Montserrat Alsina Angela Arenas
Pilar Bayer

Editores

CORBES DE SHIMURA I APLICACIONS

Publicacions de la Universitat de Barcelona

Barcelona 2005

CORBES DE SHIMURA
I APLICACIONS

amb introducció de R. Livné

Edició a cura de

M. Alsina A. Arenas P. Bayer

Amb contribucions de

M. Alsina	A. Arenas	P. Bayer
R. Re	A. Rio	V. Rotger
A. Travesa	N. Vila	X. Xarles

A. Arenas
Dept. Algebra i Geometria
Facultat de Matemàtiques, UB
Gran Via de les Corts Catalanes, 585
08007 Barcelona. Espanya
angelaarenas@ub.edu

P. Bayer
Dept. Algebra i Geometria
Facultat de Matemàtiques, UB
Gran Via de les Corts Catalanes, 585
08007 Barcelona. Espanya
bayer@ub.edu

M. Alsina
Dept. Matemàtica Aplicada III
EU Politècnica de Manresa
Agda Bases de Manresa, 61-73
08240 Manresa
montserrat.alsina@upc.edu

Classificació AMS
Primària: 11F12, 11G18, 11G20, 11R52, 11S45
Secundària: 11G25,11T71

ISBN: 84-475-2999-1
Dipòsit legal: B-53953-2055

Barcelona, 2005
Amb suport parcial de DGE MCYT BFM 2003-01898,
BFM 2003-06768, BFM 2003-06092

Prefaci

Aquest llibre ofereix una introducció a l'estudi de les corbes de Shimura definides sobre el cos del racionals i a algunes de les seves aplicacions. El seu contingut es basa en les conferències impartides en el *Seminari de Teoria de Nombres* (UB-UAB-UPC), celebrat a Barcelona, del 29 de gener al 2 de febrer de l'any 2001. Una versió preliminar d'aquelles conferències fou publicada en el volum *Corbes de Shimura* [AAB01]. La dificultat intrínseca del tema, unida a la manca general de textos introductoris, ha fet aconsellable preparar una edició ampliada d'aquelles notes.

El llibre consta d'una introducció, a càrrec de Ron Livné, de 10 capítols i d'una llista actualitzada de referències. Les paraules del professor Livné permeten copsar la importància històrica de les corbes i les varietats de Shimura i situar el contingut de cada capítol en el seu context històric. En particular, l'alumnat de tercer cicle hi trobarà una guia per iniciar-se en temes de recerca. Agraïm al professor Livné la seva valuosa aportació.

M. Alsina, A. Arenas, P. Bayer

Barcelona, 31 d'octubre de 2005

Índex

Conferenciants

M. Alsina
Deptartament de Matemàtica Aplicada III
E. U. Politècnica de Manresa,
Universitat Politècnica de Catalunya
Av. Bases de Manresa 61-73, E-08240 Manresa
montserrat.alsina@upc.edu

A. Arenas
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran via de les Corts Catalanes 585, E-08007 Barcelona
angelaarenas@ub.edu

P. Bayer
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran via de les Corts Catalanes 585, E-08007 Barcelona
bayer@ub.edu

Riccardo Re
Dipartimento di Matematica
Universita di Catania
Viale A.Doria 6, 95125 Catania, Italy
riccardo@dmi.unict.it

A. Rio
Dept. Matemàtica Aplicada II,
Universitat Politècnica de Catalunya

Jordi Girona 1-3, E-08034 Barcelona.
ana.rio@upc.edu

V. Rotger Deptartament de Matemàtica Aplicada IV
E. P. S. d'Enginyeria de Vilanova i La Geltrú
Universitat Politècnica de Catalunya
Avda. Víctor Balaguer s/n, E-08800 Vilanova i la Geltrú
vrotger@mat.upc.es

A. Travesa
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran via de les Corts Catalanes 585, E-08007 Barcelona
travesa@ub.edu

N. Vila
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran via de les Corts Catalanes 585, E-08007 Barcelona
nuriavila@ub.edu

X. Xarles
Departament de Matemàtiques
Facultat de Ciències
Universitat Autònoma de Barcelona
E-08193 Bellaterra
xarles@mat.uab.es

Introducció

R. Livné

The Shimura curves are Riemann surfaces uniformized by arithmetic groups. The first examples, the modular curves, go back in special cases at least to Gauss. These examples are atypical since the Riemann surfaces are not compact there, while they are compact in all other cases.

Historically, the next examples to appear were those coming from triangle groups (see e.g. [FK97]). Up to commensurability there are, however, only finitely arithmetic triangle groups ([Tak77a, Tak77b].

The theory of Shimura curves is currently viewed as a special case of the general theory of higher-dimensional arithmetic congruence quotients. This general theory was developed by several people, starting with Siegel, and including Baily, Piateskii-Shapiro and Shafarevich, and Shimura. Deligne's reformulation of Shimura's work [Del71] had become the standard reference for the general theory of what is now called "Shimura varieties" (the terminology was first used by Ihara for curves and by Langlands in general). The most striking result is that there exist *canonