ la función de variable compleja $Z(u, V/\kappa)$ definida por la fórmula:

$$\frac{d}{du} \log(Z(u, V/\kappa)) = \sum_{m=1}^{\infty} N_m u^{m-1}.$$

Si V es variedad abeliana, se tiene el siguiente resultado que relaciona la función Z con el endomorfismo de Frobenius "elevar a la q".

Proposición 6.3.1. *Sea A variedad abeliana de dimensión n, definida sobre un cuerpo κ de q elementos. Sean $\pi_1, ..., \pi_{2n}$ raíces características del endomorfismo "elevar a la q" de A.*
Sean: $P_0(u) = 1 - u$, $P_t(u) = \prod_{(i)}(1 - \pi_{i_1}....\pi_{i_t}u)$ para cada $0 < t \leq 2n$, donde los productos son sobre todos los subconjuntos de t raíces características del Frobenius.
Entonces:

$$Z(u, A/\kappa) = \frac{P_1(u)P_3(u)...P_{2n-1}(u)}{P_0(u)P_2(u)...P_{2n}(u)}.$$

Corolario 6.3.2. *Si las variedades abelianas A, A' son isógenas (ambas variedades y la isogenia definidas sobre κ), entonces:*

$$Z(u, A/\kappa) = Z(u, A'/\kappa).$$

Observación: Las "Conjeturas de Weil" afirman que para toda variedad algebraica V , la función $Z(u, V/\kappa)$ es una función racional, satisface una ecuación funcional, y tiene ceros de valor absoluto $q^{h/2}$ con h impar menos que $2n$ y polos de valor absoluto $q^{h'}$ con $h' = 1, 2, ..., n$. La proposición anterior junto con el resultado de Weil que dice que $|\pi_i| = q^{1/2}$ prueba ésta conjetura para variedades abelianas. La conjetura ha sido probada en el caso general por Deligne.

Función Z de una variedad sobre un cuerpo de números:
Sea k un cuerpo de números y V una variedad completa no singular definida sobre k. Para cada ideal primo $\mathfrak{P}$ de k denotemos $V(\mathfrak{P})$ a la reducción de V módulo $\mathfrak{P}$. Para casi todo $\mathfrak{P}$ (es decir,todos los ideales primos salvo un número finito) $V(\mathfrak{P})$ será una variedad completa no singular sobre el cuerpo residual $k(\mathfrak{P})$. Si esto ocurre, decimos que $\mathfrak{P}$ es un primo de buena reducción de V y definimos:

$$\zeta(s, V, \mathfrak{P}) = Z(N(\mathfrak{P})^{-s}, V(\mathfrak{P})/k(\mathfrak{P})).$$

Con estas funciones construimos la función Zeta de V/k:

$$\zeta(s, V/k) = \prod{}' \zeta(s, V, \mathfrak{P})$$

donde el producto es sobre los primos de buena reducción de V. Este producto converge si $Re\ s > 3/2$.

Conjetura 6.3.3. *Para cualquier V y k como en la discusión anterior, $\zeta(s, V/k)$ es meromorfa en todo el plano complejo y verifica una ecuación funcional.*

Probaremos a continuación un teorema de Taniyama que implica esta conjetura para el caso de variedades abelianas con multiplicación compleja.

Sea (A, ι) variedad abeliana de dimensión n con multiplicación compleja, definida sobre k, de tipo $(F, \{\varphi_i\})$, quizás no primitivo, con $[F : \mathbb{Q}] = 2n$. Sea $\tau = \iota^{-1}[\mathrm{End}(A) \cap \iota(F)]$. τ es un orden de F. Si no es $\mathfrak{O}$, el orden maximal de enteros algebraicos, sea $\mathfrak{E}$ su conductor. Podemos hallar una $\mathfrak{E}$-transformada (A_1, ι_1, λ) de (A, ι) definida sobre k tal que:

$$\iota_1(\mathfrak{O}) = \mathrm{End}(A_1) \cap \iota_1(F).$$

Si ambas variedades reducen bien en un primo $\mathfrak{P}$ las funciones $\zeta(s, A, \mathfrak{P})$ y $\zeta(s, A_1, \mathfrak{P})$ coinciden. Luego $\zeta(s, A/k)$ y $\zeta(s, A_1/k)$ sólo difieren en un número finito de factores. Por lo tanto en el estudio de la función ζ alcanza con trabajar con variedades abelianas para las cuales:

$$\iota^{-1}[\mathrm{End}(A) \cap \iota(F)] = \mathfrak{O}$$

por lo que en lo que sigue asumiremos que A lo cumple.
Sea $\mathbf{b}$ ideal entero de F, t un punto propiamente de $\mathbf{b}$-torsión de A. Sea k' extensión de Galois de k tal que t es racional sobre k'. Para todo $\sigma \in \mathrm{Gal}(k'/k)$, t^σ también es propiamente de $\mathbf{b}$-torsión, y por ende existe $\mu_\sigma \in \mathfrak{O}$ coprimo con $\mathbf{b}$ tal que: $\iota(\mu_\sigma)t = t^\sigma$, y está unívocamente determinado módulo $\mathbf{b}$ por σ.
Sea $\mu[\sigma]$ la clase de μ_σ módulo $\mathbf{b}$. Tenemos que, si $\sigma, \tau \in \mathrm{Gal}(k'/k)$:

$$t^{\sigma\tau} = (\iota(\mu_\sigma)t)^\tau = \iota(\mu_\sigma)t^\tau = \iota(\mu_\sigma\mu_\tau)t.$$

Por lo que la aplicación $\sigma \to \mu[\sigma]$ es un homomorfismo de $\mathrm{Gal}(k'/k)$ en $(\mathfrak{O}/\mathbf{b})^*$. Es claro que los elementos del grupo de Galois que están en el núcleo de este homomorfismo son precisamente aquellos que fijan $k(t)$, luego tenemos que $\sigma \to \mu[\sigma]$ es un isomorfismo entre los grupos $\mathrm{Gal}(k(t)/k)$ y $(\mathfrak{O}/\mathbf{b})^*$.
En particular vemos que $k(t)$ es extensión abeliana de k.
Sea $\mathfrak{M} = \prod' \mathfrak{P}$, donde el producto es sobre los primos de mala reducción de A. Sea b el menor entero racional positivo múltiplo de $\mathbf{b}$. Tomemos un ideal primo $\mathfrak{P}$ de k tal que $\mathfrak{P} \nmid b\mathfrak{M}$, y sea $\mathfrak{B}$ un primo en $k(t)$ que divide a $\mathfrak{P}$. Sea $N(\mathfrak{P}) = q$. Denotemos por $\tilde{}$ a la reducción módulo $\mathfrak{B}$. Sea $\sigma_{\mathfrak{P}}$ un morfismo de Frobenius de $\mathfrak{P}$ en $k(t)/k$. Como $\tilde{A}$ está definida sobre el cuerpo residual $k(\mathfrak{P})$, tenemos en $\tilde{A}$ el endomorfismo $\pi =$ "elevar a la q". Existe $\pi_{\mathfrak{P}} \in \mathfrak{O}$ tal que $\tilde{\iota}(\pi_{\mathfrak{P}}) = \pi$. Además $\iota(\pi_{\mathfrak{P}})t$ y $t^{\sigma_{\mathfrak{P}}}$ tienen igual

reducción módulo $\mathfrak{B}$. Como $\mathfrak{B}$ es coprimo con b, la reducción módulo $\mathfrak{B}$ nos da isomorfismo entre los grupos de puntos de $\mathbf{b}$-torsión de la variedad y su reducción:

$$A[\mathbf{b}] \cong \tilde{A}[\mathbf{b}].$$

Por lo tanto:

$$\iota(\pi_{\mathfrak{P}})t = t^{\sigma_{\mathfrak{P}}}.$$

En particular vemos que $\sigma_{\mathfrak{P}}$ está unívocamente determinado por $\mathfrak{P}$, de donde:
Si $\mathfrak{P}$ coprimo con $b\mathfrak{M}$, entonces $\mathfrak{P}$ no ramifica en $k(t)$.
Además se tiene, por definición del morfismo $\mu[-]$, que $\mu[\sigma_{\mathfrak{P}}]$ es la clase de $\pi_{\mathfrak{P}}$ módulo $\mathbf{b}$.
Sea d el discriminante de F sobre $\mathbb{Q}$. Si $\mathfrak{A} \in I_k(bd\mathfrak{M})$, $\mathfrak{A} = \prod \mathfrak{P}^{c(\mathfrak{P})}$ defino:

$$\sigma_{\mathfrak{A}} = \prod \sigma_{\mathfrak{P}}^{c(\mathfrak{P})}, \qquad \pi_{\mathfrak{A}} = \prod \pi_{\mathfrak{P}}^{c(\mathfrak{P})}.$$

La correspondencia $\sigma_{\mathfrak{A}} \to \pi_{\mathfrak{A}}$ es un isomorfismo entre $\mathrm{Gal}(k(t)/k)$ y $(\mathfrak{O}/\mathbf{b})^*$ por lo tanto $\sigma_{\mathfrak{A}}$ es la identidad si y sólo si $\pi_{\mathfrak{A}} \equiv 1 \pmod{\mathbf{b}}$.
Sea $(K^*, \{\psi_\alpha\})$ el reflejo de $(F, \{\varphi_i\})$. Sabemos que, para ideales primos $\mathfrak{P}$ de k:

$$(\pi_{\mathfrak{P}}) = \prod_\alpha N_{k/K^*}(\mathfrak{P})^{\psi_\alpha}$$

y luego:

$$(\pi_{\mathfrak{A}}) = \prod_\alpha N_{k/K^*}(\mathfrak{A})^{\psi_\alpha}.$$

Para $\xi \in k$, definimos:

$$\xi^* = \prod_\alpha N_{k/K^*}(\xi)^{\psi_\alpha}.$$

Sabemos que $\xi^* \in F$ y que para toda inmersión compleja τ de F en $\mathbb{C}$

$$\xi^{*\tau}\overline{\xi^{*\tau}} = N_{k/\mathbb{Q}}(\xi),$$

por lo tanto: $|\xi^{*\tau}| = \sqrt{N_{k/\mathbb{Q}}(\xi)}$.
Sean $\pi_{\mathfrak{P}}^{(1)}, ..., \pi_{\mathfrak{P}}^{(2n)}$ las raíces características de $\tilde{\iota}(\pi_{\mathfrak{P}})$. Por los resultados de Weil, sabemos que para todo i:

$$|\pi_{\mathfrak{P}}^{(i)}| = \sqrt{N(\mathfrak{P})}.$$

Además estas mismas $\pi_{\mathfrak{P}}^{(i)}$ son las raíces características de $\iota(\pi_{\mathfrak{P}})$. Por lo tanto para toda inmersión compleja τ de F en $\mathbb{C}$, $\pi_{\mathfrak{P}}^{\tau}$ es una de las $\pi_{\mathfrak{P}}^{(i)}$, de donde:

$$|\pi_{\mathfrak{P}}^{\tau}| = \sqrt{N(\mathfrak{P})}$$

y por lo tanto, para todo $\mathfrak{A} \in I_k(bd\mathfrak{M})$:

$$|\pi_{\mathfrak{A}}^{\tau}| = \sqrt{N(\mathfrak{A})}.$$

Concluimos que para todo ideal principal $\mathfrak{A} = (\xi) \in I_k(bd\mathfrak{M})$ y todo isomorfismo $\tau : F \to \mathbb{C} : |(\pi_{\mathfrak{A}}/\xi^*)^{\tau}| = 1$. Como $(\pi_{\mathfrak{A}}) = (\xi^*)$, $\pi_{\mathfrak{A}}/\xi^*$ es un entero algebraico, y por lo tanto es una raíz de la unidad.
Es decir que para todo ideal principal $\mathfrak{A} = (\xi) \in I_k(bd\mathfrak{M})$, existe $\epsilon \in F$ raíz de la unidad tal que:

$$\pi_{\mathfrak{A}} = \epsilon \prod_{\alpha} N_{k/K^*}(\xi)^{\psi_\alpha}.$$

Aplicando teoría de cuerpos de clases, la extensión abeliana $k(t)$ de k es el cuerpo de clase sobre k correspondiente a un grupo de clases de ideales H de k . Sea $\mathfrak{F}$ el conductor de H, y f el menor entero racional positivo contenido en $\mathfrak{F} \cap \mathbf{b} \cap (d)$.
Si $\xi \in k$ cumple $\xi \equiv 1 \pmod{f\mathfrak{M}}$, entonces $\mathfrak{A} = (\xi)$ está contenido en H y luego $\sigma_{\mathfrak{A}}$ es la identidad, de donde $\pi_{\mathfrak{A}} \equiv 1 \pmod{\mathbf{b}}$.
Por otro lado, de $\xi \equiv 1 \pmod{f}$ se sigue que $\xi^* \equiv 1 \pmod{f}$. Luego:

$$\epsilon = \pi_{\mathfrak{A}}/\xi^* \equiv 1 \pmod{\mathbf{b}} \qquad (3.1)$$

si $\mathfrak{A} = (\xi)$, $\xi \equiv 1 \pmod{f\mathfrak{M}}$.
Impongamos la siguiente restricción sobre el ideal $\mathbf{b}$: debe ser tal que para todo $\epsilon \in F$ raíz de la unidad diferente de 1, $\mathbf{b}$ no divida a $\epsilon - 1$. Con esta condición sobre $\mathbf{b}$ se sigue que: $\pi_{\mathfrak{A}}/\xi^* = 1$, o sea:

$$\pi_{\mathfrak{A}} = \prod_{\alpha} N_{k/K^*}(\xi)^{\psi_\alpha}$$

si $\mathfrak{A} = (\xi)$, $\xi \equiv 1 \pmod{f\mathfrak{M}}$.
Definamos el siguiente carácter de $I_k(f\mathfrak{M})$: para todo $\mathfrak{A} \in I_k(f\mathfrak{M})$, sea

$$\chi(\mathfrak{A}) = \pi_{\mathfrak{A}}/|\pi_{\mathfrak{A}}| = \pi_{\mathfrak{A}}/\sqrt{N(\mathfrak{A})}$$

de lo anterior se sigue que χ es un Grössencharacter de k módulo $f\mathfrak{M}$.
Sean $\tau_1, ..., \tau_{2n}$ los isomorfismos de F en $\mathbb{C}$. Para $\mathfrak{A} \in I_k(f\mathfrak{M})$ sean: $\chi_i(\mathfrak{A}) = \pi_{\mathfrak{A}}^{\tau_i}/\sqrt{N(\mathfrak{A})}$ y $\chi_{i_1 \ldots i_t}(\mathfrak{A}) = \chi_{i_1}(\mathfrak{A}) \ldots \chi_{i_t}(\mathfrak{A})$. Hemos visto que todos estos son Grössencharacteres módulo $f\mathfrak{M}$ y aplicando el teorema 6.3.1 queda probado el siguiente resultado de Taniyama:

Teorema 6.3.4. *Sea $(F, \{\varphi_i\})$ un tipo de multiplicación compleja, $2n = [F : \mathbb{Q}]$. Sea (A, ι) variedad abeliana de dimensión n con éste tipo de multiplicación compleja y sea k el cuerpo de números en el que A y los elementos de $\iota(F) \cap \mathrm{End}(A)$ están definidos. Sea $\mathfrak{M}$ el producto de los primos de mala reducción de A sobre k.*
Entonces, existe f entero racional positivo y Grössencharacteres $\chi_{i_1 \ldots i_t}$ de k, todos con ideal de definición $f\mathfrak{M}$, tal que la función ζ de A sobre k verifica:

$$\zeta(s, A/k) = R(s) \prod_{t=0}^{2n} \prod_{(i)} L(s - t/2, \chi_{i_1 \ldots i_t})^{(-1)^t}$$

donde: $R(s)$ es producto de funciones racionales de $N(\mathfrak{P})^{-s}$ para un número finito de ideales primos $\mathfrak{P}$ de k , el segundo producto se hace sobre todas las combinaciones de t elementos de $1, 2, ..., 2n$ y $L(s, \chi_{(i)})$ es la función L asociada al caracter $\chi_{(i)}$.

6.4 Una condición necesaria para buena reducción

Sea A una variedad abeliana de dimensión n definida sobre un cuerpo de números k. Para cada primo ℓ, denotemos por $A[\ell^\infty]$ al conjunto de puntos de orden potencia de ℓ, y por $k^{(\ell)}$ a la extensión de k generada por las coordenadas de los puntos en $A[\ell^\infty]$. Es fácil ver que $k^{(\ell)}$ es extensión de Galois de k y cada elemento de $\mathrm{Gal}(k^{(\ell)}/k)$ induce un automorfismo en $A[\ell^\infty]$, luego si elegimos coordenadas ℓ-adicas en $A[\ell^\infty]$ tenemos una representación de $\mathrm{Gal}(k^{(\ell)}/k)$ dada por matrices del $GL_{2n}(\mathbb{Z}_\ell)$, que llamaremos $\mathcal{M}_\ell$. Esta representación es fiel.
Sea $\mathfrak{P}$ un primo en k y $\mathfrak{B} \in k^{(\ell)}$ un primo que divide a $\mathfrak{P}$. Sea σ automorfismo de Frobenius de $k^{(\ell)}$ para $\mathfrak{B}/\mathfrak{P}$. Supongamos que $\mathfrak{P}$ es un primo de buena reducción para A, y sea ℓ coprimo con $\mathfrak{P}$. Elijamos coordenadas ℓ-adicas de $A[\ell^\infty]$ y de $A(\mathfrak{P})[\ell^\infty]$ tal que todo $t \in A[\ell^\infty]$ y su reducción $t(\mathfrak{B})$ tengan iguales coordenadas. Sea $\pi_{\mathfrak{P}}$ el endomorfismo " elevar a la $N(\mathfrak{P})$ " de $A(\mathfrak{P})$. Para todo $t \in A[\ell^\infty]$ tenemos:

$$t^\sigma(\mathfrak{B}) = \pi_{\mathfrak{P}}(t(\mathfrak{B})).$$

De esta igualdad y de la definición de $\mathcal{M}_\ell$ se tiene:

$$\mathcal{M}_\ell(\sigma) = M_\ell(\pi_{\mathfrak{P}}).$$

Donde M_ℓ es la representación ℓ-adica de $\mathrm{End}(A(\mathfrak{P}))$. Por lo tanto σ está unívocamente determinado por $\mathfrak{P}$, de donde se sigue que $\mathfrak{P}$ no ramifica en

$k^{(\ell)}$. Sea $f_{\mathfrak{P},\ell}$ polinomio característico de $\mathcal{M}_\ell(\sigma)$, también lo es de $\pi_{\mathfrak{P}}$ y esto prueba el siguiente resultado:

Teorema 6.4.1. *Sea $\mathfrak{P}$ primo de buena reducción para A variedad abeliana definida sobre un cuerpo de números k. Entonces, para todo primo racional ℓ coprimo con $\mathfrak{P}$, $\mathfrak{P}$ no ramifica en $k^{(\ell)}$ y el polinomio característico $f_{\mathfrak{P},\ell}$ tiene coeficientes en $\mathbb{Z}$ y no depende de ℓ.*

Bibliografía

[L] S. Lang: "Complex Multiplication" , Grund. der math. Wiss., Springer Verlag, 1983

[S] P. Samuel: "Travaux de Shimura et Taniyama sur la multiplication complexe" , Séminaire Bourbaki, 3 (Exp. 129), Paris, 1956

[S-T] G. Shimura y Y. Taniyama: "Complex Multiplication of Abelian Varieties" , The Mathematical Society of Japan, 1961

[T] "Proceedings of the Int. Symp. on Alg. Number Theory" (Artículos de Weil, Shimura y Taniyama), Science Council of Japan, Tokyo & Nikko, 1956

Capítol 7

Polaritzacions de varietats abelianes amb CM

J. Guàrdia[1]
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

Introducció

En aquest capítol intentarem assolir un objectiu ben modest: perdre la por a les polaritzacions de les varietats abelianes. Les varietats abelianes amb multiplicació complexa són un bon camp de treball per assolir aquest objectiu.

Abans de començar, fem una observació que, tot i trivial, pot evitar-nos caure en un parany habitual. Quan treballem amb un tor complex de dimensió 1 fem moltes simplificacions subconscients: d'entrada, no parlem de tors complexos, sinó de corbes el·líptiques. I a més, de manera automàtica passem a un tor normalitzat $\mathbb{C}/\langle 1, \tau \rangle$. Per què totes aquestes simplificacions són correctes? D'entrada, per què tots els tors complexos de dimensió 1 són polaritzables, i en particular projectius, per la qual cosa té sentit pensar en la corba algebraica que els correspon. Però a més, un tor complex de dimensió

[1] Amb el suport parcial de la DGES: PB 96–0166.

1 només admet una única polarització principal (és a dir, essencialment només hi ha una manera de passar d'una xarxa del tipus $\langle \omega_1, \omega_2 \rangle$ a una xarxa $\langle 1, \tau \rangle$).

Aquestes presumpcions subconscients no podem fer-les quan treballem amb tors de dimensió superior. D'entrada, no és segur que qualsevol tor sigui polaritzable (projectiu). A més, hi ha tors que poden polaritzar-se de maneres diferents. Per això es diferent, per exemple, parlar d'isomorfismes de varietats abelianes que parlar d'isomorfismes de varietats abelianes polaritzades.

7.1 Recordatori: polaritzacions de tors complexos generals

Recordem alguns fets que ja han estat explicats en una exposició anterior ([Ro 00]), però que ens anirà bé tenir a mà. Per a un tor complex $A = \mathbb{C}^n/\Lambda$ els fets següents són equivalents:

a) A és projectiu.

b) A té un feix ample L.

c) Hi ha una forma hermítica definida positiva H que pren valors enters sobre la xarxa Λ.

d) Hi ha una forma de Riemann $E = \operatorname{Im} H : \Lambda \times \Lambda \to \mathbb{Z}$.

e) Hi ha una isogènia ϕ_L de A en el tor complex dual, la representació analítica de la qual és hermítica i definida positiva.

De fet, tenim bijeccions entre els conjunts següents:

$\mathcal{P}_1 = \{$Divisors amples$\}$/equivalència algebraica

$\mathcal{P}_2 = \{$Formes de Riemann $E = \operatorname{Im} H : \Lambda \times \Lambda \to \mathbb{Z}\}$

$\mathcal{P}_3 = \{$Isogènies $\phi : A \to A^*$ amb representació racional que indueix una forma de Riemann$\}$.

Quan parlem d'una polarització del tor complex A ens referim a un objecte d'un aquests tres conjunts, en el ben entès que l'interpretarem de

la manera que ens vagi millor en cada moment. Els tres conjunts admeten una estructura natural de grup, respecte de la qual són isomorfs. Són tres presentacions del grup de Néron-Severi del tor complex A.

A nivell pràctic encara convé fer una identificació més: cal que pensem totes les polaritzacions que són múltiples racionals positius d'una polarització donada com una sola polarització. Ben escrit, direm que dues polaritzacions E_1, E_2 són equivalents si tenim enters positius m, n tals que $mE_1 = nE_2$. En una classe de polaritzacions sempre podem trobar una polarització *bàsica*, que satisfà que totes les altres polaritzacions de la classe són múltiples enters d'ella.

7.2 Polaritzacions de tors complexos de tipus CM

Sigui K un cos de tipus CM, de grau $2n$ sobre $\mathbb{Q}$. Denotarem per K_0 el subcòs totalment real de K, i per $T = \{\varphi_1, \ldots, \varphi_n\}$ un tipus CM primitiu de K. Associada a aquest CM-tipus tenim la immersió:

$$\begin{aligned} \varphi = \varphi_T : K &\longrightarrow \mathbb{C}^n \\ \alpha &\longrightarrow \varphi(\alpha) = (\varphi_1(\alpha), \ldots, \varphi_n(\alpha)). \end{aligned}$$

Fixem un sub-$\mathbb{Z}$-mòdul $\mathfrak{m} \subset K$ de rang $2n$, i considerem el tor $A = \mathbb{C}^n/\varphi(\mathfrak{m})$ de CM-tipus (K, T). Denotarem per ι la injecció $K \hookrightarrow \mathrm{End}^0(A)$, i per $\mathcal{O} = \iota^{-1}(\mathrm{End}(A))$ l'ordre de K format per les multiplicacions complexes de A. En [Fe 00] s'ha explicat que donar una polarització del tor A equival a donar un nombre algebraic ξ que satisfaci les propietats següents:

P1) $K = K_0(\xi)$;

P2) $\xi^2 \in K_0$ ($\Rightarrow -\xi^2$ és totalment positiu);

P3) $\mathrm{Im}\,\varphi_k(\xi) > 0$, per a $k = 1, \ldots, n$.

La polarització associada a aquest element ξ es calcula segons la fórmula:

$$E_\xi(\alpha, \beta) = m\mathrm{Tr}_{K/\mathbb{Q}}(\xi\alpha\overline{\beta}), \qquad \alpha, \beta \in K,$$

on m és un enter *escaient*. (Observem que canviant l'element ξ per un múltiple enter $n\xi$ obtindríem una polarització equivalent.)

Aquesta construcció planteja un interrogant: està clar que l'element ξ determina la polarització E_ξ, però aquesta correspondència és unívoca? És a dir, podem trobar diferents elements ξ que donin lloc a una mateixa polarització? Per respondre aquesta qüestió ens convé analitzar amb una mica més de detall la polarització E_ξ. Per exemple, ens anirà bé saber quina isogènia $\Phi_\xi : A \longrightarrow A^*$ determina E_ξ.

7.3 Varietat dual d'una varietat abeliana de tipus CM

En [Ro 00] s'ha explicat la construcció de la varietat abeliana dual d'un tor complex polaritzat. Ara repassarem aquesta construcció per al cas concret d'un tor complex $A = \mathbb{C}^n/\varphi(\mathfrak{m})$ de tipus CM. El procés es basa en el següent aparellament de dualitat en $\mathbb{C}^n$:

$$\langle x, y\rangle = x \cdot \overline{y} + \overline{x} \cdot y,$$

que satisfà l'agradable relació:

$$\langle \varphi(\alpha), \varphi(\beta)\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\overline{\beta}) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta\overline{\alpha}), \qquad \alpha, \beta \in K.$$

La varietat dual de A és $A^* = \mathbb{C}^n/\varphi(\mathfrak{m}^*)$, on $\mathfrak{m}^* = \{\alpha \in K | \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\overline{\mathfrak{m}}) \subset \mathbb{Z}\}$ queda determinada per la condició $\varphi(\mathfrak{m}^*) = \{z \in \mathbb{C}^n | \langle \varphi(\mathfrak{m}), z\rangle \subset \mathbb{Z}\}$. Observem que, per construcció, A^* té tot l'aspecte d'un tor complex de tipus CM. Efectivament:

Proposició 7.3.1. *La varietat abeliana A^* és una varietat abeliana de tipus CM, amb el mateix CM-tipus normalitzat que A.*

Demostració: El pas al dual dóna una bijecció $\wedge : \mathrm{End}(A) \longrightarrow \mathrm{End}(A^*)$, que composada amb la injecció $\iota : K \hookrightarrow \mathrm{End}^0(A)$ ja ens diu que A^* és una varietat abeliana de tipus CM. Per concretar el CM tipus ens cal observar que, si $S(\eta) = \mathrm{diag}(\varphi_1(\eta), \ldots, \varphi_n(\eta))$,

$$\langle S(\eta)\varphi(\alpha), \varphi(\beta)\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\eta\alpha\overline{\beta}) = \langle \varphi(\alpha), S(\overline{\eta})\varphi(\beta)\rangle.$$

Com que K és dens en $\mathbb{C}$, això ens assegura que $S(\overline{\eta})$ és la representació analítica de l'endomorfisme $\widehat{\iota(\eta)} \in \mathrm{End}(A^*)$. La injecció $\eta \mapsto \widehat{\iota(\eta)}$ ens dóna un CM-tipus que no conté la identitat. Podem normalitzar-lo composant-lo

amb la conjugació complexa: si definim

$$\iota^* : K \hookrightarrow \mathrm{End}^0(A^*)$$
$$\iota^*(\alpha) := \widehat{\overline{\alpha}}$$

veiem que el CM-tipus de (A^*, ι^*) coincideix amb el de A. □

El mateix argument usat en la demostració ens diu que

$$E_\xi(\varphi(\alpha), \varphi(\beta)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi\alpha\overline{\beta}) = \langle S(\xi)\varphi(\alpha), \varphi(\beta)\rangle.$$

és a dir, que $S(\xi)$ és la representació racional de la isogènia donada per la polarització E_ξ:

Proposició 7.3.2. *La isogènia Φ_ξ associada a la polarització E_ξ ve donada per:*

$$\begin{aligned} \Phi_\xi : A &\longrightarrow A^* \\ (x_1, \ldots, x_n) &\longrightarrow (\varphi_1(\xi)x_1, \ldots, \varphi_n(\xi)x_n). \end{aligned}$$

Per acabar de lligar les coses, podem calcular també la representació racional de Φ_ξ. Per fer-ho, fixem una $\mathbb{Z}$-base $\{u_1, \ldots, u_n\}$ de $\mathfrak{m}$ i prenem la base dual $\{u_1^*, \ldots, u_n^*\}$ de $\mathfrak{m}^*$ (respecte a l'aparellament $\mathrm{Tr}_{K/\mathbb{Q}}$). Si escrivim $\Phi_\xi(u_j) = \sum \lambda_{jk} u_k^*$, llavors

$$\lambda_{jk} = \langle \Phi_\xi(\varphi(u_j)), \varphi(u_k)\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\xi u_j \overline{u_k}) = E(u_j, u_k).$$

Així doncs:

Proposició 7.3.3. *La representació racional de la isogènia Φ_ξ respecte a bases duals de $\mathfrak{m}$ i $\mathfrak{m}^*$ és la matriu de la forma de Riemann E_ξ en aquestes bases. En particular,* $\deg \Phi_\xi = \det E_\xi$.

Proposició 7.3.4.

a) Siguin $\xi_1, \xi_2 \in K$ dos elements que satisfan les propietats P1-P3. Denotem per $\Phi_{\xi_1}^{-1}$ la isogènia inversa (mòdul $\mathbb{Q}$) de Φ_{ξ_1}. La composició $\Phi_{\xi_1}^{-1} \circ \Phi_{\xi_2}$ és un endomorfisme de A, que correspon a la multiplicació per $\xi_1^{-1}\xi_2$, és a dir:

$$\Phi_{\xi_1}^{-1} \circ \Phi_{\xi_2} = \iota(\xi_1^{-1}\xi_2).$$

L'element $\xi_1^{-1}\xi_2$ pertany al subcòs totalment real K_0 i és totalment positiu.

b) Les polaritzacions E_{ξ_1}, E_{ξ_2} són equivalents si i només si hi ha una unitat $u \in \mathcal{O}^*$ i un nombre racional positiu $s \in \mathbb{Q}^+$ tal que $\xi_1^{-1}\xi_2 = su\overline{u}$.

c) $\mathrm{Aut}(\{A, \Phi_\xi\}) = \iota(\mu(\mathcal{O}^*))$.

Demostració: El primer apartat és conseqüència directa de l'expressió de la isogènia Φ_ξ donada en la proposició 7.3.2. Quant al segon apartat, podem suposar que les dues polaritzacions són principals (i.e., són de grau 1) i veure que tenim un isomorfisme de varietats abelianes polaritzades entre (A, Φ_{ξ_1}) i (A, Φ_{ξ_2}). Això equival a l'existència d'un automorfisme f que faci commutar el diagrama:

$$\begin{array}{ccccc} & A & \xrightarrow{\Phi_{\xi_1}} & A^* & \\ f & \downarrow & & \downarrow & \hat{f} \\ & A & \xrightarrow{\Phi_{\xi_1}} & A^*. & \end{array}$$

Ha de ser $f = \iota(u)$ per algun element $u \in \mathcal{O}^*$, i llavors $\hat{f} = \iota^*(\overline{u})$. Tenint en compte les representacions analítiques dels morfismes anteriors veiem que $\overline{u}\xi_2 u = \xi_1$, que és la relació que buscàvem. Invertint el raonament també veiem que si ξ_1, ξ_2 satisfan aquesta relació donen lloc a polaritzacions equivalents.

Pel que fa a l'apartat *c)*, queda clar que $\mathrm{Aut}(\{A, \Phi_\xi\}) = \{u \in \mathcal{O}^* | \, u\overline{u} = 1\}$. En ser $\{\varphi_1, \ldots, \varphi_n\}$ un tipus CM, d'aquí deduïm que $\varphi_i(u)\overline{\varphi_i(u)} = 1$, i per tant tots els conjugats de u tenen valor absolut 1. Això només pot passar si u és una arrel de la unitat. □

7.4 Un exemple

Il·lustrem els continguts de la secció anterior amb un exemple. Sigui $\zeta = e^{2\pi i/5}$ i considerem el cos $K = \mathbb{Q}(\zeta)$. És un cos de tipus CM, perquè és una extensió quadràtica totalment imaginària del cos $K_0 = \mathbb{Q}(\sqrt{5})$. Fixem el CM-tipus $T = (\varphi_1, \varphi_2)$, on φ_1 és la identitat i $\varphi_2(\zeta) = \zeta^2$.

Prenem com a $\mathbb{Z}$-submòdul de K l'anell d'enters $\mathfrak{m} = \mathcal{O}_K$. Un element ξ que ens permet polaritzar el tor corresponent a $\mathfrak{m}$ és $\xi = \zeta - \zeta^4$. Per determinar la polarització E_ξ, fixem com a $\mathbb{Z}$-base de $\mathcal{O}_K$ els elements

$\{u_1, u_2, u_3, u_4\} = \{1, \zeta, \zeta^2, z^3\}$. Es comprova ràpidament que:

$$E_\xi(\varphi(u_k), \varphi(u_{k+1})) = -E_\xi(\varphi(u_{k+1}), \varphi(u_k)) = 5, \ k = 1, 2, 3$$

$$E_\xi(\varphi(u_j), \varphi(u_k)) = 0 \ \text{ en la resta de casos.}$$

Així doncs, la matriu de E_ξ en aquesta base és

$$M_\xi = \begin{pmatrix} 0 & -5 & 0 & 0 \\ 5 & 0 & -5 & 0 \\ 0 & 5 & 0 & -5 \\ 0 & 0 & 5 & 0 \end{pmatrix}.$$

Aquesta matriu ens dóna una polarització de grau $\sqrt{\det M_\xi} = 5^2$ en el tor complex $A = \mathbb{C}^2/\varphi(\mathfrak{m})$. Per calcular $\mathfrak{m}^* = \{\alpha \in K | \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\overline{\mathfrak{m}})\}$, prenem $\alpha = \sum_k \lambda_k \zeta^k$ i imposem que $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta) \in \mathbb{Z}$ (notem que $\overline{\mathfrak{m}} = \mathfrak{m}$):

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 4\lambda_0 - \lambda_1 - \lambda_2 - \lambda_3$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta) = -\lambda_0 - \lambda_1 - \lambda_2 - \lambda_3$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta^2) = -\lambda_0 - \lambda_1 - \lambda_2 + 4\lambda_3$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta^3) = -\lambda_0 - \lambda_1 + 4\lambda_2 - \lambda_3.$$

Jugant amb aquestes expressions, veiem que són enteres si, i només si, $5\lambda_1 \in \mathbb{Z}$, $5\lambda_3 \in \mathbb{Z}$, $5\lambda_4 \in \mathbb{Z}$, $\sum_k \lambda_k \in \mathbb{Z}$. Així doncs:

$$\mathfrak{m}^* = \mathbb{Z}\langle \frac{1-\zeta}{5}, \frac{\zeta^2-\zeta}{5}, \frac{\zeta^3-\zeta}{5}, \zeta \rangle =: \mathbb{Z}\langle v_1, v_2, v_3, v_4 \rangle,$$

i la varietat abeliana dual de A és $A^* = \mathbb{C}^2/\varphi(\mathfrak{m}^*)$. Notem que

$$\mathfrak{m}^* = \frac{\xi}{5}\mathbb{Z}[\zeta] = \frac{\xi}{5}\mathfrak{m}.$$

La isogènia Φ_ξ que correspon a la polarització E_ξ és

$$\begin{array}{ccc} A & \longrightarrow & A^* \\ (z_1, z_2) & \longrightarrow & ((\zeta - \zeta^4)z_1, (\zeta^2 - \zeta^3)z_2). \end{array}$$

La seva representació analítica és, òbviament:

$$S_\xi = \begin{pmatrix} \zeta - \zeta^4 & 0 \\ 0 & \zeta^2 - \zeta^3 \end{pmatrix}, \qquad \det S_\xi = -\sqrt{5}.$$

Tenim que

$$\ker \Phi_\xi = \frac{\xi^{-1}\mathfrak{m}^*}{\mathfrak{m}} = \frac{\frac{1}{5}\mathfrak{m}}{\mathfrak{m}} = \frac{\frac{1}{5}\mathbb{Z}[\zeta]}{\mathbb{Z}[\zeta]} \simeq \frac{\mathbb{Z}[\zeta]}{(5)} \simeq (\mathbb{Z}/5\mathbb{Z})^4,$$

i per tant el grau de Φ_ξ és 5^4 i l'exponent és 5. Per calcular la representació racional de Φ_ξ, hem de fixar bases de $\varphi(\mathfrak{m})$ i $\varphi_(\mathfrak{m}^*)$. Escollim

$$e_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, e_2 = \begin{pmatrix} \zeta \\ \zeta^2 \end{pmatrix}, e_3 = \begin{pmatrix} \zeta^2 \\ \zeta^4 \end{pmatrix}, e_4 = \begin{pmatrix} \zeta^3 \\ \zeta \end{pmatrix},$$

com a base de $\varphi(\mathfrak{m})$ i calculem la corresponent base dual de $\varphi(\mathfrak{m}^*)$. Aquesta ve donada per la inversa de la matriu $(\mathrm{Tr}_{K/\mathbb{Q}}(u_j\overline{v_k}))_{j,k}$. Fent els càlculs obtenim

$$e_1^* = \begin{pmatrix} \frac{1-\zeta^4}{5} \\ \frac{1-\zeta^3}{5} \end{pmatrix}, e_2^* = \begin{pmatrix} \frac{\zeta-\zeta^4}{5} \\ \frac{\zeta^2-\zeta^3}{5} \end{pmatrix}, e_3^* = \begin{pmatrix} \frac{\zeta^2-\zeta^4}{5} \\ \frac{\zeta^4-\zeta^3}{5} \end{pmatrix}, e_4^* = \begin{pmatrix} \frac{\zeta^3-\zeta^4}{5} \\ \frac{\zeta-\zeta^3}{5} \end{pmatrix},$$

com a base de $\varphi(\mathfrak{m}^*)$. Tenim que:

$$\begin{aligned} \Phi_\xi(e_1) &= 5e_2^*, \\ \Phi_\xi(e_2) &= -5e_1^* + 5e_3^*, \\ \Phi_\xi(e_3) &= -5e_2^* + 5e_4^*, \\ \Phi_\xi(e_4) &= -5e_3^*. \end{aligned}$$

Per tant la representació racional de la isogènia Φ_ξ és

$$R_\xi = \begin{pmatrix} 0 & -5 & 0 & 0 \\ 5 & 0 & -5 & 0 \\ 0 & 5 & 0 & -5 \\ 0 & 0 & 5 & 0 \end{pmatrix},$$

i coincideix amb la matriu de E_ξ en la base $\{e_1, e_2, e_3, e_4\}$. Veiem novament que el grau de la isogènia Φ_ξ és $\det R_\xi = 5^4$.

Posats a fer, també podem comprovar que se satisfan les relacions de Riemann: si $\Pi = (e_1, e_2, e_3, e_4)$, $\Pi' = (e_1^*, e_2^*, e_3^*, e_4^*)$ es té que

$$\begin{pmatrix} S_\xi & 0 \\ 0 & \overline{S_\xi} \end{pmatrix} \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} = \begin{pmatrix} \Pi' \\ \overline{\Pi}' \end{pmatrix} R_\xi.$$

Hem vist que l'exponent de Φ_ξ és 5, la qual cosa ens diu que podem trobar una isogènia g tal que $g \circ \Phi_\xi = [5]_A$. Naturalment aquesta isogènia és

$$\begin{aligned} \Phi_\xi^{-1} : A^* &\longrightarrow A \\ (z_1, z_2) &\longrightarrow (\frac{5}{\zeta - \zeta^4} z_1, \frac{5}{\zeta^2 - \zeta^3} z_2). \end{aligned}$$

Aquesta isogènia ha de tenir grau $\frac{\deg[5]_A}{\deg \Phi_\xi} = 1$, és a dir, és un isomorfisme. La representació racional de g respecte a les bases $\{e_1^*, e_2^*, e_3^*, e_4^*\}$ i $\{e_1, e_2, e_3, e_4\}$ és

$$5R_\xi^{-1} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & 0 \end{pmatrix}.$$

Val a dir, però, que aquesta isogènia no pot provenir d'una polarització, perquè $\operatorname{Im} \frac{5}{\zeta - \zeta^4} < 0$. En canvi, la isogènia $-g$ sí que prové d'una polarització: és la que dóna l'element $-\frac{5}{\zeta - \zeta^4}$. Podem comprovar-ho mitjançant les relacions de Riemann:

$$\begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} (-5R_\xi^{-1}) \begin{pmatrix} \Pi' \\ \overline{\Pi}' \end{pmatrix}^{-1} = \begin{pmatrix} -\frac{5}{z - z^4} & 0 & 0 & 0 \\ 0 & -\frac{5}{z^2 - z^3} & 0 & 0 \\ 0 & 0 & \frac{5}{z - z^4} & 0 \\ 0 & 0 & 0 & \frac{5}{z^2 - z^3} \end{pmatrix}.$$

7.5 CM-tipus polaritzats

A partir d'aquí suposarem que el tor complex $A = \mathbb{C}^n/\varphi(\mathfrak{m})$ amb el que treballem és principal, és a dir, que $\mathrm{End}(A) \simeq \mathcal{O}_K$ és l'ordre maximal de K. En aquest cas, podem suposar que la xarxa $\mathfrak{m}$ és un ideal fraccionari de K, de manera que l'ideal $\mathfrak{m}^*$ també ho és i ve donat per:

$$\mathfrak{m}^* = (\mathfrak{d}_{K/\mathbb{Q}}\overline{\mathfrak{m}})^{-1},$$

on $\mathfrak{d}_{K/\mathbb{Q}}$ denota la diferent absoluta del cos K.

Fixem un element $\xi \in K$ satisfent les propietats P1-P3, és a dir, fixem una polarització E_ξ en A. La isogènia $\Phi_\xi : A \longrightarrow A^*$ ara és una $(\xi)\mathfrak{d}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$-transformació (cf. [Fe 00]). Considerem l'ideal $\mathfrak{f} := \xi\mathfrak{d}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$ de K. En realitat aquest és un ideal de K_0 estès: $\mathfrak{f} = (\xi\mathfrak{d}_{K/K_0})(\mathfrak{d}_{K_0/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}})$ i $\xi\mathfrak{d}_{K/K_0}$ és un ideal de K_0, perquè si $\theta \in \mathcal{O}_K$, llavors $\xi(\theta - \overline{\theta})$ és invariant per la conjugació complexa. Denotarem per $\mathfrak{f}_0$ aquest ideal $(\xi\mathfrak{d}_{K/K_0})(\mathfrak{d}_{K_0/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}})$ de K_0. Direm que A és *una varietat abeliana CM de tipus polaritzat* $(K,T,\mathfrak{f}_0)$.

Ara sorgeixen una sèrie de qüestions típiques : donat un CM-tipus (K,T) i un ideal fraccionari $\mathfrak{f}_0$ de K_0, com podem saber si existeix alguna varietat abeliana CM de tipus polaritzat $(K,T,\mathfrak{f}_0)$? N'hi ha més d'una? Si és així, com podem detectar si són isomorfes?

Proposició 7.5.1. *Siguin (K,T) un tipus CM i $\mathfrak{f}_0$ un ideal de K_0. Condició necessària i suficient per a que existeixi una varietat abeliana CM de tipus polaritzat $(K,T,s\mathfrak{f}_0)$ per algun $s \in \mathbb{Q}^+$ és que existeixin un ideal $\mathfrak{m}$ de K i un element $\xi \in K$ satisfent les propietats P1-P3, tals que $\mathfrak{f}_0\mathcal{O}_K = \xi\mathfrak{d}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$.*

Suposem que tenim una varietat abeliana A de CM-tipus (K,T), amb dues polaritzacions E_{ξ_1}, E_{ξ_2} que donen lloc al mateix ideal $\mathfrak{f}_0$ de K_0. Això vol dir que les dues isogènies $\Phi_{\xi_1}, \Phi_{\xi_2}$ són $\mathfrak{f}_0 O_K$-multiplicacions, o sigui que els parells $(A, E_{\xi_1}), (A, E_{\xi_2})$ són isomorfs com a varietats abelianes polaritzades. Així doncs, la isogènia $\Phi_{\xi_1}^{-1}\Phi_{\xi_2} = \iota(\xi_1^{-1}\xi_2)$ ha de ser un isomorfisme. Ja sabíem (per la proposició 7.3.4) que $\xi_1^{-1}\xi_2$ és un element totalment positiu de K_0, però hem vist que en aquest cas a més és una unitat de K_0.

Si seguim el raonament anterior al revés, queda clar que a partir d'una varietat abeliana polaritzada (A, E_{ξ_1}) de tipus polaritzat $(K,T,\mathfrak{f}_0)$ podem construir-ne moltes d'isomorfes multiplicant l'element ξ_1 per una unitat totalment positiva de K_0. Si multipliquem per unitats del tipus $u\overline{u}$ amb $u \in \mathcal{O}_K^*$, les varietats que obtindrem seran isomorfes a la de partida com a varietats abelianes polaritzades.

Siguin

$$U = \{\text{unitats totalment positives de } K_0\},$$

$$U_1 = N_{K/K_0}(\mathcal{O}_K^*) \subseteq U.$$

Observem que U_1 és un subgrup d'índex finit de U.

Proposició 7.5.2. *Si existeix una varietat abeliana CM de tipus polaritzat $(K, T, \mathfrak{f}_0)$, llavors hi ha exactament $d = [U : U_1]$ classes d'isomorfisme de varietats abelianes polaritzades de tipus polaritzat $(K, T, \mathfrak{f}_0)$.*

Podem fer tots aquests comptes per al cos ciclotòmic d'exponent 5, $K = \mathbb{Q}(\zeta)$, que ja hem estudiat en la secció 7.4. En aquest cas tenim que

$$O_K^* = \langle -\zeta, 1+\zeta \rangle \simeq \mathbb{Z}/10Z \times \mathbb{Z}$$

$$O_{K_0}^* = \langle -1, \tfrac{1+\sqrt{5}}{2} \rangle \simeq \mathbb{Z}/2Z \times \mathbb{Z}$$

$$U = \langle \left(\tfrac{1+\sqrt{5}}{2}\right)^2 \rangle, U_1 = \langle N_{K/K_0}(1+\zeta) \rangle = \langle \left(\tfrac{1+\sqrt{5}}{2}\right)^2 \rangle.$$

Veiem que totes les varietats abelianes de tipus CM amb el mateix CM-tipus que la varietat que hem estudiat en la secció 7.4 són isomorfes com a varietats abelianes polaritzades.

7.6 CM-tipus polaritzats i isogènies

Fixem un CM-tipus (K, T), i una CM varietat abeliana polaritzada principal $(A = \mathbb{C}^n/\varphi(\mathfrak{m}), \Phi_\xi)$ de tipus polaritzat $(K, T, \mathfrak{f}_0)$. Sabem que existeixen $h = \#\mathrm{Cl}(K)$ classes d'isomorfisme de varietats abelianes (sense polaritzar) del mateix CM-tipus (K, T). Escollim representants $A_1 = A, A_2, \ldots, A_h$ d'aquestes classes d'isomorfisme. Totes aquestes varietats abelianes són isògines, per la qual cosa podem pensar-les com $\mathfrak{a}_k$-transformacions de A $(k = 2, \ldots, h)$ donades per certs ideals $\mathfrak{a}_k$ de $\mathcal{O}_K$. De fet, podem suposar directament que les varietats escollides són de la forma $A_k = \mathbb{C}^n/\varphi(\mathfrak{a}_k^{-1}\mathfrak{m})$. En aquesta situació podem concretar quan podem polaritzar les A_k amb el mateix tipus polaritzat $(K, T, \mathfrak{f}_0)$ que A:

Proposició 7.6.1. *La varietat $A_k = \mathbb{C}^n/\varphi(\mathfrak{a}_k^{-1}\mathfrak{m})$ admet una polarització de tipus polaritzat $(K, T, \mathfrak{f}_0)$ si i només si l'ideal $\mathfrak{a}_k\overline{\mathfrak{a}_k}$ és principal i està generat per un element $\alpha_k \in K_0$ totalment positiu:*

$$\mathfrak{a}_k\overline{\mathfrak{a}_k} = (\alpha_k), \qquad \alpha_k \in K_0, \qquad \alpha_k >> 0.$$

Observem que l'element α_k de la proposició no és únic. L'elecció d'un α_k equival a fixar una polarització de tipus $(K, T, \mathfrak{f}_0)$ en A_k i una isogènia $\lambda : A \longrightarrow A_k$.

Demostració: Recordem com es recupera l'ideal $\mathfrak{f}_0$ a partir de la polarització de la varietat:

$$\mathfrak{f}_0\mathcal{O}_K = \xi\mathfrak{d}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}.$$

Si l'ideal $\mathfrak{a}_k$ satisfà la condició de la proposició tindrem que

$$\mathfrak{f}_0\mathcal{O}_K = \xi\mathfrak{d}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}} = (\xi\alpha_k)\mathfrak{d}_{K/\mathbb{Q}}(\mathfrak{a}_k^{-1}\mathfrak{m})(\overline{\mathfrak{a}_k^{-1}\mathfrak{m}}).$$

Recíprocament, suposem que A_k admet una polarització Φ_{ξ_k} de tipus polaritzat $(K, T, \mathfrak{f}_0)$, de forma que

$$\mathfrak{f}_0\mathcal{O}_K = (\xi_k)\mathfrak{d}_{K/\mathbb{Q}}(\mathfrak{a}_k^{-1}\mathfrak{m})(\overline{\mathfrak{a}_k^{-1}\mathfrak{m}}).$$

Fixem una isogènia $\lambda : A \longrightarrow A_k$. Considerem el diagrama:

$$\begin{array}{ccccc} A & \longrightarrow & A^* & \xrightarrow{\Phi_\xi^{-1}} & A \\ \lambda\downarrow & & \downarrow\hat{\lambda} & & \\ A_k & \xrightarrow{\Phi_{\xi_k}} & A_k^*. & & \end{array}$$

La composició $g_\lambda = \hat{\lambda}\Phi_{\xi_k}\lambda$ és una segona polarització $\Phi_{\xi'_k}$ de A, la qual cosa ens diu, per la proposició 7.3.4, que $g_\lambda\Phi_\xi^{-1} = \iota(\alpha_k)$ on $\alpha_k = \xi'_k\xi^{-1}$ és un element totalment positiu de K_0. Com que λ ha de ser una $\mathfrak{a}_k$-multiplicació, $\hat{\lambda}$ serà una $\overline{\mathfrak{a}_k}$-multiplicació, i g_λ serà una $\mathfrak{f}\mathfrak{a}_k\overline{\mathfrak{a}_k}$-multiplicació. Així doncs $g_\lambda\Phi_\xi^{-1} = \iota(\alpha_k)$ serà alhora una $\mathfrak{a}_k\overline{\mathfrak{a}_k}$-multiplicació i una $\mathcal{O}_K$-multiplicació de A en A. Això força la igualtat $\mathfrak{a}_k\overline{\mathfrak{a}_k} = \alpha_k\mathcal{O}_K$. □

7.7 La família de les varietats abelianes amb CM

Una foto de família del conjunt de les varietats abelianes amb multiplicació complexa per un mateix cos seria així: fixat el CM-tipus (K, T) sabem que hi ha $h = \#\mathrm{Cl}(K)$ classes d'isomorfisme de varietats abelianes principals del tipus donat. Si en cadascuna d'aquestes classes fem una classificació més fina, trobem d classes d'isomorfisme de varietats abelianes principals polaritzades de tipus polaritzat $(K, T, \mathfrak{f}_0)$, amb $\mathfrak{f}_0$ un ideal de $\mathcal{O}_{K_0}$.

Acabem amb una observació: en aquesta família pot haver-hi *incestos*, és a dir, podem trobar varietats abelianes polaritzades amb multiplicació complexa amb CM-tipus diferent que siguin isomorfes. Una feina pendent és caracteritzar completament aquests *incestos*.

Bibliografia

[Fe 00] J. Fernández. Construcció de varietats abelianes amb cm. 2000. en aquest volum.

[Ro 00] V. Rotger. *Enciclopèdia de butxaca de varietats abelianes.* Barcelona, 2000.

Capítol 8

Teoria de cossos de classes i multiplicació complexa

J. Guàrdia[1],
V. Rotger[1]
J.C. Lario
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

Introducció

Aquest capítol consta de tres parts: en la secció 1 presentem un esbós de la demostració del primer teorema principal de la multiplicació complexa que apareix en [Sh 98]. En la secció 2 s'explica l'enunciat de la versió adèlica d'aquest teorema. Finalment, en la secció 3, s'explica un resultat de Wei.

Notació: Al llarg d'aquest capítol, seguirem les notacions i convencions introduïdes en els capítols anteriors, especialment en [Fe 00] i [Gu 00]. En particular (K,T) sempre serà un CM-tipus CM, (K',T') denotarà el CM-tipus reflex i K_0 serà el subcòs totalment real maximal de K.

[1]Amb el suport parcial de la DGES: PB 96–0166.

8.1 El teorema principal de la multiplicació complexa

Aquesta secció és un esbós de la demostració del teorema principal de la multiplicació complexa que es troba en [Sh 98]. Exposarem els resultats principals de la demostració, intentant posar de manifest les idees que hi ha al darrera. Ometrem les demostracions detallades, perquè, per descomptat, és millor llegir-les directament en el llibre de Shimura.

8.1.1 CM tipus polaritzats i formes hermítiques

Siguin (A_1, ι_1, ξ_1), (A_2, ι_2, ξ_2) dues varietats abelianes polaritzades de CM-tipus polaritzat $(K, T, \mathfrak{f}_0)$. Podem suposar que $A_1 = \mathbb{C}^n/\varphi(\mathfrak{m})$ i $A_2 = \mathbb{C}^n/\varphi(\mathfrak{a}^{-1}\mathfrak{m})$ per a certs ideals $\mathfrak{m}, \mathfrak{a}$ de K. Cada isogènia $\lambda : A_1 \longrightarrow A_2$ determina un element totalment positiu $\alpha_\lambda \in K_0$ tal que $\Phi_{\xi_1}^{-1}\hat{\lambda}\Phi_{\xi_2}\lambda = \iota_1(\alpha_\lambda)$ i $\mathfrak{a}\overline{\mathfrak{a}} = (\alpha_\lambda)$ (cf. [Gu 00], sec. 7).

Lema 8.1.1. *Sigui $\xi \in \mathfrak{a}^{-1}$, i sigui λ una isogènia de A_1 en A_2. Se satisfà la relació:*

$$\alpha_{\lambda\iota_1(\xi)} = \alpha_\lambda \xi\overline{\xi}.$$

Aquest resultat ens fa veure que l'aplicació:

$$\begin{aligned} H_\lambda : \mathfrak{a}^{-1} &\longrightarrow \mathbb{C} \\ \xi &\longrightarrow \alpha_{\lambda\iota(\xi)} = \alpha_\lambda \xi\overline{\xi} \end{aligned}$$

s'estén a una forma hermítica sobre K. Partint de dues varietats abelianes polaritzades isògines, hem arribat a una forma hermítica sobre K. Podem estudiar aquestes formes hermítiques en abstracte. Fixem un CM-tipus (K, T). A cada ideal $\mathfrak{a}$ de $\mathcal{O}_K$ que satisfaci la propietat:

$$(*) \qquad \mathfrak{a}\overline{\mathfrak{a}} = (\alpha),\ \alpha \in K_0,\ \alpha \text{ totalment positiu.}$$

podem associar-li la forma hermítica:

$$\begin{aligned} K &\longrightarrow \mathbb{C} \\ w &\longrightarrow \alpha w\overline{w}, \end{aligned}$$

Aquesta forma, que denotarem $\{\mathfrak{a}, \alpha\}$, és definida positiva, i pren valors algebraics enters sobre $\mathfrak{a}^{-1}$.

Direm que dues formes hermítiques del tipus anterior, $\{\mathfrak{a}, \alpha\}, \{\mathfrak{b}, \beta\}$ són equivalents si per algun element $\mu \in K$ es té que $\mathfrak{b} = \mu\mathfrak{a}$ i $\beta = \alpha\mu\overline{\mu}$. Aquesta és una relació d'equivalència en el conjunt

$$S = \{\text{parells } (\mathfrak{a}, \alpha) \text{ que satisfan la condició } (*)\}.$$

Denotarem per $\mathfrak{C}(K)$ el conjunt de les classes d'equivalència per aquesta relació. Podem definir una operació natural entre els elements de $\mathfrak{C}(K)$, mitjançant la multiplicació component a component. Amb aquesta operació, el conjunt $\mathfrak{C}(K)$ esdevé un grup abelià. L'element neutre d'aquest grup és la classe d'equivalència de la forma $\{\mathcal{O}_K, 1\}$.

8.1.2 El CM-símbol d'Artin

Suposem donats un CM-tipus polaritzat $(K, T, \mathfrak{f}_0)$ i dues varietats abelianes polaritzades $\mathcal{P}_1 = (A_1, \iota_1, \xi_1)$, $\mathcal{P}_2 = (A_2, \iota_2, \xi_2)$ de CM-tipus polaritzat $(K, T, \mathfrak{f}_0)$. Sabem que A_2 ha de ser una $\mathfrak{a}$-transformació de A_1 per a cert ideal $\mathfrak{a}$ de K. A cada isogènia $\lambda : A_1 \longrightarrow A_2$ li hem associat una forma hermítica $H_\lambda = \{\mathfrak{a}, \alpha_\lambda\}$. Aquesta forma depèn de λ, però la seva classe en $\mathfrak{C}(K)$, gràcies al lema 8.1.1, és la mateixa per a qualsevol isogènia de A_1 en A_2. Aquesta classe la denotarem

$$\{\mathcal{P}_1 : \mathcal{P}_2\} := (\mathfrak{a}, \alpha_\lambda).$$

Proposició 8.1.2. *Siguin $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ tres varietats abelianes polaritzades amb el mateix CM-tipus polaritzat. Se satisfan les relacions següents*

a) $\{\mathcal{P}_3 : \mathcal{P}_2\}\{\mathcal{P}_2 : \mathcal{P}_1\} = \{\mathcal{P}_3 : \mathcal{P}_1\}$;

b) $\mathcal{P}_1 \simeq \mathcal{P}_2 \Leftrightarrow \{\mathcal{P}_1 : \mathcal{P}_2\} = (\mathcal{O}_K, 1)$;

c) $\mathcal{P}_1 \simeq \mathcal{P}_2 \Leftrightarrow \{\mathcal{P}_1 : \mathcal{P}_3\} = \{\mathcal{P}_2 : \mathcal{P}_3\}$.

Sigui $\mathcal{P} = (A, \iota, \xi)$ una varietat abeliana principal polaritzada de tipus $(K, T, \mathfrak{f}_0)$. Sigui L un cos de nombres sobre el qual $\mathcal{P}$ està definida (L haurà de contenir el cos reflex K' de K). Estenent L si cal, podem suposar que

i) L/K' és una extensió normal,

ii) Per a qualsevol $\sigma \in \mathrm{Gal}(L/K')$, tots els elements de $\mathrm{Hom}(A, A^\sigma)$ estan definits sobre L.

Sigui $\sigma \in \mathrm{Gal}(L/K')$. Sobre la varietat abeliana A^σ es pot definir de manera natural una estructura de CM-varietat polaritzada, amb el mateix tipus $(K, T, \mathfrak{f}_0)$ que A. Denotarem per $\mathcal{P}^\sigma := (A^\sigma, \xi_\sigma)$ aquesta nova varietat.

Proposició 8.1.3. *La forma hermítica $\{\mathcal{P}^\sigma : \mathcal{P}\}$ és independent de la varietat $\mathcal{P}$.*

La proposició 8.1.2 ens permet assegurar, doncs, que l'aplicació:

$$\begin{array}{rcl} u : \mathrm{Gal}(L/K') & \longrightarrow & \mathfrak{C}(K) \\ \sigma & \longrightarrow & u(\sigma) := [\sigma] := \{\mathcal{P}^\sigma : \mathcal{P}\} \end{array}$$

és un morfisme de grups, que anomenarem **CM-símbol d'Artin**.

8.1.3 El "first main theorem"

Sigui $(K, T, \mathfrak{f}_0)$ un CM-tipus polaritzat. Fixem una varietat abeliana polaritzada $\mathcal{P}$ de tipus $(K, T, \mathfrak{f}_0)$ i denotem per L_0 el seu cos de mòduli. Considerem la composició $L_0^* = L_0 K'$ El teorema principal de la multiplicació complexa ens descriurà la teoria de cossos de classes de l'extensió L_0^*/K'. Escollim un cos de nombres L sobre el qual estigui definida la varietat polaritzada $\mathcal{P}$. En particular, L contindrà L_0 i K'. Suposarem, com abans, que

i) L/K' és una extensió normal,

ii) Per a qualsevol $\sigma \in \mathrm{Gal}(L/K')$, tots els elements de $\mathrm{Hom}(A, A^\sigma)$ estan definits sobre L.

En aquestes condicions, sabem que el CM-símbol d'Artin és un morfisme de grups. Podem determinar el seu nucli:

$$\sigma \in \ker(u) \Longleftrightarrow [\sigma] = (\mathcal{O}_K, 1) \Longleftrightarrow \mathcal{P}^\sigma \simeq \mathcal{P} \Longleftrightarrow \sigma|_{L_0} = Id \Longleftrightarrow \sigma|_{L_0^*} = Id.$$

Així doncs $\ker(u) = \mathrm{Gal}(L/L_0^*)$, i el CM-símbol d'Artin dóna lloc a una injecció:

$$\overline{u} : \mathrm{Gal}(L_0^*/K') \simeq \mathrm{Gal}(L/K')/\mathrm{Gal}(L/L_0^*) \hookrightarrow \mathfrak{C}(K).$$

Com que el grup $\mathfrak{C}(K)$ és abelià, l'extensió L_0^*/K' ha de ser una extensió abeliana. Per poder dir més coses d'aquesta extensió, hem de saber calcular el CM-símbol d'Artin.

Sigui S el conjunt format pels primers de K' sobre els quals la varietat $\mathcal{P}$ té mala reducció i pels primers que ramifiquen en L_0^*. Posem $\mathfrak{m} = \prod_{\mathfrak{p} \in S} \mathfrak{p}$.

Proposició 8.1.4. *Sigui $\mathfrak{p} \notin S$ un primer de K' i sigui $\mathfrak{P}$ un primer de L que divideix $\mathfrak{p}$. Si $\sigma = \left(\frac{L/K'}{\mathfrak{P}}\right)$ és el morfisme de Frobenius associat a aquests primers:*

$$[\sigma] = \left(\prod_{\varphi \in T'} \mathfrak{p}^{\varphi}, N_{K'/\mathbb{Q}}(\mathfrak{p})\right).$$

Sigui $I_{K'}(\mathfrak{m})$ el grup dels ideals de K' coprimers amb $\mathfrak{m}$, i sigui $P_{K'}(\mathfrak{m})$ el subgrup de $I_{K'}(\mathfrak{m})$ format pels ideals principals (α), de manera que $\mathbf{Cl}_{\mathfrak{m}}(K) = I_{K'}(\mathfrak{m})/P_{K'}(\mathfrak{m})$ és el grup de classes d'ideals mòdul $\mathfrak{m}$. Considerem la composició $\tilde{u}$ del CM-símbol d'Artin amb el símbol d'Artin usual associat a l'extensió L_0^*/K':

$$\tilde{u} : I_{K'}(\mathfrak{m}) \xrightarrow{\left(\frac{L_0^*/K'}{\cdot}\right)} \mathrm{Gal}(L_0^*/K') \hookrightarrow \mathfrak{C}(K).$$

Tenim que:

$$P_{K'}(\mathfrak{m}) \subset H_1 := \ker \tilde{u} = \left\{ \mathfrak{a} \in I_{K'}(\mathfrak{m}) | \left(\prod_{\varphi^* \in T'} \mathfrak{a}^{\varphi^*}, N_{K'/\mathbb{Q}}(\mathfrak{a}) \right) = (\mathcal{O}_K, 1) \right\}.$$

Sigui $H_0 = \left\{ \mathfrak{a} \in I_{K'} | \exists \mu \in K \left(\prod_{\varphi^* \in T'} \mathfrak{a}^{\varphi^*}, \mu\overline{\mu} \right) = (\mathcal{O}_K, 1) \right\}$. Aquest grup de classes satisfà

$$P_{K'} \subset H_0 \subset I_{K'},$$

$$H_0 \cap I_{K'}(\mathfrak{m}) = H_1.$$

D'aquestes relacions traiem que

$$\mathrm{Gal}(L_0^*/K') \simeq I_{K'}(\mathfrak{m})/H_1 \simeq I_{K'}/H_0.$$

Teorema 8.1.5. (Primer teorema principal de la multiplicació complexa) *L'extensió L_0^*/K' és abeliana no ramificada i L_0^* és el cos de classes de K' corresponent al grup d'ideals H_0.*

8.1.4 Acotacions al teorema principal

Acabem aquesta exposició amb tres observacions sobre el teorema principal de la multiplicació complexa.

En primer lloc, notem que podem utilitzar aquest teorema com un bitllet d'anada i tornada entre el país de les varietats abelianes CM i el país de les extensions abelianes dels cossos de classes dels cossos CM. Podem viatjar d'un lloc a l'altre de manera explícita.

Ens cal dir que, igual com en el cas de les corbes el·líptiques, el primer teorema principal de la multiplicació complexa es complementa amb un **segon teorema principal**, que s'ocupa de les extensions abelianes ramificades dels cossos de tipus CM. Les tècniques que s'utilitzen per arribar a aquest segon teorema són essencialment les mateixes que hem emprat per al primer. El lector interessat en el tema trobarà aquest segon teorema en [Sh 98].

Els teoremes principals de la multiplicació complexa per a corbes el·líptiques són més *eficients* que els que tenim en el cas general, perquè ens permeten arribar a construir el cos de Hilbert i els *ray class fields* dels cossos quadràtics. En canvi, les versions d'aquests teoremes per a dimensió superior no ens diuen que puguem arribar tan amunt. La raó última d'aquestes diferències és que, en dimensió 1, totes les corbes el·líptiques del mateix CM-tipus que una donada són isomorfes a alguna conjugada seva (dit en altres paraules, el polinomi irreductible de l'invariant j té grau igual al nombre de classes del cos de la multiplicació complexa). Aquesta situació tan favorable no sol donar-se en dimensió superior.

8.2 El teorema principal, versió adèlica

Sigui (K,T) un CM-tipus. Considerem una varietat abeliana complexa polaritzada $\mathcal{P} = (A,L)$ de tipus (K,T). Suposem $\mathcal{P}$ definida sobre un cos de nombres k. En [Fe 00] es va veure que necessàriament el cos k conté el cos reflex K' de K. L'objectiu d'aquesta secció és descriure l'acció de $\mathrm{Gal}(\mathbb{C}/K')$ sobre la varietat abeliana polaritzada $\mathcal{P}$ i sobre els seus punts de torsió.

En [Ba 00] es va introduir el grup d'ideles $\mathbb{I}_{K'}$ del cos K' que mitjançant la teoria de cossos de classes ens descriu el grup de Galois de la màxima extensió abeliana ${K'}^{\mathrm{ab}}/K'$ del cos K': tenim un isomorfisme de grups, conegut com la llei de reciprocitat d'Artin

$$r_{K'} : \mathrm{Gal}({K'}^{\mathrm{ab}}/K') \xrightarrow{\cong} C_{K'} = \mathbb{I}_{K'}/{K'}^{*}.$$

La versió adèlica del teorema principal de la multiplicació complexa tradueix l'acció de Galois sobre la varietat abeliana en termes d'ideles. Per a fer-ho,

cal conèixer la relació entre les ideles i els ideals dels cossos K i K', que resumim en la proposició següent.

Proposició 8.2.1. *Sigui (K',T') el CM-tipus reflex de (K,T).*

i) L' aplicació norma

$$\begin{array}{rcl} N_{K'} : K' & \to & K \\ x & \to & \Pi_{\Phi' \in T'} \Phi'(x) \end{array}$$

s'estén de manera natural al grup d'ideles dels cossos K' i K:

$$N_{K'} : \mathbb{I}_{K'} \longrightarrow \mathbb{I}_K.$$

ii) Sigui $\mathfrak{a} \subset K$ un ideal i sigui $t \in \mathbb{I}_K$ un idele. Aleshores existeix un únic ideal $\mathfrak{b} \subset K$ tal que per tota plaça no arquimediana v de K, $\mathfrak{b}_v = t_v \cdot \mathfrak{a}_v$. Aquest ideal és de fet

$$\mathfrak{b} = \cap_v t_v \cdot \mathfrak{a}_v$$

on v recorre les places no arquimedianes de K.

Teorema 8.2.2. (Teorema principal de la CM, versió adèlica) *Sigui (K,T) un CM-tipus. Considerem una varietat abeliana complexa polaritzada $\mathcal{P} = (A,L)$ de tipus (K,T), definida sobre un cos $k \supset K'$. Sigui $\mathfrak{a} \subset K$ un ideal de K tal que existeix un isomorfisme de varietats abelianes complexes*

$$\theta : \mathbb{C}^n / T(\mathfrak{a}) \xrightarrow{\cong} A$$

i notem E a la forma de Riemann associada a la polarització $\theta^*(L)$ en $\mathbb{C}^n/T(\mathfrak{a})$.

Sigui $\sigma \in \mathrm{Gal}(\mathbb{C}/K')$ i sigui $s = r_{K'}(\sigma)$ la idele associada a la restricció de σ a la màxima extensió abeliana $K'^{\,ab}$ de K'.

Aleshores:

i) $\mathcal{P}^\sigma$ és una varietat abeliana de tipus (K,T). Sigui $t = N_{K'}(s^{-1}) \in \mathbb{I}_K$ i considerem l'ideal $\mathfrak{b} = t \cdot \mathfrak{a} \subset K$. Existeix un isomorfisme de varietats abelianes complexes

$$\theta_\sigma : \mathbb{C}^n / T(\mathfrak{b}) \xrightarrow{\cong} A^\sigma$$

tal que la forma de Riemann associada a la polarització $\theta_\sigma^*(L^\sigma)$ en $\mathbb{C}^n/T(\mathfrak{b})$ és $c_1(\theta_\sigma^*(L^\sigma) = N_{K'/\mathbb{Q}}(s) \cdot E$.

ii) *$k(A_{tors})/k$ és una extensió abeliana.*

iii) *Tenim uns isomorfismes naturals*

$$K'/\mathfrak{a} \xrightarrow{\theta\cdot T} A_{tors},$$

$$K'/\mathfrak{b} \xrightarrow{\theta_\sigma\cdot T} A^{\sigma}_{tors}.$$

iv) *L'isomorfisme θ_σ es pot triar de manera única tal que obtenim un diagrama commutatiu d'isomorfismes*

$$\sigma\cdot\theta\cdot T = \theta_\sigma\cdot T\cdot(\cdot t).$$

Observem que aquesta relació ens descriu l'acció de Galois sobre la torsió de la varietat abeliana en termes d'ideles.

8.3 Un resultat de Wei

Sigui G un grup i $H \subseteq G$ un subgrup d'índex finit. Triem γ's en G de manera que formin un sistema de representants de les classes laterals per l'esquerra:

$$G = \bigcup \gamma H\,.$$

Per a cada $g \in G$ tenim una igualtat $g\gamma = \gamma' h_\gamma$ per a cert representant γ' i $h_\gamma \in H$. L'aplicació $G \to H$ que envia $g \mapsto \prod_\gamma h_\gamma$ està mal definida, però no ja és així quan la definim sobre els abelianitzats respectius. Així formem el *transferidor*:

$$\begin{aligned} \mathrm{Ver}\colon G^{\mathrm{ab}} &\longrightarrow H^{\mathrm{ab}} \\ g \bmod G' &\longmapsto \prod_\gamma h_\gamma \bmod H'\,. \end{aligned}$$

Recordem que $G^{\mathrm{ab}} = G/G'$ és el màxim quocient abelià de G; si G és abelià, $G^{\mathrm{ab}} = G$ i $\mathrm{Ver}(g) = g^{[G:H]}$.

Combinant amb la teoria de Galois, el transferidor satisfà bones propietats respecte les torres d'extensions normals. En particular, commuta functorialment amb l'isomorfisme de reciprocitat d'Artin. Aquest fet és l'instrument clau per al resultat principal de la tesi de W. Weil (1994).

Sigui K un cos de nombres de tipus CM. Considerem el diagrama de cossos:

$$\begin{tikzcd}
 & & \overline{\mathbf{Q}} \\
 & K^{\mathrm{ab}} \arrow[ur, dash] \arrow[d, dash] & \\
K \arrow[ur, dash] \arrow[d, dash, "2"'] & K_0^{\mathrm{ab}} \arrow[d, dash] & \\
K_0 \arrow[ur, dash] \arrow[d, dash, "\mathrm{tr}"'] & & \\
 & \mathbf{Q}^{\mathrm{ab}} & \\
\mathbf{Q} \arrow[ur, dash] & &
\end{tikzcd}$$

Sigui H la imatge de $\mathrm{Gal}(K_0^{\mathrm{ab}}/K_0\mathbf{Q}^{\mathrm{ab}})$ pel transferidor:

$$\begin{tikzcd}
\mathrm{Ver}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/K_0)^{\mathrm{ab}} \arrow[r] \arrow[d, dash, "\sim"'] & \mathrm{Gal}(\overline{\mathbf{Q}}/K)^{\mathrm{ab}} \arrow[d, dash, "\sim"'] \\
\mathrm{Gal}(K_0^{\mathrm{ab}}/K_0) & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\
\mathrm{Gal}(K_0^{\mathrm{ab}}/K_0\mathbf{Q}^{\mathrm{ab}}) \arrow[u, hook] \arrow[r, dashed] & H \arrow[u, hook]
\end{tikzcd}$$

Teorema 8.3.1 (W. Wei). *Si adjuntem a K els moduli de totes les varietats abelianes amb CM i reflex dins K, així com els seus punts de torsió obtenim el subcòs de K^{ab} fix per H.*

Aquest resultat explica que no podem aspirar a reconstruir K^{ab} només a base de varietats abelianes amb CM i llurs punts de torsió, com passa en el cas de cossos quadràtics imaginaris. En general, només obtenim $(K^{\mathrm{ab}})^H$. Per així dir-ho, la distància que ens separa d'obtenir tot K^{ab} ve marcada per les extensions abelianes de la subextensió totalment real K_0 de K, a part d'afegir les arrels de la unitat.

Per a més detalls podeu consultar la pàgina `html` de J. Milne (director de tesis de W. Wei) a `math.uiuc.edu`.

Bibliografia

[Ba 00] P. Bayer. El problema 12 de Hilbert. 2000. en aquest volum.

[Fe 00] J. Fernández. Construcció de varietats abelianes amb cm. 2000. en aquest volum.

[Gu 00] J. Guardia. Polaritzacions de varietats abelianes amb multiplicació complexa. 2000. en aquest volum.

[Ro 00] V. Rotger. *Enciclopèdia de butxaca de varietats abelianes.* Barcelona, 2000.

[Sh 98] G. Shimura. *Abelian Varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series.* Princeton Univ. Press, 1a edition, 1998.

Capítol 9

Formes modulars de Hilbert

A. Arenas[1]
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

En aquestes notes donem una breu introducció a la teoria clàssica de les formes modulars de Hilbert així com de la relació entre les funcions modulars de Hilbert i la teoria de cossos de classes (cf. [Fr], [Ga], [Shi4]).

Introducció

L'acció del grup modular $SL(2,\mathbb{Z})$ sobre el semiplà superior de Poincaré $\mathbb{H}$ s'esten de manera natural al cas del grup $\Gamma = SL(2,\mathcal{O}_F)$ en $\mathbb{H}^m$, on $\mathcal{O}_F$ és l'anell d'enters d'un cos de nombres totalment real F de grau m. $SL(2,\mathcal{O}_F)$ s'anomena el grup modular de Hilbert. Tot i que D. Hilbert no va publicar res sobre aquest tema, va encarregar al seu deixeble O. Blumenthal l'estudi de dominis fonamentals i cossos de funcions dels grups modulars de Hilbert [Bl]. Posteriorment, E. Hecke en els seus treballs sobre multiplicació complexa ([He1], [He2]) posà de manifest l'important paper que les funcions modulars de Hilbert tenen en la teoria de cossos de classes. També es va veure més tard la importància d'aquestes funcions en l'estudi de la deter-

[1]Amb el suport parcial de la DGES: PB 96–0166.

minació del nombre de representacions per formes quadràtiques en cossos de nombres totalment reals. Els quocients de $\mathbb{H}^m$ pels grups modulars de Hilbert compactificats foren estudiats, des del punt de vista de la teoria de funcions, per Maass ([Ma1], [Ma3]) i Gundlach [Gu] i així s'obtingueren exemples no trivials d'espais complexes compactes amb el resultat de que els cossos de funcions corresponents són cossos de funcions algèbriques. El 1970 Hirzebruch ([Hir1], [Hir2]) aconseguí resoldre les singularitats en el cas $m = 2$ i això va permetre precisar molts resultats relatius a l'estructura dels anells de formes modulars de Hilbert per a alguns cossos quadràtics reals. Finalment, cal esmentar l'impuls donat per G. Shimura, Hida, etc. en l'estudi de les varietats jacobianes intermèdies de varietats modulars de Hilbert que estiguin associades a caràcters de Hecke de cossos CM ([Shi1], [Shi2], [Shi3], [Hi1], [Hi2]).

9.1 El grup modular de Hilbert

Sigui F un cos de nombres totalment real de grau m i $\mathcal{O} = \mathcal{O}_F$ el seu anell d'enters. Donat un element a de F el considerarem a $\mathbb{R}^m$ via la immersió canònica $\sigma : F \hookrightarrow \mathbb{R}^m$ i el denotarem $a = (a_1, \ldots, a_m)$, $a_i \in \mathbb{R}$, $1 \leq i \leq m$. De la mateixa manera, donada una matriu $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2, F)$ denotarem per $\gamma = (\gamma_1, \ldots, \gamma_m) \in SL(2, \mathbb{R})^m$ les matrius $\gamma_j = \left(\begin{smallmatrix} a_j & b_j \\ c_j & d_j \end{smallmatrix}\right)$ donades per la immersió canònica de les entrades de γ. Notem que podem interpretar $SL(2, \mathcal{O})$ com un subgrup discret de $SL(2, \mathbb{R})^m$ ja que $\sigma(\mathcal{O})$ és una ret de $\mathbb{R}^m$.

Denotem per $\mathbb{H}^m = \{z = (z_1, \ldots, z_m) \in \mathbb{C}^m \mid Im\, z_j > 0,\ 1 \leq j \leq m\}$, el producte de m còpies del semiplà superior de Poincaré.

Definició 9.1.1. *El grup modular de Hilbert* Γ_F, d'un cos totalment real F de grau m, és el subgrup discret $\Gamma_F = SL(2, \mathcal{O})$ de $SL(2, \mathbb{R})^m$ amb la següent acció sobre $\mathbb{H}^m$:

Si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_F$ i $z \in \mathbb{H}^m$

$$\gamma z = \frac{az + b}{cz + d} := \left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \ldots, \frac{a_m z_m + b_m}{c_m z_m + d_m} \right) \in \mathbb{H}^m.$$

Propietats 9.1.2. Es té que:

i) Γ_F actua de forma pròpia i discontínua en $\mathbb{H}^n$.

ii) $\Gamma_F / \{\pm I\}$ actua fidelment en $\bar{\mathbb{H}}^m$, on $\bar{\mathbb{H}} = \mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ i $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

L'acció sobre el punt de l'infinit $\infty = (\infty, \ldots, \infty)$ s'estén de la manera usual: $\gamma\infty = (\frac{a_1}{c_1}, \ldots, \frac{a_m}{c_m})$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_F$. Notem que si $c_j = 0$, aleshores $\frac{a_j}{c_j} = \infty$.

Tot seguit donarem la definició de punt parabòlic i de punt el·líptic d'un subgrup discret qualsevol de $SL(2,\mathbb{R})^m$.

Definició 9.1.3. Sigui Γ un subgrup discret de $SL(2,\mathbb{R})^m$. Es defineix:

i) El grup de les *translacions* de Γ

$$\mathcal{T}_\Gamma = \{v \in \mathbb{R}^m \mid (z \mapsto z + v) \in \Gamma\},$$

ii) El grup dels *multiplicadors* de Γ

$$\mathcal{M}_\Gamma = \left\{ \lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{R}^m \;\middle|\; \begin{array}{l} \lambda_j > 0, \ 1 \leq j \leq m \\ \exists u \in \mathbb{R}^m, \ (z \mapsto \lambda z + u) \in \Gamma \end{array} \right\}.$$

iii) El punt de l'infinit $\infty = (\infty, \ldots, \infty)$ és un *punt parabòlic* respecte de Γ si i només si $\mathcal{T}_\Gamma \cong \mathbb{Z}^m$ i $\mathcal{M}_\Gamma \cong \mathbb{Z}^{m-1}$.

iv) Un punt $s \in \bar{\mathbb{R}}^m$, $\bar{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$, és un *punt parabòlic* respecte de Γ si i només si l'infinit és un punt parabòlic respecte del subgrup discret conjugat $\gamma\Gamma\gamma^{-1}$, on $\gamma(s) = \infty, \gamma \in SL(2,\mathbb{R})^m$. Aquesta definició és independent de l'element γ escollit que transforma s en ∞.

Tant el grup de les translacions com el dels multiplicadors s'obtenen de forma natural amb l'estudi del grup d'isotropia del punt de l'infinit.

Cal remarcar que el grup dels multiplicadors actua sobre el grup de les translacions: $(\lambda, v) \mapsto \lambda.v = (\lambda_1 v_1, \ldots, \lambda_m v_m)$. Això és correcte ja que si $\varphi(z) = \lambda z + u$ per a algun u tal que $\varphi \in \Gamma$ i $\tau(z) = z + v$, aleshores $\varphi \circ \tau \circ \varphi^{-1}$ és la translació $z \mapsto z + \lambda$ i d'ací s'obté fàcilment la relació: $\lambda_1 \ldots \lambda_m = 1$, d'on aplicant la immersió logarítmica i el fet de que $\mathcal{M}_\Gamma \subset \mathbb{R}^m$ és un subgrup discret resulta que $\mathcal{M}_\Gamma \cong \mathbb{Z}^k$, per a un cert $k < m$.

Definició 9.1.4. Un punt $z \in \mathbb{H}^m$ és un punt el·líptic respecte de un subgrup discret Γ de $SL(2,\mathbb{R})^m$ si existeix un element $\gamma = (\gamma_1, \ldots, \gamma_m)$ de Γ que fixa el punt z (i.e. $\gamma z = z$) tal que:

i) $\gamma_j \neq \pm I, \quad 1 \leq j \leq m.$

ii) Tota γ_j, $\quad 1 \leq j \leq m$, és d'ordre finit.

El conjunt de punts el·líptics respecte de Γ és un subgrup discret de $\mathbb{H}^m$.

Sigui $(\mathbb{H}^m)^*$ la unió de $\mathbb{H}^m$ amb el conjunt de punts parabòlics de Γ. En $(\mathbb{H}^m)^*$ es considera una topologia única tal que en $\mathbb{H}^m$ indueix la usual. A més a més, $\mathbb{H}^m$ és un subconjunt obert i dens dins $(\mathbb{H}^m)^*$. Si l'infinit és un punt parabòlic respecte de Γ, aleshores un sistema fonamental d'entorns de l'infinit ve donat pels conjunts

$$\mathcal{U}_N = \left\{ z \in \mathbb{H}^m \;\middle|\; \prod_{j=1}^{m} \operatorname{Im} z_j > N \right\} \cup \{\infty\}$$

per a $N = 1, 2, \ldots$, i aquest sistema es "transporta" als altres punts parabòlics, és a dir, si s és un altre punt parabòlic respecte de Γ i si $\gamma \in SL(2,\mathbb{R})^m$ compleix $\gamma(s) = \infty$, aleshores $\gamma^{-1}(\mathcal{U}_N)$ és un sistema fonamental d'entorns de s i és fàcil comprovar que aquest sistema és equivalent al definit per qualsevol altre $\gamma' \in SL(2,\mathbb{R})^m$ tal que $\gamma'(s) = \infty$.

És immediat comprovar que Γ actua sobre $(\mathbb{H}^m)^*$ i tot i que $(\mathbb{H}^m)^*$ no és localment compacte (si $(\mathbb{H}^m)^* \neq \mathbb{H}^m$), resulta que el quocient $X_\Gamma := \frac{(\mathbb{H}^m)^*}{\Gamma}$ sempre és Hausdorff i localment compacte.

Teorema 9.1.5. *Sigui Γ_F el grup modular de Hilbert $SL(2,\mathcal{O})$. Aleshores*

i) Els punts parabòlics respecte del grup modular de Hilbert són precisament les imatges de $F \cup \{\infty\}$ en $\bar{\mathbb{R}}^m$ a través de la immersió canònica.

ii) L'espai quocient

$$X_{\Gamma_F} = \frac{\mathbb{H}^m \cup F \cup \{\infty\}}{\Gamma_F}$$

és compacte. En particular, té un nombre finit de classes de punts parabòlics i de classes de punts el·líptics i si $m > 1$, aquestes classes són els punts singulars de X_{Γ_F} considerada com a varietat analítica de dimensió complexa m.

iii) El nombre de classes de punts parabòlics, respecte de Γ_F, és el nombre de classes del cos F ([Sh], §28).

Exemples de grups modulars de Hilbert

i) Cas $m = 1$ i.e., $F = \mathbb{Q}$ i $\Gamma_\mathbb{Q} = SL(2,\mathbb{Z}) = \langle s, t \rangle$. Es recupera el grup modular clàssic generat per $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i $t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

ii) $F = \mathbb{Q}(\sqrt{2})$, $[F : \mathbb{Q}] = 2$, $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ i $h_F = 1$, amb la qual cosa només existeix la Γ_F-classe de punts parabòlics de l'infinit.

Es té que el grup de Hilbert $\Gamma_F = SL(2, \mathbb{Z}[\sqrt{2}]) = \langle s, t,\ t_{\sqrt{2}},\ \gamma_{1+\sqrt{2}} \rangle$ on

$$s = \left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right),$$

$$t = \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right),$$

$$t_{\sqrt{2}} = \left(\begin{pmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -\sqrt{2} \\ 0 & 1 \end{pmatrix} \right),$$

$$\gamma_{1+\sqrt{2}} = \left(\begin{pmatrix} 1+\sqrt{2} & 0 \\ 0 & -1+\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1-\sqrt{2} & 0 \\ 0 & -1-\sqrt{2} \end{pmatrix} \right).$$

Definició 9.1.6. Sigui $\mathfrak{n} \subset \mathcal{O}$ un ideal propi no nul. El subgrup

$$\Gamma_F[\mathfrak{n}] = \{\gamma \in \Gamma_F \,|\, \gamma \equiv I \pmod{\mathfrak{n}}\}$$

s'anomena el *subgrup de congruència principal* de Γ_F de *nivell* $\mathfrak{n}$. $\Gamma_F[\mathfrak{n}]$ és el nucli del monomorfisme natural de grups: $SL(2, \mathcal{O}) \longrightarrow SL(2, \mathcal{O}/\mathfrak{n})$, per tant $\Gamma_F(\mathfrak{n})$ és normal dins de Γ_F. Com que $SL(2, \mathcal{O}/\mathfrak{n})$ és finit per ser-ho $\mathcal{O}/\mathfrak{n}$, resulta que $\Gamma_F(\mathfrak{n})$ és d'índex finit en Γ_F.

Un subgrup de Γ_F s'anomena un *subgrup de congruència de nivell* $\mathfrak{n}$ si conté $\Gamma_F[\mathfrak{n}]$. Un subgrup Γ' de Γ_F s'anomena un *subgrup de congruència* si existeix un ideal enter $\mathfrak{n} \subset \mathcal{O}_F$ tal que Γ' és un subgrup de congruència de nivell $\mathfrak{n}$. Els subgrups de Γ_F:

$$\Gamma_0(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_F \;\middle|\; c \equiv 0 \pmod{\mathfrak{n}} \right\}$$

$$\Gamma_1(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{n}) \;\middle|\; a \equiv d \equiv 1 \pmod{\mathfrak{n}} \right\}$$

són subgrups de congruència.

9.2 Formes modulars de Hilbert

Abans de definir les formes modulars de Hilbert, recordem que si $f : \mathbb{H}^m \to \mathbb{C}$ és holomorfa i compleix $f(z+v) = f(z)$ per a tot $z \in \mathbb{H}^m$ i tot v d'una ret L de $\mathbb{R}^m$, aleshores f admet un únic desenvolupament en sèrie de Fourier absoluta i uniformement convergent en subconjunts compactes de $\mathbb{H}^m$:

$$f(z) = \sum_{n \in L'} a_n \ \exp(2\pi i \langle n, z \rangle),$$

on la suma està estesa a la ret dual L' de L,

$$L' = \{w \in \mathbb{R}^m \mid \langle w, v \rangle \in \mathbb{Z}, \text{ per a tot } v \in L\}$$

on $\langle w, v \rangle$ abreuja l'expressió $w_1 v_1 + \cdots + w_m v_m$. Un element $w \in L'$ és no negatiu, i.e. $w \geq 0$, si i només si cada component de w és no negativa.

Si $f : \mathbb{H}^m \to \mathbb{C}$ és holomorfa i periòdica respecte de la ret de translacions $\mathcal{T}_\Gamma$ d'un subgrup discret Γ de $SL(2,\mathbb{R})^m$ que admet l'infinit com a punt parabòlic aleshores diem que f és *regular* en el punt de l'infinit si en el desenvolupament de Fourier anterior (per $L = \mathcal{T}_\Gamma$), els únics coeficients a_n no nuls que hi surten corresponen a n's no negatives. En aquest cas, també es diu que f és holomorfa en el punt de l'infinit.

Observació 9.2.1. Si a més de ser f regular en el punt de l'infinit, f s'anul·la en l'infinit, i.e. $f(\infty) := a_0 = 0$, aleshores es pot provar que $a_n \neq 0$ exigeix que totes les components de n siguin estrictament positives.

Definició 9.2.2. Una *forma automorfa de pes* $2k$, $k = (\kappa_1, \ldots, \kappa_m) \in \mathbb{Z}^m$ *respecte d'un subgrup discret* Γ de $SL(2,\mathbb{R})^m$ de quocient $(\mathbb{H}^n)^*/\Gamma$ compacte és una funció holomorfa $f : \mathbb{H}^m \to \mathbb{C}$ que compleix

i) $f(\gamma z) = \Big(\prod_{j=1}^{m} (c_j z_j + d_j)^{2\kappa_j}\Big) f(z)$, per a qualsevol $\gamma = (\gamma_1, \ldots, \gamma_m)$ de Γ, $\gamma_j = \left(\begin{smallmatrix} a_j & b_j \\ c_j & d_j \end{smallmatrix}\right)$, $1 \leq j \leq m$.

ii) f és regular (o holomorfa) en tots els punts parabòlics de Γ.

Expliquem tot seguit el que significa aquesta segona condició. Primer de tot la regularitat de f en el punt de l'infinit ja ha estat explicada si l'infinit és un punt parabòlic respecte de Γ. Ara, si $s \neq \infty$ és un punt parabòlic

respecte de Γ, sigui $\gamma \in SL(2,\mathbb{R})^m$ tal que $\gamma(s) = \infty$ i aleshores la funció

$$f_\gamma(z) := \prod_{j=1}^{m} \left((c_j z_j + d_j)^{2\kappa_j}\right) f(\gamma^{-1} z)$$

és regular en l'infinit, on ara denotem $\gamma_j^{-1} = \left(\begin{smallmatrix} a_j & b_j \\ c_j & d_j \end{smallmatrix}\right)$, $1 \leq j \leq m$.

En aquest segon cas la regularitat no depèn de la γ escollida que transforma s en ∞, a l'igual que la anul·lació o no de f_γ en l'infinit (però si $f_\gamma(\infty)$ és no nul, aquest valor si que depèn de γ). Si en ii) a més f s'anul·la en tots els punts parabòlics, la forma automorfa s'anomena *forma parabòlica*.

Si Γ_F és el grup modular de Hilbert d'un cos de nombres F totalment real i Γ és commensurable amb Γ_F (és a dir, $\Gamma \cap \Gamma_F$ té índex finit en Γ i en Γ_F) aleshores, una forma automorfa respecte de Γ s'anomena habitualment una *forma modular de Hilbert*.

Remarca 9.2.3. La condició ii) només cal comprovar-la per a un sistema complet de representants de punts parabòlics mòdul Γ-equivalència, en el sentit de que si per un punt parabòlic es compleix, aleshores es compleix automàticament per a tots els Γ-equivalents.

Notació 9.2.4. Si $k = (\kappa_1, \ldots, \kappa_m) \in \mathbb{Z}^m$, denotem per $\mathcal{M}_{2k}(\Gamma_F)$ l'espai vectorial sobre $\mathbb{C}$ de les formes modulars de Hilbert de pes $2k$ respecte de Γ_F. Denotem per $S_{2k}(\Gamma_F)$ l'espai vectorial de les formes parabòliques de Hilbert i

$$\mathcal{A}(\Gamma_F) = \left\{ f/g \mid \exists\, k \in \mathbb{Z}^m \text{ tal que } f, g \in \mathcal{M}_{2k}(\Gamma_F), \quad g \not\equiv 0 \right\}$$

el cos de les funcions modulars de Hilbert de pes 0 (cf. [Shi4]).

Observació 9.2.5. *Sigui* $k = (\kappa_1, \ldots, \kappa_m) \in \mathbb{Z}^m$. *Si* $\mathcal{M}_{2k}(\Gamma_F) \backslash S_{2k}(\Gamma_F) \neq \emptyset$, *aleshores* $\kappa_1 = \cdots = \kappa_m$.

Aquesta condició s'obté en estudiar l'acció dels multiplicadors sobre els desenvolupaments en sèrie de Fourier de les formes modulars no parabòliques.

La construcció general de formes parabòliques de Hilbert s'obté a partir de certes sèries de Poincaré. Anem ara a definir les sèries d'Eisenstein, respecte de Γ_F, una per a cada Γ_F-classe de punts parabòlics.

Sèries de Eisenstein. Sigui $\Gamma = \Gamma_F$ el grup modular de Hilbert d'un cos de nombres totalment real F. Es defineix la sèrie d'Eisenstein de pes $2k$, $k = (\kappa, \ldots, \kappa) \in \mathbb{Z}^m$, $\kappa \geq 2$, respecte del punt parabòlic de l'infinit

$$E_{2k}(z) = \sum \Big(\prod_{j=1}^{m} (c_j z_j + d_j) \Big)^{-2\kappa}$$

on la suma està estesa a un sistema complet qualsevol de representants de les classes laterals $\Gamma_\infty \gamma$ de Γ (Γ_∞ denota el subgrup d'isotropia de l'infinit). La sèrie d'Eisenstein de pes $2k$, $k = (\kappa, \ldots, \kappa) \in \mathbb{Z}^m$, $\kappa \geq 2$, respecte d'un punt parabòlic s de Γ_F es defineix transformant s en ∞ mitjançant un element adient $\gamma_0 \in SL(2, \mathbb{R})^m$ considerant després la corresponent sèrie d'Eisenstein respecte de l'infinit i tornant per γ_0^{-1}. S'obté la següent expressió

$$E_{2k}^s(z) = \sum \prod_{j=1}^{m} (c_j z_j + d_j)^{-2\kappa}$$

estant la suma estesa a un sistema complet de representants de les classes $(\gamma_0 \Gamma \gamma_0^{-1})_\infty \gamma$ amb $\gamma \in \gamma_0 \Gamma$.

Aquestes sèries són convergents per a $\kappa \geq 2$. Satisfan $E_{2k}^s(z) \in \mathcal{M}_{2k}(\Gamma)$. Els seus valors només depenen (llevat de constant) de la Γ-classe de s i s'anul·len en els punts parabòlics no equivalents a s.

Teorema 9.2.6. [Kl] *Sigui $\Gamma = \Gamma_F$ el grup modular de Hilbert d'un cos de nombres totalment real F de nombre de classes h.*

Aleshores

i) Si $s_1, \ldots, s_h$ són representants de les Γ-classes de punts parabòlics, les sèries d'Eisenstein $E_{2k}^{s_j}(z)$, $1 \leq j \leq h$, són linealment independents i generen un espai vectorial $\mathcal{E}(\Gamma)$ que només depèn de Γ i s'anomena l'espai de les sèries d'Eisenstein de pes $2k$ ($\kappa \geq 2$) respecte de Γ.

ii) $\mathcal{M}_{2k}(\Gamma) = S_{2k}(\Gamma) \oplus \mathcal{E}(\Gamma)$.

Observació 9.2.7. Si $\kappa = 1$ i $m \geq 2$, es pot definir la sèrie d'Eisenstein de pes $(2, \ldots, 2)$ respecte de Γ pel límit

$$E_2(z) = \lim_{\sigma \to 0^+} \sum \Big(\prod_{j=1}^{m} (c_j z_j + d_j) \Big)^{-2+\sigma}$$

on la suma està estesa a un sistema complet de representants de les classes laterals $\Gamma_\infty \gamma$ de Γ.

Teorema 9.2.8. *Sigui $k = (\kappa_1, \ldots, \kappa_m) \in \mathbb{Z}^m$ i $\Gamma = \Gamma_F$ el grup modular de Hilbert d'un cos de nombres totalment real F de grau m i de nombre de classes h. Aleshores*

1) $\mathcal{M}_{2k}(\Gamma) = 0$, si existeix un $\kappa_j < 0$.

2) $\mathcal{M}_0(\Gamma) \cong \mathbb{C}$, $0 = (0, \ldots, 0)$.

3) $\mathcal{M}_{2k}(\Gamma)$ i $S_{2k}(\Gamma)$ són $\mathbb{C}$-espais vectorials de dimensió finita [Ma2]. *En particular:*

$$\dim \mathcal{M}_{2k}(\Gamma) = h + \dim S_{2k}(\Gamma).$$

La dimensió dels espais de formes parabòliques de Hilbert es pot calcular a partir de la fórmula de les traces de Selberg (cf. [Sh]).

Exemples 9.2.9. i) Sigui $F = \mathbb{Q}(\sqrt{p})$, p primer. Aleshores la dimensió de l'espai de formes parabòliques de Hilbert de pes (2,2) és ([Hir2], [Pr] i [Si]):

$$\begin{cases} 0 & \text{si } p = 2, 3, 5 \\ \frac{1}{2}\,\zeta_F(-1) + \dfrac{h(-4p)}{8} + \dfrac{h(-3p)}{6} - 1 & \text{si } p \equiv 1 \pmod 4 \\ \dfrac{1}{2}\,\zeta_F(-1) + \dfrac{3}{4}\,h(-p) + \dfrac{1}{6}\,h(-12p) - 1 & \text{si } p \equiv 3 \pmod 8, \quad p > 5 \\ \dfrac{1}{2}\,\zeta_F(-1) + \dfrac{1}{6}\,h(-12p) - 1 & \text{si } p \equiv 7 \pmod 8 \end{cases}$$

on $\zeta_F(s)$ denota la funció zeta de Dedekind del cos de nombres F i $\zeta_F(-1) = 2^{-2} d_F^{3/2} \pi^{-4} \zeta_F(2)$ (d_F denota el discriminant de F).

ii) Si $F = \mathbb{Q}(\sqrt{6})$, aleshores la dimensió de l'espai de formes parabòliques de Hilbert de pes $k = (\kappa, \kappa)$, $\kappa > 2$, $S_k(SL(2, \mathbb{Z}[\sqrt{6}]))$ és [Ge]:

$$\frac{(\kappa-1)^2}{4} + \frac{3}{4} + \begin{cases} 0 & \text{si } \kappa \not\equiv 1 \pmod 3, \ \kappa \text{ parell}, \\ -1 & \text{si } \kappa \equiv 1 \pmod 3, \ \kappa \text{ parell}. \end{cases}$$

$$\frac{(\kappa-1)^2}{4} + \begin{cases} -1 & \text{si } \kappa \equiv 1 \pmod 3, \ \kappa \text{ senar}, \\ 0 & \text{si } \kappa \not\equiv 1 \pmod 3, \ \kappa \text{ senar}. \end{cases}$$

Donem ara propietats rellevants en el cas $F = \mathbb{Q}(\sqrt{2})$, (cf. [Gu], [Co1]). En aquest cas, $F = \mathbb{Q}(\sqrt{2})$, el nombre de classes és 1, per tant per a cada $\kappa \in \mathbb{Z}^+$ tenim una única sèrie d'Eisenstein $E_{2k}(z_1, z_2) \in \mathcal{M}_{2k}(\Gamma_F)$, $k = (\kappa, \kappa)$, que és la corresponent al punt parabòlic de l'infinit.

Teorema 9.2.10. *Sigui $F = \mathbb{Q}(\sqrt{2})$ i sigui $\Gamma_F = SL(2, \mathbb{Z}[\sqrt{2}])$ el corresponent grup modular de Hilbert.*

Aleshores:

i) L'anell graduat de les formes modulars de Hilbert de pes parell respecte del grup modular de Hilbert Γ_F és $\mathbb{C}[E_2, E_4, E_6]$.

ii) $f_4(z_1, z_2) = \frac{11\,E_2^2 - E_4}{576}$ és una forma parabòlica respecte de Γ_F de pes (4,4) *i*

$$f_6(z_1, z_2) = \frac{361\,E_2^2 - E_6 - 50976\,E_2\,f_4}{224640}$$

és una forma parabòlica respecte de Γ_F de pes (6,6).

iii) El cos de les funcions modulars de Hilbert de pes 0 *respecte de Γ_F és: $\mathcal{A} = \mathbb{C}(u, v)$ on $u = u(z_1, z_2) = E_2^2/f_4$ i $v = v(z_1, z_2) = E_2\,f_4/f_6$.*

El desenvolupament en sèrie de Fourier de les sèries d'Eisenstein $E_{2k}(z_1, z_2) \in \mathcal{M}_{2k}(\Gamma_F)$, $k = (\kappa, \kappa)$, $\kappa \in \mathbb{Z}^+$, respecte de la ret dual $\mathcal{T}'$ de les translacions de $\Gamma_F = SL(2, \mathbb{Z}[\sqrt{2}])$ en la base $\left\{\left(\frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2\sqrt{2}}, \frac{-1}{2\sqrt{2}}\right)\right\}$ és del tipus:

$$\sum_{(m,n)\in\mathbb{Z}^2} a_{mn}\ \exp\left[2\pi i\left[\left(\frac{m}{2} + \frac{n}{2\sqrt{2}}\right)z_1 + \left(\frac{m}{2} - \frac{n}{2\sqrt{2}}\right)z_2\right]\right]$$

amb les condicions:
$\frac{m}{2} + \frac{n}{2\sqrt{2}} \geq 0$ i $\frac{m}{2} - \frac{n}{2\sqrt{2}} \geq 0$ que són equivalents a $m \geq 0$ i $|n| \leq \sqrt{2}\,m$, i per tant, si fem $q = \exp[\pi i(z_1 + z_2)]$, i $q_0 = \exp\left[\pi i\left(\frac{z_1 - z_2}{\sqrt{2}}\right)\right]$ aleshores la sèrie de dalt s'escriu sota la forma

$$\sum_{\substack{m\geq 0\\ |n|\leq\sqrt{2}\,m}} a_{mn}\ q^m\ q_0^n = a_{00} + \sum_{\substack{m>0\\ |n|<m\sqrt{2}}} a_{mn}\ q^m\ q_0^n.$$

De fet resulta que llevat d'una constant multiplicativa es té (per a $m > 0$) $a_{mn} = \sigma_{2k-1}(n + m\sqrt{2})$, amb $\sigma_t(\alpha) = \sum_{(\mu)|(\alpha)} |\mu\mu'|^t$, per a qualsevol α de $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$.

Per a $\kappa = 1$, la corresponent sèrie d'Eisenstein normalitzada té el següent desenvolupament:

$$E_2(z) = 1 + q(48\,q_0^{-1} + 144 + 48\,q_0)$$
$$+\, q^2(336\,q_0^{-2} + 384\,q_0^{-1} + 720 + 384\,q_0 + 336\,q_0^2) + \ \ldots$$

Anàlogament es tenen els desenvolupaments de E_4 i E_6. En particular les formes parabòliques

$$f_4(z_1, z_2) \in S_4(\Gamma_F) \ \text{ i } \ f_6(z_1, z_2) \in S_6(\Gamma_F)$$

tenen els desenvolupaments:

$$f_4(z_1, z_2) = q\,(q_0^{-1} - 2 + q_0) + q^2(-4\,q_0^{-2} - 8\,q_0^{-1} + 24 - 8\,q_0 - 4\,q_0^2) + \ \ldots$$

$$f_6(z_1, z_2) = q + 2\,q^2(-q_0^{-2} - 8\,q_0^{-1} + 6 - 8\,q_0 - q_0^2) + \ldots$$

9.3 Aplicacions

E. Hecke a la seva tesi doctoral (1910) donà la primera aplicació aritmètica de l'estudi de les funcions modulars de Hilbert de pes zero ($m = 2$). Més concretament, sota certes restriccions Hecke (cf. [He1]) afirmà que en molts casos valors singulars de funcions modulars de Hilbert generen extensions abelianes de cossos biquadràtics (extensions quadràtiques totalment imaginaries d'un cos real quadràtic).

Els següents exemples ([Co1], [Co2], [Co3]) il·lustren els resultats de Hecke en termes de representacions, per formes quadràtiques, d'elements primers de l'anell d'enters d'un cos quadràtic real.

Exemples 9.3.1. Siguin $F = \mathbb{Q}(\sqrt{2})$ i π un element primer del seu anell d'enters $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ de norma $p \in \mathbb{Z}^+$ i L el cos biquadràtic $F(i\,\sqrt{2+\sqrt{2}})$. Aleshores:

i) π és representat per la forma quadràtica $X^2 + (2+\sqrt{2})\,Y^2$ si i només si p descompon en $L\Big(u(z,z'),\ v(z,z')\Big) = L$ on $z = i\,\sqrt{2+\sqrt{2}},\ z' = i\,\sqrt{2-\sqrt{2}};\ u(z,z') = 576,\ v(z,z') = 12.$

ii) π és representat per la forma quadràtica $X^2 + 2(2+\sqrt{2})Y^2$ si i només si p descompon en $L\Big(u(t,t'),\ v(t,t')\Big) = L(i)$ on $t = 2i(3+2\sqrt{2})\ \sqrt{2+\sqrt{2}}$, $t' = 2i(3-2\sqrt{2})\ \sqrt{2-\sqrt{2}}$, $u(t,t') = 721\Big(388 + 275\sqrt{2} + 30(1+\sqrt{2})^3\ \sqrt{2+\sqrt{2}}\Big)$, $v(t,t') = 6(2+5\sqrt{2} + 6\sqrt{2+\sqrt{2}})$.

Bibliografia

[Bl] O. Blumenthal, Über Modulfunktionen von mehreren Veränderlichen, I, II, *Math. Ann.* **56** (1903), 509–548, **58** (1904), 497–527.

[Co1] H. Cohn, An Explicit Modular Equation in Two Variables and Hilbert's Twelfth Problem, *Math. of Comput.* **38** (1982), 227–236.

[Co2] H. Cohn, Some examples of Weber-Hecke ring class field theory, *Math. Annalen* **265** (1983), 83–100.

[Co3] H. Cohn, *Some Special Complex Multiplications in Two Variables Using Hilbert Singular Moduli*, Number Theory Seminar (1989-90), Springer, 75–84.

[Fr] E. Freitag, *Hilbert Modular Forms*, Springer, 1990.

[Ga] P.B. Garret, *Holomorphic Hilbert Modular Forms*, Brooks/Cole Pub. Comp. 1990.

[Ge] G. van der Geer, Hilbert Modular Forms for the Field $\mathbb{Q}(\sqrt{6})$, *Math. Ann.* **233** (1978), 163–179.

[Gu] K.B. Gundlach, Die Bestimmung der Funktionen zu einiger Hilbertschen Modulgruppen, *Jour. reine angew. Math.* **220** (1965), 109–153.

[He1] E. Hecke, Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie, *Math. Annalen* **71** (1912), 1–37.

[He2] E. Hecke, Über die Konstruktion relativ-Abelscher Zahlkörper durch Modulfunktionen von zwei Variablen, *Math. Annalen*, (1913), 465–510.

[Hi1] H. Hida, On abelian varieties with complex multiplication as factors of the abelian variety attached to Hilbert modular forms, *Japan J. Math.* **5** (1979), 157–208.

[Hi2] H. Hida, On abelian varieties with complex multiplication as factors of the jacobians of Shimura curves, *Amer. J. Math.* **103** No. 4 (1981) 727–776.

[Hir1] F. Hirzebruch, *The Hilbert modular group, resolution of the singularities at the cusps and related problems*, Sém. Bourbaki, (1970-71), 275–288.

[Hir2] F. Hirzebruch, Hilbert modular surfaces, *L'Ens. Math.* **19** (1973), 183–281.

[Kl] H.D. Kloosterman, Theorie der Eisensteinschen Reihen von mehreren Veränderlichen, *Abh. Math. Sem. Hab.* **6** (1928), 163–188.

[Ma1] H. Maass, Über Gruppen von hyperabelschen Transformationen, *S. Ber. Heidelberg. Akad. Wiss.* (1940), 3–26.

[Ma2] H. Maass, Zur Theorie der automorphen Funktionem von n Veränderlichen, *Math. Ann.* **117** (1940), 538–578.

[Ma3] H. Maass, Über die Erweiterungsfähigkeit der Hilbertschen Modulgruppe, *Math. Zeitschrift* **51** (1948), 255–261.

[Pr] A. Prestel, Die elliptischen Fixpunkte der Hilbertschen Modulgruppen, *Math. Annalen* **177** (1968), 181–209.

[Sh] H. Shimizu, On discontinuous groups operating on the product of upper half planes, *Ann. of Math.* **77** (1963), 33–71.

[Shi1] G. Shimura, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, *Nagoya Math. J.* **43** (1971), 199–208.

[Shi2] G. Shimura, On the factors of the jacobian variety of a modular function field, *J. Math. Soc. Japan* **25** (1973), 523–544.

[Shi3] G. Shimura, On Eisenstein Series of Hilbert Modular Groups, *Rev. Mat. Iberoam.* **1** No. 3 (1985), 1–42.

[Shi4] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton Univ. Press, 1998.

[Si] C.L. Siegel, Zur Bestimmung des Volumens des Fundamentalbereichs der unimodularen Gruppe, *Math. Annalen* **137** (1959), 427–432.

Capítol 10

Superfícies abelianes amb CM

G. Cardona
Dept. de Matemàtica Aplicada 2
Universitat Politècnica de Catalunya
Pau Gargallo 5,
E-08028 Barcelona

Introducció

Un cop vist el cas de les varietats abelianes amb CM de dimensió 1, és a dir, les corbes el·líptiques, el següent cas a estudiar és el de les varietats de dimensió 2, és a dir, les superfícies abelianes amb CM. Dins aquest cas, si ens centrem en aquelles que són principalment polaritzades i simples ens trobem amb que necessitem estudiar les jacobianes de corbes de gènere 2. Aquesta xerrada està dirigida a l'estudi de les corbes de gènere 2 en general. En la xerrada de Jordi Guàrdia, es descriurà com buscar corbes de gènere 2 on la seva jacobiana té CM.

10.1 Models de corbes de gènere 2

Anem, en primer lloc, a descriure els models de corbes de gènere 2.

Sigui C de gènere 2 definida sobre $\overline{K}$. Els següent fets són ben coneguts:

- C és hiperel·líptica.
- C admet un model afí
$$y^2 = f(x)$$
amb $f \in \overline{K}[X]$ separable de grau 5 ó 6.
- Qualsevol altre model s'obté amb canvis associats a $M = \left(\begin{smallmatrix} m & n \\ q & p \end{smallmatrix}\right) \in \mathbf{GL}_2(\overline{K})$,
$$x' = \frac{mx+n}{px+q}$$
$$y' = \frac{(\det M)y}{(px+q)^3}.$$
Dit d'una altra manera, a partir d'un model d'una corba C obtenim totes les seves isomorfes fent canvis del tipus descrit.

10.2 Invariants d'Igusa de corbes de gènere 2

De la mateixa manera que en les corbes el·líptiques tenim l'invariant j, ens interessa poder classificar les corbes de gènere 2 a partir de certs invariants. Per motius històrics, introduïm en primer lloc els invariants d'Igusa. Més endavant veurem la teoria general d'invariants.

Considerem C una corba de gènere 2 donada per un model $y^2 = f(x)$ i posem:
$$\begin{aligned} f(x) &= a_0x^6 + a_1x^5 + \ldots a_5x + a_6 \\ &= a_0 \prod_{i=1}^{6} (x - \alpha_i). \end{aligned}$$

A partir de la descomposició de f en $\overline{K}$, definim els *invariants d'Igusa*
$$\begin{aligned} I_2(C) &= a_0^2 \sum (12)^2(34)^2(56)^2, \\ I_4(C) &= a_0^4 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\ I_6(C) &= a_0^6 \sum (12)^2(23)^2(31)^2(45)^2(56)^2 \\ &\qquad (64)^2(14)^2(25)^2(36)^2, \\ I_{10}(C) &= a_0^{10} \prod (ij)^2 = \operatorname{disc} f, \end{aligned}$$

on (ij) indica $\alpha_i - \alpha_j$ i els sumatoris s'estenen a totes les permutacions donant expressions diferents; dit d'una altra manera, s'estén als elements de $\mathfrak{S}_n$ mòdul el grup de simetries de les expressions.

Notem que, per ser simètrics, aquests invariants admeten una expressió polinòmica en els coeficients de f.

10.3 Formes binàries sèxtiques, covariants i invariants

Per tal de posar la descripció dels invariants de corbes de gènere 2 dins un marc més còmode, parlarem de formes binàries sèxtiques. Donada corba de gènere 2 per un model $y^2 = f(x)$, podem associar-li una forma binària sèxtica obtinguda per l'homogeneïtzació del polinomi f,

$$F(x_1, x_2) = x_2^6 f(x_1/x_2).$$

Les formes sèxtiques equivalents a una donada s'obtenen per canvis de variable anàlegs al cas de corbes de gènere 2. En concret, venen donats per:

$$\begin{aligned} x_1 &= mx_1' + nx_2' \\ x_2 &= px_1' + qx_2' \end{aligned}$$

amb $\left(\begin{smallmatrix} m & n \\ p & q \end{smallmatrix}\right) \in \mathbf{GL}_2(\overline{K})$.

Per tal de classificar formes sèxtiques, introduïm el que coneixem com a covariants i invariants.

Els covariants són polinomis

$$P \in \mathbb{Z}[a_0, a_1, a_2, a_3, a_4, a_5, a_6, x_1, x_2],$$

que en fer el canvi $M = \left(\begin{smallmatrix} m & n \\ p & q \end{smallmatrix}\right)$ compleixen:

$$P|_M = (\det M)^{-k} P.$$

Aquestes expressions són necessàriament homogènies en x_i i a_i, en el sentit que posant el polinomi en la forma

$$\sum_k c_k \prod a_i^{n_{i,k}} \prod x_i^{m_{i,k}},$$

es té que $\sum_i n_{i,k}$ i $\sum_i m_{i,j}$ no depenen de k. Anomenem *ordre* del covariant el grau en x_1, x_2 i *grau* del covariant el grau en les a_i.

A més de la definició dels covariants, cal notar que existeix un mètode explícit per a trobar-los tots. Aquesta construcció fa servir una operació, anomenada *Ueberschiebung*, que proporciona un covariant a partir d'altres dos. Partint del covariant donat per la forma, és a dir $P = F$, i aplicant reiteradament aquest procediment, els obtenim tots.

Dins els covariants de les formes sèxtiques, són especialment importants els que anomenem invariants i, a partir d'ells, definim els invariants absoluts.

Els *invariants* són els covariants d'ordre 0, mentre que per *invariants absoluts* entenem els quocients de dos invariants del mateix grau.

El conjunt dels invariants de les formes sèxtiques formen una $\mathbb{Z}$-àlgebra; és important destacar que aquesta àlgebra és finitament generada. De fet, està generada per 5 invariants:

$$C_2, C_4, C_6, C_{10}, R$$

de graus 2, 4, 6, 10 i 15, respectivament.

A més, els invariants C_i són independents i generen l'àlgebra d'invariants de grau parell.

Així doncs, si D és un invariant de grau parell $2k$, aquest es pot escriure de manera única en la forma

$$D = \sum_{2n_2+4n_4+6n_6+10n_{10}=2k} a_{(n)} C_2^{n_2} C_4^{n_4} C_6^{n_6} C_{10}^{n_{10}},$$

amb $a_{(n)} \in \mathbb{Q}$.

En particular, l'invariant R^2, de grau 30 s'escriu en termes dels C_i. El mateix passa amb els invariant d'Igusa definits abans.

A més dels invariants, notem que existeixen 3 covariants quadràtics,

$$X_1, X_2, X_3$$

que compleixen les igualtats següents:

$$\sum_{i,j} A_{i,j} X_i X_j = 0$$

$$\sum_{i,j,k} a_{i,j,k} X_i X_j X_k = R^3 f,$$

on $A_{i,j}$ i $a_{i,j,k}$ són invariants de grau $2(i+j+1)$ i $2(i+j+k+1)$ i, per tant, s'escriuen en funció de C_2, C_4, C_6 i C_{10}.

Si prenem els X_i com a variables, notem que tenim definida una cònica i una cúbica amb paràmetres que depenen dels invariants C_i de la forma.

A partir d'ara, i gràcies a la identificació feta entre corbes de gènere 2 i formes sèxtiques, parlarem d'invariants i covariants de corbes de gènere 2.

10.4 Condicions d'isomorfisme

Amb la maquinària dels invariants que hem introduït, podem donar condicions d'isomorfisme entre corbes de gènere 2.

Teorema 10.4.1. *Dues corbes C, C' de gènere 2, amb invariants C_i i C'_i respectivament, són isomorfes si, i només si, existeix λ tal que*

$$C_i = \lambda^i C'_i.$$

En aquesta situació, direm que els invariants C_i i C'_i són equivalents.

Podem donar versions equivalents de l'anterior resultat:

- C i C' són isomorfes si, i només si, existeix λ tal que per a tot invariant I de grau k, es té $I(C) = \lambda^k I(C')$.
- C i C' són isomorfes si, i només si, coincideixen tots els seus invariants absoluts.
- C i C' són isomorfes si, i només si, coincideixen els seus invariants absoluts:
$$\frac{C_2^5}{I_{10}}, \frac{C_4^5}{I_{10}^2}, \frac{C_6^5}{I_{10}^3}.$$

Notem que, en fer la darrera identificació hem fet servir invariants absoluts amb denominadors potències de I_{10}, que no s'anul·la mai.

Si $I_2 \neq 0$, podem donar una formulació equivalent en termes de 3 invariants absoluts especialment senzills:

$$i_1 = \frac{I_2^5}{I_{10}},\ i_2 = \frac{I_2^3 I_4}{I_{10}},\ i_3 = \frac{I_2^2 I_6}{I_{10}},$$

que anomenem els invariants absoluts d'Igusa. El fet que el denominador sigui de grau 10, resulta en expressions computacionalment més senzilles.

Com a recíproc del teorema de classificació tenim el següent teorema d'existència.

Teorema 10.4.2. *Donats $C_2, \ldots, C_{10}$, existeix una corba de gènere 2 definida sobre $\overline{K}$ tal que els seus invariants són equivalents a $C_2, \ldots, C_{10}$.*

Per al cas particular de treballar amb els invariants absoluts d'Igusa, podem reescriure l'anterior resultat com:

Teorema 10.4.3. *Donats i_1, i_2 i i_3, existeix una corba de gènere 2 definida sobre $\overline{K}$ tal que els seus invariants absoluts d'Igusa són i_1, i_2 i i_3.*

10.5 Grup d'automorfismes

Com a aplicació dels invariants de corbes de gènere 2, tenim que podem determinar el seu grup d'automorfismes coneixent els seus invariants.

Sigui C de gènere 2; el seu grup d'automorfismes ve donat per les següents possibilitats en funció de relacions entre els seus invariants.

Aut(C)	Condicions
Cas 0	
C_2	$R \neq 0$
Cas 1	
$C_2 \times C_2$	$R = 0$
Cas 1a	
$C_2 \times D_6$	$C_6^2 - 1/6C_4^3 = 0$
	$9C_{10} - 2C_4(6C_6 + C_2C_4) = 0$
Cas 1b	
D_8	$3C_2C_4^2 - 6C_4C_6 + 4C_2^2C_6 - 18C_{10} = 0$
	$4C_4^3 + 5C_2C_4C_6 + 6C_6^2 - 3C_2C_{10} = 0$
Cas 1a1	
$2\,D_{12}$	$6C_4 - C_2^2 = 0$
	$6C_6 + C_2C_4 = 0$
	$C_{10} = 0$
Cas 1b2	
$\tilde{S}_4$	$C_4 = 0$
	$C_6 = 0$
	$C_{10} = 0$
Cas 2	
C_{10}	$C_2 = 0$
	$C_4 = 0$
	$C_6 = 0$

10.6 El cos de definició

Fins ara, hem estat treballant sobre un cos algebraicament tancat. El que pretenem fer és relacionar el cos de definició de la corba amb el cos on es troben definits els seus invariants.

Una corba $C_{/K}$ de gènere 2 diem que està completament definida sobre K, i ho notarem com $C_{//K}$, si existeix un morfisme $\pi : C \to \mathbb{P}^1$ de grau 2 definit sobre K. Aquesta condició és equivalent a que admeti un model del tipus $y^2 = f(x)$ amb coeficients a K.

Donat que definim els invariants d'una corba a partir d'un model, és evident que si $C_{//K}$, aleshores $C_i \in K$.

El recíproc no és en general cert. Donada una quaterna $C_2, \ldots, C_{10} \in K$, per tal de decidir si existeix una corba de gènere 2 totalment definida sobre K que els té com a invariants, hem de tenir en compte quin seria el seu grup d'automorfismes, que determinem fent servir la taula anterior.

Teorema 10.6.1. *Donats C_2, C_4, C_6, $C_{10} \in K$ corresponents al cas de grup d'automorfismes no abelià o cíclic d'ordre 10, aleshores existeix una corba de gènere 2 totalment definida sobre K que els té com a invariants.*

Teorema 10.6.2. *Donats C_2, C_4, C_6, $C_{10} \in K$ corresponents al cas 0, existeix $C_{//K}$ de gènere 2 que els té com a invariants si, i només si, la cònica*

$$L : \sum A_{i,j} x_i x_j$$

té un punt K-racional.

Teorema 10.6.3. *Per al cas 1, existeix una construcció anàloga amb uns altres covariants i invariants.*

10.7 Construcció explícita

Anem a veure com poder fer explícit el teorema d'existència de models vist anteriorment. Evidentment, aquesta construcció explícita depèn del grup d'automorfismes de la corba, que podem determinar coneixent els invariants.

Cas 0:

Suposem trobat un punt K-racional de la cònica L. Amb aquest punt construïm un isomorfisme:

$$\begin{aligned} \varphi_{/K} : \mathbb{P} &\to L \\ x &\mapsto (x_1, x_2, x_3) \end{aligned}$$

Al substituir en la cúbica

$$M : \sum a_i a_j a_k x_i x_j x_k$$

obtenim

$$R^3 f(x),$$

un model de la corba buscada.

Observació 10.7.1. *Com "més senzill" sigui el punt racional de L trobat, "més senzill" serà el model obtingut.*

Cas 1:

Aquest cas, que no expliquem amb detall, es resol amb un procediment anàleg a l'anterior fent servir uns altres invariants i covariants quadràtics.

Cas 1a:

En aquest cas, basta prendre la corba:

$$y^2 = x^6 + x^3 + \frac{3C_4C_6 - C_{10}}{50C_{10}}$$

Cas 1b:

Anàlogament, podem prendre:

$$y^2 = x^5 + x^3 + \frac{3\left({C_4}^3 - 6\,{C_6}^2\right)}{20\left(-{C_4}^3 + 6\,{C_6}^2 + 12\,C_2\,C_{10}\right)}x$$

Cas 1a1=1b1

Aquest cas, i els dos següents, representen una única classe d'isomorfisme de corbes. Podem prendre com a model:

$$y^2 = x(x^2-1)(x-2)(x-1/2)$$

Cas 1b2

Anàlogament:

$$y^2 = x(x^2-1)(x^2+1)$$

Cas 2:

Anàlogament:

$$y^2 = x^5 - 1$$

10.8 Invariants a partir de matrius

En aquesta secció donem resposta al següent problema: Donada una matriu de períodes d'una superfície abeliana, que suposem principalment polaritzada i simple, trobar els invariants d'una corba de gènere 2 tal que la seva jacobiana és isomorfa sobre $\mathbb{C}$ a la superfície abeliana donada.

Sigui $T \in \mathbb{H}_2$; la funció θ de T amb característiques $a, b \in (\frac{1}{2}\mathbb{Z})^2$ es defineix com:

$$\theta[a,b](z,T) = \sum_{n\in\mathbb{Z}^2} \exp\left(\pi i(n+a)^t T(n+a) + 2\pi i(n+a)^t(z+b)\right).$$

Definim els "thetanullwerte" com:

$$\theta\begin{bmatrix} m & n \\ p & q \end{bmatrix} = \theta[(m,n),(p,q)](0,T)$$

i considerem els següents valors:

$$v[0] = \theta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad v[1] = \theta \begin{bmatrix} 1/2 & 0 \\ 0 & 0 \end{bmatrix}$$

$$v[3] = \theta \begin{bmatrix} 0 & 1/2 \\ 1/2 & 0 \end{bmatrix} \qquad v[5] = \theta \begin{bmatrix} 0 & 0 \\ 1/2 & 0 \end{bmatrix}$$

$$v[21] = \theta \begin{bmatrix} 0 & 0 \\ 1/2 & 0 \end{bmatrix} \qquad v[23] = \theta \begin{bmatrix} 1/2 & 1/2 \\ 0 & 0 \end{bmatrix}$$

$$v[25] = \theta \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} \qquad v[41] = \theta \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$v[43] = \theta \begin{bmatrix} 0 & 0 \\ 0 & 1/2 \end{bmatrix} \qquad v[45] = \theta \begin{bmatrix} 0 & 1/2 \\ 0 & 0 \end{bmatrix}$$

Amb aquests, definim unes expressions:

$$\begin{aligned} h[4] &= v[0]^8 + v[1]^8 + v[3]^8 + v[5]^8 + \\ &\qquad v[21]^8 + v[23]^8 + v[25]^8 + v[41]^8 + v[43]^8 + v[45]^8 \\ h[10] &= (v[0]\ v[1]\ v[3]\ v[5]\ v[21]\ v[23] v[25]\ v[41]\ v[43]\ v[45])^2 \\ h[12] &= v[0]^4\ v[1]^4\ v[3]^4\ v[5]^4\ v[21]^4\ v[41]^4 + \ldots \text{ 14 sumands més} \\ h[16] &= v[0]^4\ v[1]^4\ v[3]^4\ v[5]^4\ v[21]^4\ v[23]^8\ v[41]^4 + \ldots \text{ 59 sumands més.} \end{aligned}$$

Finalment,

$$\begin{aligned} i_1 &= \frac{h[12]^5}{h[10]^6} \\ i_2 &= \frac{h[12]^3 h[4]}{h[10]^4} \\ i_3 &= \frac{h[12]^2 h[16]}{h[10]^4} \end{aligned}$$

són els invariant absoluts d'Igusa d'una corba de gènere 2 amb jacobiana isomorfa a la varietat abeliana donada per la matriu de períodes T.

10.9 Endomorfismes de jacobianes de corbes hiperel·líptiques

10.9.1 Correspondències i endomorfismes

En aquesta secció donem una introducció a les correspondències en corbes i com es lliguen amb els endomorfismes de la jacobiana.

Sigui C una corba (llisa, projectiva,...). Una correspondència $\mathcal{C} : C \dashrightarrow C$ és, equivalentment:

i) Un divisor de Weil a la superfície producte $C \times C$.

ii) Una suma formal de diagrames:

$$\begin{array}{ccc} & \Gamma & \\ \swarrow & & \searrow \\ C & & C \end{array}$$

on Γ és una corba i els morfismes són aplicacions racionals entre corbes.

iii) Una aplicació $C \to \operatorname{Div}^k C$, que estenem per linealitat a divisors de la corba.

Una correspondència és principal si és de la forma:

- $D \times C$ o $C \times D$ amb $D \in \operatorname{Div} C$ o
- (φ) amb $\varphi \in \overline{K}(C \times C)$.

La classe de correspondències mòdul principals, $\operatorname{Corr}(C)$, admet estructura d'anell amb la suma formal i la composició (definida, per exemple, via l'aplicació $\operatorname{Div}(C) \to \operatorname{Div}(C)$).

Tenim un isomorfisme d'anells entre les correspondències d'una corba i els endomorfismes de la seva jacobiana:

$$\begin{aligned} \operatorname{Corr} C &\xrightarrow{\sim} \operatorname{End}(J(C)) \\ \mathcal{C} &\mapsto ([D] \mapsto [\mathcal{C}(D)]), \end{aligned}$$

on la suma formal de correspondències correspon a suma d'endomorfismes i la composició de correspondències a composició d'endomorfismes.

10.9.2 Correspondències en corbes hiperel·líptiques

Sigui C una corba de hiperel·líptica amb model $y^2 = f(x)$ i $\mathcal{C}$ una correspondència:

$$\mathcal{C} : C \dashrightarrow C.$$

Prenem com a model de $C \times C$ el donat pels elements (x_1, y_1, x_2, y_2) amb $y_i^2 = f(x_i)$. Aleshores,

Proposició 10.9.1. *Una equació de la correspondència $\mathcal{C}$ ve donada per un parell d'equacions:*

$$\begin{aligned} F(x_1, x_2) &= 0 \\ H(y_1 y_2, x_1, x_2) &= 0 \end{aligned}$$

amb $\deg_{y_1 y_2} H \in \{0, 1\}$.

Cal tenir en compte que:

- Si $\deg_{y_1 y_2} H = 0$, la component és principal, donat que podem reduir-la a una única equació.
- Si $\deg_{y_1 y_2} H = 1$, podem escriure H com

$$y_1 y_2 - G(x_1, x_2) = 0,$$

i necessàriament es compleix:

$$G(x_1, x_2)^2 \equiv f(x_1) f(x_2) \pmod{F(x_1, x_2)}$$

Observació 10.9.2. *Per tal de trobar les components irreductibles d'una correspondència, cal fer:*

1. *Factoritzar el polinomi F com:*

$$F(x_1, x_2) = F_1(x_1, x_2) \cdots F_k(x_1, x_2),$$

2. *buscar una factorització de H corresponent a la de F,*

$$H \equiv H_1 \cdots H_k H' \pmod{y_1^2 - f(x_1),\ y_2^2 - f(x_2),\ F(x_1, x_2)},$$

és a dir:

- *O bé* $H_i = y_1y_2 - G_i$, *complint l'equació de compatibilitat:*
$$G_i^2 \equiv f(x_1)f(x_2) \pmod{F_i(x_1,x_2)}$$
i tenim una component no trivial:
$$\begin{cases} F_i(x_1,x_2) = 0 \\ H_i(y_1y_2,x_1,x_2) = y_1y_3 - G_i(x_1,x_2) = 0 \end{cases}$$
- *O bé* $F_i|H_i$ *i la component serà principal (trivial).*

10.9.3 Exemples

Per tal d'il·lustrar la construcció general, donem exemples de correspondències donades per equacions.

- La correspondència identitat:
$$F(x_1,x_2) = x_1 - x_2$$
$$G(x_1,x_2) = f(x_1)$$
- La correspondència associada a $[2] \in \mathrm{End}(J(C))$:
$$F(x_1,x_2) = (x_1 - x_2)^2$$
$$G(x_1,x_2) = f(x_1)$$
- La correspondència associada a $[-1] \in \mathrm{End}(J(C))$:
$$F(x_1,x_2) = x_1 - x_2$$
$$G(x_1,x_2) = -f(x_1)$$
- La correspondència associada a $[n] \in \mathrm{End}(J(C))$:
$$F(x_1,x_2) = (x_1 - x_2)^{|n|}$$
$$G(x_1,x_2) = \mathrm{sgn}(n)f(x_1)$$
- La correspondència associada a un automorfisme de la corba:
$$(x,y) \mapsto \left(\frac{mx+n}{px+q}, \frac{(mq-np)y}{(px+q)^3}\right)$$
$$F(x_1,x_2) = x_2(px_1+q) - (mx_1+n)$$
$$G(x_1,x_2) = \frac{(mq-np)f(x_1)}{(px_1+q)^3}$$

Notem que, per a una corba hiperel·líptica genèrica, les úniques correspondències que té són les associades a la multiplicació per enters a la jacobiana.

10.9.4 Operacions amb correspondències

Un cop vista la representació de les correspondències en corbes hiperel·líptiques, ens cal un mètode per a operar-les.

Suposem donades dues correspondències:

$$\mathcal{C}_1 : \begin{cases} F_1(x_1, x_2) = 0 \\ H_1(y_1y_2, x_1, x_2) = y_1y_2 - G_1(x_1, x_2) = 0 \end{cases}$$

$$\mathcal{C}_2 : \begin{cases} F_2(x_2, x_3) = 0 \\ H_2(y_2y_3, x_2, x_3) = y_2y_3 - G_2(x_2, x_3) = 0 \end{cases}$$

Volem, en primer lloc, una representació de la correspondència suma; diguem $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. Aleshores, una representació de $\mathcal{C}$ ve donada per:

$$\mathcal{C} : \begin{cases} F(x_1, x_2) = F_1(x_1, x_2)F_2(x_1, x_2) \\ H(y_1y_2, x_1, x_2) = H_1(y_1y_2, x_1, x_2)H_2(y_1y_2, x_1, x_2) \\ \qquad \bmod (y_1y_2)^2 - f(x_1)f(x_2) \end{cases}$$

Per tal de trobar $\mathcal{C}$, una inversa (respecte la suma) de $\mathcal{C}_1$, podem fer:

$$\mathcal{C} : \begin{cases} F(x_1, x_2) = F_1(x_1, x_2) \\ H(y_1y_2, x_1, x_2) = H_1(-y_1y_2, x_1, x_2) \end{cases}$$

Pel que respecta a la composició de correspondències, diguem $\mathcal{C} = \mathcal{C}_2 \cdot \mathcal{C}_1$. Una representació de $\mathcal{C}$ ve donada per

$$\begin{cases} F_3(x_1, x_3) = \mathrm{Res}(F_1(x_1, x_2), F_2(x_2, x_3), x_2) \\ H_3(y_1y_3, x_1, x_3) = \mathrm{Res}(y_1y_3f(x_2) - G_1(x_1, x_2)G_2(x_2, x_3), F(x_1, x_2), x_2) \\ \qquad \bmod (y_1y_3)^2 - f(x_1)f(x_3) \end{cases}$$

Nota: Una sessió feta amb Mathematica va il·lustrar el procediment explicat per al cas d'una corba de gènere 2 amb jacobiana amb multiplicació complexa pel cos de descomposició del polinomi $x^4 + 4x^2 + 2$.

Capítol 11

Teoria de cossos de classes efectiva (exemples CM)

J. Guàrdia[1]
Dept. d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona

Introducció

En aquesta exposició intentarem analitzar fins a quin punt són efectius els teoremes que lliguen la teoria de cossos de classes amb les varietats abelianes amb multiplicació complexa. Anirem veient, mitjançant exemples, quines coses es poden fer i quines no, on són les dificultats i fins a quin punt podem esperar que s'arribaran a superar algun dia.

11.1 Un exemple en dimensió 1

Considerem el cos $K = \mathbb{Q}(\sqrt{-10})$, que té nombre de classes $h(-40) = 2$. Les dues formes quadràtiques reduïdes de discriminant -40 són $(7, -4, 2)$ i $(1, 0, 10)$ que donen lloc als dos nombres quadràtics $\tau_1 = \sqrt{-10}$ i

[1]Amb el suport parcial de la DGES: PB 96–0166.

$\tau_2 = \frac{2+\sqrt{-10}}{7}$. El valor de la funció j en aquests dos nombres és:

$$j_1 = j(\tau_1) = 8640(24635 + 11016\sqrt{5})$$
$$j_2 = j(\tau_2) = 8640(24635 - 11016\sqrt{5}).$$

El polinomi irreductible sobre $\mathbb{Q}$ d'aquests nombres és

$$H_{-10}(X) = X^2 - 425692800X + 9103145472000.$$

La teoria de les corbes el·líptiques amb multiplicació complexa ens diu que el cos de Hilbert de K és el cos $K(j_1) = K(j_2) = K(\sqrt{5})$. Com és que, essent el resultat final tan *petit*, els nombres j_i i el polinomi $H_{-10}(X)$ són tan *grans*?

Una raó heurística és la següent: la teoria ens diu que el polinomi $H_{10}(X)$ és un dels factors irreductibles dels polinomis modulars $\Phi_{10}(X,X)$ i $\Phi_{11}(X,X)$ (entre d'altres). Cadascun d'aquests polinomis ocupa vàries planes (cf. [Ba 92]). El polinomi $\Phi_{10}(X,X)$ un cop factoritzat és

$$\begin{aligned}\Phi_{10}(X,X) = \; & (-1728 + X)^2 \left(9103145472000 - 425692800\,X + X^2\right) \\ & \left(-1790957481984 - 153542016\,X + X^2\right)^2 \\ & \left(14670139392 - 4834944\,X + X^2\right)^2 \\ & \left(-121287375 + 191025\,X + X^2\right)^2 \\ & \left(1566028350940383 - 58682638134\,X + 39491307\,X^2 + X^3\right)^2 \\ & (20919104368024767633 + 109873509788637459\,X - \\ & 429878960946\,X^2 + 331531596\,X^3 + X^4)^2\end{aligned}$$

Weber proposa una manera alternativa de construir el cos de Hilbert dels cossos quadràtics, que dona resultats molt millors. Sigui

$$\eta(\tau) := q^{1/24}\theta_{00}(\tau)^{1/3}\theta_{01}(\tau)^{1/3}\theta_{10}(\tau)^{1/3}$$

la funció η de Dedekind. Considerem les anomenades *funcions de Weber*:

$$\mathfrak{f}(\tau) := \zeta_{48}^{-1}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} \qquad \mathfrak{f}_1(\tau) := \frac{\eta(\tau/2)}{\eta(\tau)}.$$

Teorema 11.1.1 ([We 08]). *Sigui m un enter no divisible per 3. El* ring class field *de $\mathbb{Z}[\sqrt{-m}]$ és $\mathbb{Q}(\sqrt{-m},\beta)$, on*

$$\begin{aligned}
\beta &= \mathfrak{f}(\sqrt{-m})^2 && si \quad m \equiv 3 \pmod 4,\\
\beta &= \mathfrak{f}(\sqrt{-m})^4 && si \quad m \equiv 5 \pmod 8,\\
\beta &= \sqrt{2}\mathfrak{f}(\sqrt{-m})^2 && si \quad m \equiv 1 \pmod 8,\\
\beta &= \sqrt{2}\mathfrak{f}(\sqrt{-m}) && si \quad m \equiv 7 \pmod 8,\\
\beta &= \mathfrak{f}(\sqrt{-m}) && si \quad m \equiv 3 \pmod 8,\\
\beta &= \sqrt{2}\mathfrak{f}_1(\sqrt{-m})^2 && si \quad m \equiv 2 \pmod 8,\\
\beta &= \sqrt{2}\mathfrak{f}(\sqrt{-m})^4 && si \quad m \equiv 4 \pmod 8.
\end{aligned}$$

Si apliquem aquest teorema al nostre cas concret, obtenim que el Hilbert *class field* de $K = \mathbb{Q}(\sqrt{-10})$ és $K(\beta)$, on $\beta = 1+\sqrt{5}$. Com veiem la millora és espectacular.

11.2 Varietats abelianes ciclotòmiques: construcció geomètrica

Entendrem per varietat abeliana ciclotòmica una varietat abeliana amb multiplicació complexa per un cos de nombres ciclotòmic. Sabem com construir les varietats ciclotòmiques *de manera algebraica*, i en la secció propera en parlarem. Però ara veurem una construcció *geomètrica* de les varietats ciclotòmiques.

Sigui C una corba no singular definida sobre un cos de nombres K amb un automorfisme σ d'ordre $n > 2$. Aquest automorfisme indueix un automorfisme $\tilde{\sigma}$ de la jacobiana $J(C)$ de la corba, i dóna lloc a una inclusió $\mathbb{Q}(\zeta_n) \subseteq \mathrm{End}_0(J(C))$, on ζ_n és una arrel n-èsima primitiva de la unitat.

Si tenim sort i $g(C) = \dim J(C)$ coincideix amb $\varphi(n)/2 = [Q(\zeta_n) : Q]/2$, tindrem que $J(C)$ és una varietat abeliana ciclotòmica. Aquest és el cas, per exemple, de la corba de Klein, que té gènere 3 i un automorfisme d'ordre 7.

Si $\dim J(C) > \varphi(n)/2$ no podem dir gran cosa de $J(C)$, però podem provar d'analitzar la corba quocient $C/\langle\sigma\rangle$: en alguns casos la seva jacobiana sí que serà una varietat abeliana ciclotòmica. És el cas que es dóna en les

corbes de Fermat. Com que aquest és un cas molt estudiat, li dedicarem unes ratlles.

Fixem un nombre primer $p \in \mathbb{Z}$ i una arrel p-èsima primitiva de la unitat ζ. La corba de Fermat d'exponent p és la corba F_p donada per l'equació:

$$X^p + Y^p = 1.$$

Entre els molts automorfismes que tenen aquestes corbes sempre hi ha els següents:

$$\sigma_k(x,y) := (\zeta^{p-k}x, \zeta y), \qquad 1 \leq k \leq p-2.$$

Els automorfismes σ_k tenen ordre p. Les corresponents corbes quocients són:

$$C_{p,k} := F_p/\langle \sigma_k \rangle : V^p = U(1-U)^k.$$

Les corbes $C_{p,k}$ tenen totes gènere $g(C_{p,k}) = \frac{p-1}{2}$, i un automorfisme $\overline{\zeta}$ d'ordre p, donat per

$$\overline{\zeta}(u,v) = (u, \zeta v).$$

Ens trobem en la situació descrita anteriorment: l'automorfisme $\overline{\zeta}$ indueix un automorfisme $\tilde{\zeta}$ de $J(C_{p,k})$, que dóna lloc a una inclusió $\mathbb{Q}(\zeta) \subseteq \mathrm{End}_0 J(C_{p,k})$. Com que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1 = 2\dim J(C_{p,k})$, tenim que $J(C_{p,k})$ té multiplicació complexa per $\mathbb{Q}(\zeta)$, és a dir, és una varietat abeliana ciclotòmica. Podrem descriure el seu CM-tipus analitzant l'acció de l'automorfisme $\overline{\zeta}$ sobre les formes diferencials de $C_{p,k}$.

És un fet ben conegut (cf. [La 82]) que l'espai de les formes diferencials de primera espècie sobre la corba de Fermat, $H^0(F_p, \Omega^1)$ està generat per les formes $\omega_{r,s} = X^{r-1}Y^{s-1}\frac{dX}{Y^{p-1}}$, amb $1 \leq r, s$, $r+s < p$. D'aquestes en podem deduir una base de $H^0(C_{p,k}, \Omega^1)$: sigui

$$S_k := \{m \in (\mathbb{Z}/p\mathbb{Z})^* | \langle m \rangle + \langle mk \rangle < p\},$$

on $\langle \cdot \rangle$ denota el residu mòdul p. És té que:

$$H^0(C_{p,k}, \Omega^1) = \langle \omega_{\langle m \rangle, \langle mk \rangle} \rangle_{m \in S_k}.$$

L'acció de l'automorfisme $\overline{\zeta}$ sobre l'espai $H^0(C_{p,k}, \Omega^1)$ és diagonal:

$$\overline{\zeta}^*(\omega_{\langle m \rangle, \langle mk \rangle}) = \zeta^m \omega_{\langle m \rangle, \langle mk \rangle}.$$

Si identifiquem $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ amb $(\mathbb{Z}/p\mathbb{Z})^*$ de la manera usual (cf. la secció següent), veiem que el CM-tipus de la varietat abeliana $J(C_{p,k})$ és

$$\{t \in (\mathbb{Z}/p\mathbb{Z})^* | t + \langle tk \rangle \leq p-1\}.$$

Koblitz i Rohrlich ([Ko 78]), estudiant directament les xarxes de períodes de les corbes de Fermat i les subxarxes corresponents a les corbes $C_{p,k}$, estableixen els criteris següents per determinar quan les $J(C_{p,k})$ són isògines entre elles i quan són simples:

Proposició 11.2.1 (Koblitz-Rohrlich). *Si $p > 3$ aleshores:*

1) $J(C_{p,k}) \sim J(C_{p,k'}) \iff \exists\, m \in (\mathbb{Z}/p\mathbb{Z})^*$ *tal que* $\{1, k, p-1-k\} = \{\langle m\rangle, \langle mk'\rangle, \langle -m(k'+1)\rangle\}$.

2) Si $p \equiv 2 \pmod 3$ *totes les* $J(C_{p,k})$ *són absolutament simples.*

3) Si $p \equiv 1 \pmod 3$ *les* $J(C_{p,k})$ *són totes absolutament simples, llevat de* $J(C_{p,w})$ *i* $J(C_{p,w'})$*, on* w, w' *són les dues arrels de* $X^2 + X + 1$ *en* $\mathbb{Z}/p\mathbb{Z}$.

Exercici: Proveu la proposició anterior a partir dels resultats explicats en [Gu 00].

Exemples:

La corba de Fermat F_5 té gènere 6. Les corbes quocients $C_{5,1}, C_{5,2}$ i $C_{5,3}$ són totes tres hiperel·líptiques de gènere 2. Les corbes $C_{5,1}$ i $C_{5,3}$ són isomorfes, o sigui que les seves jacobianes són varietats abelianes polaritzades isomorfes. El criteri de Koblitz-Rohrlich ens diu que les tres jacobianes són absolutament simple, i que $J(C_{5,1}) \sim J(C_{5,2})$. Observem que el CM-tipus d'aquestes dues varietats abelianes isògines és diferent!

$p=5$		
k	$C_{5,k}$	CM-tipus
1	$V^5 = U(1-U)$	$(1,2)$
2	$V^5 = U(1-U)^2$	$(1,3)$
3	$V^5 = U(1-U)^3$	$(1,2)$
$C_{5,1} \simeq C_{5,3} \Rightarrow J(C_{5,1}) \simeq J(C_{5,3})$		
$J(C_{5,1}) \simeq J(C_{5,3}) \sim J(C_{5,2})$		

La corba de Fermat F_7 té gènere 15. Les corbes quocients $C_{7,k}, C_{5,2}$ i $C_{5,3}$ tenen gènere 3. Les corbes $C_{7,1}$ i $C_{7,5}$ són isomorfes, o sigui que les seves jacobianes són varietats abelianes polaritzades isomorfes. Passa el mateix amb les corbes $C_{7,2}$ i $C_{7,4}$, però en aquest cas les jacobianes no són simples. Tenim a més que $J(C_{7,1}) \sim J(C_{7,3})$. De nou ens trobem amb dues varietats abelianes isògines que tenen CM-tipus diferent.

$p=7$			
k	$C_{7,k}$	CM-tipus	Observacions
1	$V^7 = U(1-U)$	$(1,2,3)$	Hiperel·líptica
2	$V^7 = U(1-U)^2$	$(1,2,4)$	$J(C_{7,2}) \sim E^3$
3	$V^7 = U(1-U)^3$	$(1,5,3)$	Hiperel·líptica
4	$V^7 = U(1-U)^4$	$(1,2,4)$	$J(C_{7,4}) \sim E^3$
5	$V^7 = U(1-U)^5$	$(1,2,3)$	Hiperel·líptica
$C_{7,1} \simeq C_{7,5} \Rightarrow J(C_{7,1}) \simeq J(C_{7,5})$			
$C_{7,2} \simeq C_{7,4} \Rightarrow J(C_{7,2}) \simeq J(C_{7,4})$			
$J(C_{7,1}) \simeq J(C_{7,5}) \sim J(C_{7,3})$			

La corba de Fermat F_{11} té gènere 45. Les corbes quocient $C_{11,k}$ tenen gènere 5. Tenim isomorfismes $C_{11,1} \simeq C_{11,9}$, $C_{11,2} \simeq C_{11,8}$, $C_{11,3} \simeq C_{11,7}$ i $C_{11,4} \simeq C_{11,6}$, que donen lloc a isomorfismes entre les jacobianes corresponents. Les corbes $C_{11,1}, C_{11,5}$ i $C_{11,9}$ són hiperel·líptiques. Totes les jacobianes són absolutament simples.

$p = 11$		
k	$C_{11,k}$	CM-tipus
1	$V^{11} = U(1-U)$	$(1,2,3,4,5)$
2	$V^{11} = U(1-U)^2$	$(1,2,3,7,6)$
3	$V^{11} = U(1-U)^3$	$(1,2,8,4,5)$
4	$V^{11} = U(1-U)^4$	$(1,2,3,4,6)$
5	$V^{11} = U(1-U)^5$	$(1,9,3,7,5)$
6	$V^{11} = U(1-U)^6$	$(1,2,3,4,6)$
7	$V^{11} = U(1-U)^7$	$(1,2,8,4,5)$
8	$V^{11} = U(1-U)^8$	$(1,2,3,7,6)$
9	$V^{11} = U(1-U)^9$	$(1,2,3,4,5)$
$C_{11,1} \simeq C_{11,9} \Rightarrow J(C_{11,1}) \simeq J(C_{11,9})$		
$C_{11,2} \simeq C_{11,8} \Rightarrow J(C_{11,2}) \simeq J(C_{11,8})$		
$C_{11,3} \simeq C_{11,7} \Rightarrow J(C_{11,3}) \simeq J(C_{11,7})$		
$C_{11,4} \simeq C_{11,6} \Rightarrow J(C_{11,4}) \simeq J(C_{11,6})$		
$J(C_{11,1}) \simeq J(C_{11,9}) \sim J(C_{11,5})$		
$J(C_{11,2}) \simeq J(C_{11,8}) \sim J(C_{11,3}) \simeq J(C_{11,7}) \sim J(C_{11,4}) \simeq J(C_{11,6})$		

11.3 Varietats abelianes ciclotòmiques: construcció algebraica

En la secció anterior hem construït de manera geomètrica alguns exemples de varietats abelianes ciclotòmiques. Ara veurem el procés general per construir totes les varietats abelianes ciclotòmiques.

En primer lloc, determinarem tots els CM-tipus ciclotòmics. Tot seguit trobarem una polarització per a cada CM-tipus. Amb el CM-tipus i la polarització donats, aprendrem a calcular una matriu de períodes normalitzada d'una varietat abeliana ciclotòmica. Finalment, analitzarem què podem dir del cos de moduli d'aquesta varietat.

11.3.1 CM-tipus ciclotòmics

Fixem un nombre primer senar p, i una arrel primitiva p-èsima de la unitat, $\zeta = e^{2\pi i/p}$. El cos ciclotòmic $K = \mathbb{Q}(\zeta)$ és un CM-cos. El subcòs $K_0 = \mathbb{Q}(\zeta + z^{-1})$ és la subextensió maximal totalment real, i l'extensió K/K_0 és quadràtica totalment imaginària. Identificarem el grup de Galois de $K/\mathbb{Q}$ amb $(\mathbb{Z}/p\mathbb{Z})^*$ de la manera usual:

$$\begin{array}{rcl} \mathrm{Gal}(K/\mathbb{Q}) & \longleftrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ \varphi_k(\zeta) = \zeta^k & \longleftrightarrow & k. \end{array}$$

Com que $\overline{\varphi}_k = \varphi_{p-k}$, donar un CM-tipus de K equival a escollir un element de cada parella $\{k, p-k\}$. Així doncs, podem identificar els conjunts:

$$\{\text{CM-tipus de} K\} = (\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}).$$

Amb això veiem de manera immediata que hi ha $2^{(p-3)/2}$ CM-tipus normalitzats (és a dir, CM-tipus que contenen la identitat), i tenim un mètode evident per enumerar-los. En les taules següents presentem els CM-tipus que existeixen per a $p = 5, 7$ i 11. Senyalem amb un asterisc els CM-tipus no simples. Al costat de cada CM-tipus indiquem una corba $C_{p,k}$ la jacobiana de la qual el té com a CM-tipus. Com es veu immediatament, no tots

els CM-tipus s'obtenen d'aquesta forma.

$p=5$	
$(1,2)$	$C_{5,1}$
$(1,3)$	$C_{5,3}$

$p=7$	
$(1,2,3)$	$C_{7,1}$
$(1,2,4)*$	$C_{7,4}$
$(1,5,3)$	$C_{7,3}$
$(1,5,4)$	??

$p=11$	
$(1,2,3,4,5)$	$C_{11,1}$
$(1,2,3,4,6)$	$C_{11,4}$
$(1,2,3,7,5)$	??
$(1,2,3,7,6)$	$C_{11,2}$
$(1,2,8,4,5)$	$C_{11,3}$
$(1,2,8,4,6)$	??
$(1,2,8,7,5)$	??
$(1,2,8,7,6)$	??
$(1,9,3,4,5)$	??
$(1,9,3,4,6)$	??
$(1,9,3,7,5)$	$C_{11,5}$
$(1,9,3,7,6)$	??
$(1,9,8,4,5)$	??
$(1,9,8,4,6)$	??
$(1,9,8,7,5)$	??
$(1,9,8,7,6)$	??

11.3.2 Polaritzacions

Fixem un CM-tipus ciclotòmic normalitzat $T = (1, \pm 2, \ldots, \pm(p-1)/2)$. Siguin $\varphi_T = (\varphi_1, \ldots, \varphi_{(p-1)/2})$ els K-automorfismes associats. Volem determinar les polaritzacions de les varietats abelianes ciclotòmiques que tinguin T per CM-tipus. Com s'explica en [Fe 00], això equival a trobar elements $\xi_T \in K$ tals que

- $K = K_0(\xi_T)$,
- $\xi_T^2 \in K_0$ ($\Rightarrow -\xi^2$ totalment positiu),
- $\mathrm{im}(\varphi_k(\xi_T)) > 0, k = 1, \ldots, (p-1)/2$.

Podem establir una *estratègia* per calcular aquests elements ξ_T basant-nos en els tres punts següents:

a) Per al tipus "trivial" $T_0 = (1, 2, \ldots, (p-1)/2)$ podem prendre sempre $\xi := \xi_{T_0} := \zeta - \zeta^{-1}$.

b) Per a la resta de tipus podrem trobar un ξ_T de la forma $\xi_T = \alpha_T \xi$, amb $\xi \in \mathcal{O}_K$.

c) Donats $T = (1, \varepsilon_2 2, \ldots, \varepsilon_{\frac{p-1}{2}} \dfrac{p-1}{2})$, $T' = (1, \varepsilon_2' 2, \ldots, \varepsilon'_{\frac{p-1}{2}} \dfrac{p-1}{2})$, sigui $T'' = (1, \varepsilon_2 \varepsilon_2' 2, \ldots, \varepsilon_{(p-1)/2} \varepsilon'_{\frac{p-1}{2}} \dfrac{p-1}{2})$. Podem escollir $\alpha_{T''} = \alpha_T \alpha_{T'}$.

Per als casos $p = 5, 7$ i 11 obtenim els resultats següents:

$p = 5 \quad \xi = \zeta - \zeta^4$		
T	α_T	ξ_T
$(1,2)$	1	$\zeta - \zeta^4$
$(1,3)$	$\zeta + \zeta^4$	$\zeta^2 - \zeta^3$

$p = 7 \quad \xi = \zeta - \zeta^6$		
T	α_T	ξ_T
$(1,2,3)$	1	$\zeta - \zeta^6$
$(1,2,-3)$	$-(\zeta^2 + \zeta^5)$	$\zeta - \zeta^6 + \zeta^4 - \zeta^3$
$(1,-2,3)$	$-(\zeta^3 + \zeta^4)$	$\zeta^3 - \zeta^4 + \zeta^2 - \zeta^5$
$(1,-2,-3)$	$\zeta + \zeta^6$	$\zeta^2 - \zeta^5$

$p=11 \quad \xi=\zeta_{11}-\zeta_{11}^{10}$	
T	α_T
$(1,2,3,4,5)$	1
$(1,2,-3,-4,-5)$	$\zeta_{11}+\zeta_{11}^{10}$
$(1,-2,-3,-4,5)$	$\zeta_{11}^{2}+\zeta_{11}^{9}$
$(1,2,-3,-4,5)$	$-(\zeta_{11}^{3}+\zeta_{11}^{8})$
$(1,2,-3,4,5)$	$-(\zeta_{11}^{4}+\zeta_{11}^{7})$
$(1,-2,3,-4,5)$	$-(\zeta_{11}^{5}+\zeta_{11}^{6})$
...	...

11.3.3 Construcció dels tors complexos

Un cop tenim fixat un CM-tipus T i una polarització ξ_T, ja podem construir totes les varietats abelianes principals de tipus (K,T,ξ_T). Seran les varietats provinents dels tors complexos $C^{(p-1)/2}/\varphi_T(\mathfrak{m})$, on $\mathfrak{m}$ recorre les classes d'ideals de $\mathcal{O}_K$. Utilitzarem la forma de Riemann E_{ξ_T} donada per ξ_T per calcular una matriu de períodes normalitzada d'aquest tor.

Desenvoluparem tots els càlculs per al cas concret $p=5$, $T_0=(1,2)$ i $\xi_{T_0}=\xi=\zeta-\zeta^4$. Com el nombre de classes de K val 1, només ens cal considerar l'ideal $\mathfrak{m}=\mathcal{O}_K=\mathbb{Z}\langle 1,\zeta,\zeta^2,\zeta^3,\zeta^4\rangle$. La xarxa de períodes $W=\varphi_T(\mathfrak{m})$ és

$$W=\mathbb{Z}\langle w_1,w_2,w_3,w_4\rangle=\begin{pmatrix} 1 & \zeta & \zeta^2 & \zeta^3 \\ 1 & \zeta^2 & \zeta^4 & \zeta^2 \end{pmatrix}.$$

La forma de Riemann E_ξ es calcula amb la fórmula:

$$E_\xi(\varphi_T(\alpha),\varphi_T(\beta))=\mathrm{Tr}_{K/\mathbb{Q}}(\xi\alpha\beta).$$

Amb això trobem que:

$$(E(w_j, w_k))_{k,j} = \begin{pmatrix} 0 & -5 & 0 & 0 \\ 5 & 0 & -5 & 0 \\ 0 & 5 & 0 & -5 \\ 0 & 0 & 5 & 0 \end{pmatrix}.$$

A partir de les dades anteriors, busquem una base simplèctica de $\varphi(\mathfrak{m})$ respecte de E_ξ. Això es fa amb el procés d'ortogonalització de Gram-Schmidt. Obtenim que

$$u_1 = w_1,\ u_2 = w_1 + w_3,\ u_3 = w_2,\ u_4 = w_4$$

és una base simplèctica. (Notem que la polarització E_ξ no és principal, sinó que té grau 5^2. Si volem una polarització principal, podem utilitzar $\frac{1}{5}E_\xi = E_{\frac{\zeta}{5}}$). La matriu formada per aquests períodes és:

$$\Omega = (\Omega_1|\Omega_2) = \begin{pmatrix} 1 & 1+\zeta^2 & \zeta & \zeta^3 \\ & & & \\ 1 & 1+\zeta^4 & \zeta^2 & \zeta \end{pmatrix}.$$

A partir d'aquesta obtenim una matriu de períodes normalitzada per al tor complex $\mathbb{C}^2/\varphi(\mathfrak{m})$:

$$Z_{5,0} = \Omega_1^{-1}\Omega_2 = \begin{pmatrix} \zeta^2 - \zeta^3 & -1-\zeta^2 \\ & \\ -1-\zeta^2 & -\zeta^4 \end{pmatrix}.$$

En la taula següent donem les matrius de períodes de les varietats abelianes

ciclotòmiques principals per a $p = 5$:

$p = 5$	
$T_1 = (1,2)$	$Z_{5,1} = \begin{pmatrix} \zeta^2 - \zeta^3 & -1 - \zeta^2 \\ -1 - \zeta^2 & -\zeta^4 \end{pmatrix}$
$T_2 = (1,3)$	$Z_{5,2} = \begin{pmatrix} -\zeta^4 & -\zeta - \zeta^3 \\ -\zeta - \zeta^3 & \zeta \end{pmatrix}$

11.3.4 Determinació del cos de moduli

La projectivitat d'un tor complex $C^g/(I|Z)$ garanteix la convergència de les funcions $\theta[c](z;Z)$. Justament amb aquestes funcions podem construir explícitament immersions projectives del tor: per a $d \in \mathrm{N}$ prou gran, l'aplicació

$$\begin{aligned} f_d : \mathbb{C}^n/(I|Z) &\longrightarrow \mathbf{P}^N \\ z &\longrightarrow (\theta[c](dz))_c, \end{aligned}$$

on c recorre els punts de d-torsió del tor i $N = d^{2g} - 1$, és una immersió tancada del tor en P^N. La imatge de f_d és una varietat abeliana algebraica A, determinada per certes equacions. Se sap que hom pot descriure aquesta varietat mitjançant equacions quadràtiques i cúbiques. Els coeficients que apareixen en aquestes equacions són fraccions polinòmiques dels *Thetanullwerte*, és a dir, dels valors $\theta[c](0)$.

Els quocients dels *Thetanullwerte* són exemples de formes modulars de Siegel. Quan el tor complex de partida té multiplicació complexa per un cos K, aquests quocients prenen valors algebraics, i permeten construir el cos de moduli de la varietat A. Aquest cos de moduli és un subcòs d'un *ring class field* de K. D'una manera anàloga, amb les coordenades de les imatges per f_d dels punts de torsió del tor podem construir *ray class fields* de K.

El programa exposat en els paràgrafs anteriors és tan bonic com teòric. Aconseguir dur a terme de manera efectiva aquest programa és una tasca dels matemàtics del segle XXI. Ara per ara, sabem desenvolupar el programa complet per a dimensió 1 i 2, i podem fer alguns passos en casos concrets de dimensió superior.

Com a exemple, repassem les construccions en dimensió 1. Donat un tor complex $\mathbb{C}/\langle 1,\tau\rangle$, les funcions θ clàssiques ens en donen una immersió projectiva:

$$\begin{array}{ccc} \mathbb{C}/\langle 1,\tau\rangle & \xrightarrow{f_2} & \mathbf{P}^3 \\ z & \longrightarrow & (\theta_{j,k}(2z,\tau))_{j,k=0,1}. \end{array}$$

Siguin $A=\theta_{0,0}(0,\tau)$, $B=\theta_{0,1}(0,\tau)$ i $C=\theta_{1,0}(0,\tau)$ els *Thetanullwerte*. La imatge de f_2 és la intersecció de les dues quàdriques:

$$\left\{ \begin{array}{l} A^2X_0^2 = B^2X_1^2 + C^2X_2^2, \\ \\ A^2X_3^2 = C^2X_1^2 - B^2X_2^2. \end{array} \right\}$$

Naturalment, aquesta imatge és una corba el·líptica, que té invariant

$$j(\tau) = 256\frac{A^8 - B^4C^4}{A^8B^8C^8}.$$

Per a corbes de gènere 2 la situació és força més complicada, però encara se'n té control, gràcies als treballs de Rosenhain, Igusa i Mestre, que el lector pot trobar explicats en l'exposició anterior ([Ca 00]). Un punt clau que permet resoldre aquest cas és el fet que totes les varietats abelianes irreductibles de dimensió 2 són jacobianes de corbes. Això permet que donada una matriu satisfent les condicions de Riemann, siguem capaços de calcular una corba de gènere 2 que la tingui com a matriu de períodes. Si fem aquests càlculs per a la matriu $Z_{5,1}$ que hem trobat en l'apartat anterior, obtenim que la jacobiana de la corba

$$C : Y^2 = X^5 - 1$$

és justament $J(C) = \mathbb{C}^2/Z_{5,1}$.

Per a les varietats ciclotòmiques, podem intentar donar raonaments ad-hoc en alguns casos. Per exemple, com que el nombre de classes del cos

ciclotòmic d'exponent 5 és 1, per a cada CM-tipus tindrem una sola classe d'isomorfisme de varietats abelianes amb aquell CM-tipus. D'aquí podem concloure que la jacobiana de la corba $C_{5,2}$ ha de ser isomorfa al tor complex $\mathbb{C}^2/(I|Z_{5,2})$.

Podem traslladar el raonament anterior a les varietats ciclotòmiques principals que s'obtenen per a $p = 7$. En la taula següent identifiquem la majoria d'aquestes varietats com a jacobianes de corbes $C_{7,k}$:

$p = 7$	
$T_1 = (1,2,3)$	$J(C_{7,1})$
$T_2 = (1,2,4)*$	$J(C_{7,2})$
$T_3 = (1,5,3)$	$J(C_{7,3})$
$T_4 = (1,5,4)$	?

Com veiem, no tenim identificada la varietat ciclotòmica que correspon al CM-tipus T_4. Una matriu de períodes d'aquesta varietat ha de ser

$$Z_{7,4} = \begin{pmatrix} -\zeta_7^5 & -(\zeta_7^5+\zeta_7^4+\zeta_7^2+1) & \zeta_7^5+\zeta_7^3+\zeta_7+1 \\ -(\zeta_7^5+\zeta_7^4+\zeta_7^2+1) & (\zeta_7^2+1)(\zeta_7^3-\zeta_7^2+\zeta_7+1) & \zeta_7^5+\zeta_7^3+\zeta_7^2+2 \\ \zeta_7^5+\zeta_7^3+\zeta_7+1 & \zeta_7^5+\zeta_7^3+\zeta_7^2+2 & \zeta_7^2 \end{pmatrix}.$$

Atès que la dimensió de l'espai de moduli de varietats abelianes de dimensió 3 coincideix amb la dimensió de l'espai de moduli de corbes de gènere 3, té sentit plantejar els problemes següents:

Exercici: Determinar una corba $C_{/\mathbb{Q}(\zeta)}$ tal que la seva jacobiana $J(C)$ sigui isògina a $\mathbb{C}^2/(I|Z_4)$.

Exercici: (*Més fàcil*) Determinar UNA corba $C_{/\mathbb{Q}(\zeta)}$ tal que la seva jacobiana $J(C)$ sigui isògina a $\mathbb{C}^2/(I|Z_4)$.

Aquests problemes poden tenir més d'una solució: per al tipus $T_2 = (1,2,4)$, per exemple, tindríem $C_{7,2}$ i la corba de Klein, que no són isomorfes.

11.4 Corbes de gènere 2 amb CM definides sobre els racionals

En [VW 99] Van Wamelen formula l'afirmació següent:

Afirmació: *Hi ha 19 classes d'isomorfisme de corbes C de gènere 2 definides sobre el cos dels nombres racionals tals que la seva jacobiana $J(C)$ és simple i té multiplicació complexa per l'anell d'enters d'un cos quàrtic.*

La justificació d'aquesta afirmació consisteix en una cerca experimental d'aquestes corbes. Tot seguit farem un resum d'aquesta cerca i en comentarem els resultats.

Sigui K un cos quàrtic de tipus CM, i sigui L la seva clausura normal. Hi ha tres situacions possibles:

$$a)\ L = K,\ \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/4Z,$$

$$b)\ L = K,\ \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2Z \times \mathbb{Z}/2\mathbb{Z},$$

$$c)\ L \neq K,\ \mathrm{Gal}(K/\mathbb{Q}) = D_4.$$

En el cas *c)* no hi ha corbes $\mathbb{Q}$-definides amb CM per K (cf. [Sh 94], pàg. 132), de manera que es pot obviar. El cas *b)* correspon a varietats no simples, per la qual cosa no ens interessa. Així doncs, suposarem que estem en el cas *a)*.

La idea de van Wamelen per trobar corbes de gènere 2 amb les propietats desitjades és trobar prèviament les seves jacobianes, a partir de la seva caracterització com a varietats abelianes de tipus CM. Per a corbes de gènere 2, el teorema de Torelli és efectiu gràcies als treballs d'Igusa i Mestre: podem reconstruir la corba a partir dels períodes de la seva jacobiana (cf. [Ca 00]).

Resumim en el teorema següent els resultats que necessitarem de la teoria de varietats abelianes amb CM. Aquests resultats han anat apareixent en les exposicions anteriors d'aquest volum, però les incloem per a comoditat del lector.

Teorema 11.4.1. *Siguin K un cos de tipus CM de grau qualsevol i T un CM-tipus de K.*

1) Totes les varietats abelianes principals de tipus (K,T) són tors com-

plexos $C^n/\varphi_T(\mathfrak{a})$, polaritzats segons:

$$E(\varphi_T(\alpha), \varphi_T(\beta)) = \mathrm{Tr}(\xi\alpha\overline{\beta}),$$

on:

- $\mathfrak{a}$ *és un ideal fraccionari de* K,
- $K = K_0(\xi)$, $\xi^2 \in K_0$, $\mathrm{im}\,\varphi(\xi) > 0\ \forall\varphi \in T$,
- $\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\overline{\mathfrak{a}} = (\xi^{-1})$.

2) *Dues varietats abelianes principals i simples* $(\mathbb{C}^n/\varphi_T(\mathfrak{a}), \xi_1)$, $(\mathbb{C}^n/\varphi_T(\mathfrak{b}), \xi_2)$ *del mateix tipus són isomorfes si i només si hi ha un* $\gamma \in K$ *tal que* $\gamma\mathfrak{a} = \mathfrak{b}$ *i* $\xi_1 = \gamma\overline{\gamma}\xi_2$.

3) *Dues polaritzacions* ξ_1, ξ_2 *sobre* $\mathbb{C}^n/\varphi_T(\mathfrak{a})$ *donen lloc a varietats abelianes polaritzades isomorfes si i només si hi ha unitat* $u \in \mathcal{O}_K^*$ *tal que* $\xi_1 = u\overline{u}\xi_2$.

En base als resultats anteriors, van Wamelen formula l'algoritme següent per a calcular totes les varietats abelianes principalment polaritzades i principals (VAPPP) amb multiplicació complexa per un cos de tipus CM qualsevol.

Algoritme 11.4.2. (Càlcul de les VAPPP amb CM per K)
Pas 1: *Determinar totes les classes d'ideals* $[\mathfrak{a}]$ *tals que* $[\mathfrak{a}\overline{\mathfrak{a}}] = [\mathcal{D}_{K/\mathbb{Q}}^{-1}]$.

Pas 2: *Per a cadascuna d'aquestes classes, triar un representant* $\mathfrak{a}$ *i un generador* b *de l'ideal* $\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\overline{\mathfrak{a}}$.

Pas 3: *Triar un sistema de representants* $\{u^+\}$ *de* $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$.

Pas 4: *Per a cada parella* $(\mathfrak{a}, b)$ *del pas 2, comprovar si hi ha una* $u \in \mathcal{O}_K$ *tal que* $ub = -\overline{ub}$, *i calcular* $\xi_0 = (ub)^{-1}$.

Pas 5: *Per a cada tripleta* $(\mathfrak{a}, b, \xi_0)$ *i per a cada representant* u^+ *del pas 2, calcular* $\xi = u^+\xi_0$, *i determinar el tipus* T *tal que* $\mathrm{im}\,\varphi(\xi) > 0$ *per a cada* $\varphi \in T$.

Pas 6: *Per a cada parella* $(\mathfrak{a}, \xi)$ *calcular la matriu de períodes* $\tau \in \mathbb{H}_n$ *corresponent a* $(\mathbb{C}^n/\varphi_T(\mathfrak{a}), \xi)$.

Aquest algoritme té una *pega*: pot trobar varietats repetides, perquè és possible que varietats amb CM-tipus diferent siguin isomorfes, i no disposem d'una caracterització clara d'aquesta situació.

Ara el treball de Van Wamelen és essencialment calculístic: per a cada CM-cos quàrtic K fa la llista de varietats abelianes amb CM per $\mathcal{O}_K$. Per a

cada varietat que troba, calcula numèricament els invariants d'Igusa d'una corba de gènere 2 que la té per jacobiana. Amb aquestes aproximacions numèriques pot decidir si la corba està definida sobre els racionals. Si aquest és el cas, segueix el mètode de Mestre per trobar-ne l'equació.

El treball de Van Vamelen requereix d'una gran destresa en el càlcul. Els problemes més difícils que cal atacar són:

- Construir taules de cossos quàrtics.

  Aquesta feina la fan molt bé a Bordeus, i a més, posen els resultats a disposició de tothom (`ftp://megrez.math.u-bordeaux.fr`). Van Vamelen revisa tots els cossos quàrtics cíclics amb discriminant menor que 10^6. Entre aquests només en troba 54 que siguin de tipus CM.

- Optimitzar la convergència de les sèries que defineixen les funcions θ.

  S'aconsegueix maximitzant la part imaginària de la matriu de períodes que considerem. Això equival a disposar d'un domini fonamental $\mathbb{H}_2 \backslash Sp_4(\mathbb{Z})$ i saber reduir les matrius de períodes a aquest domini (cf. [Go 59]).

- Reconèixer nombres racionals (els invariants d'Igusa) a partir de la seva expressió decimal.

  Això és una aplicació estàndard de l'algoritme LLL. La dificultat és que, vistos els resultats que s'obtenen, cal treballar amb gran precisió (uns 300 decimals).

- Trobar punts de la cònica de Mestre.

  Aquest problema seria senzill si els coeficients de la cònica fossin petits, però els coeficients que s'obtenen arriben a tenir 500 xifres. La cerca de punts implica factoritzar alguns enters d'aquesta grandària.

- Reduir els coeficients d'una equació hiperel·líptica.

  A partir dels punts sobre la cònica de Mestre es dedueix fàcilment l'equació de la corba hiperel·líptica corresponent, però s'obtenen equacions amb coeficients de 5000 xifres, que cal reduir mitjançant transformacions afins.

Van Wamelen aplica l'algoritme 11.4.2 als 54 CM-cossos quàrtics cíclics de discriminant menor que 10^6. D'aquests cossos, n'hi ha 7 amb nombre de classes 1, i 8 amb nombre de classes 2. Naturalment, els que tenen

nombre de classes 1 donen lloc a VAPPP's $\mathbb{Q}$-definides. Dels vuit cossos amb nombre de classes 2, sis donen lloc a VAPPP's $\mathbb{Q}$-definides. Per als altres dos, que són $\mathbb{Q}(\sqrt{-6+2\sqrt{2}})$ i $\mathbb{Q}(\sqrt{-119+28\sqrt{17}})$, només pot arribar a calcular els invariants d'Igusa de les VAPPP's (que surten quadràtics), però no aconsegueix trobar les equacions de les corbes.

En total, Van Vamelen troba 19 corbes de gènere 2 $\mathbb{Q}$-definides amb jacobiana simple i amb multiplicació complexa per l'anell d'enters d'un cos quàrtic cíclic.

11.5 Conclusions

Acabem fent una llista dels principals problemes que caldria resoldre per tal que la teoria de la multiplicació complexa permeti fer teoria de cossos de classes efectiva.

- Generalitzar la j de Klein o els invariants d'Igusa per a varietats abelianes de dimensió $g \geq 3$. Això implicarà conèixer bé les formes modulars de Siegel per al grup $Sp_{2g}(\mathbb{Z})$) i els seus subgrups de congruència.
- Determinar els dominis fonamentals de $\mathbb{H}_g \backslash \Gamma, \Gamma \subseteq Sp_g(\mathbb{Z})$. Això serà necessari per poder avaluar numèricament les formes modulars de Siegel.
- Aprendre a reconèixer els cossos de definició de les varietats abelianes amb multiplicació complexa a partir dels seus invariants. En particular, pot ser necessari aprendre a donar equacions de les varietats.
- Millorar *a la Weber* els invariants. Això pot traduir-se en trobar bones equacions modulars.

Com veiem, hi ha un llarg camí per recórrer.

Bibliografia

[Ba 92] Bayer, P. i Travesa A. (eds.). *Corbes modulars: taules.* Barcelona, 1992.

[Ca 00] G. Cardona. *Superfícies abelianes amb CM.* Barcelona, 2000.

[Fe 00] J. Fernández. Construcció de varietats abelianes amb cm. 2000. en aquest volum.

[Go 59] E. Gottschling. Explizite bestimmung der randflaechen des fundamentalbereiches der modulgruppe zweiten grades. *Math. Ann.*, 138:103–124, 1959.

[Gu 00] J. Guardia. Polaritzacions de varietats abelianes amb multiplicació complexa. 2000. en aquest volum.

[Ko 78] Rohrlich D. Koblitz, N. Simple factors in the jacobian of a Fermat curve. *Canadian J. of Math.*, XXX(6):1183–1205, 1978.

[La 82] S. Lang. *Introduction to algebraic and abelian functions*, volume 89 of *GTM*. Springer V., 2nd edition, 1982.

[Sh 94] G. Shimura. *Introduction to the Arithmetic theory of automorphic forms*, volume 11. Pub. Math. Soc. Japan, 1994.

[VW 99] P. Van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. of Comp.*, 68(225):307–320, 1999.

[We 08] H. Weber. *Lehrbuch der Algebra.* Braunchsweig, 2n edition, 1908.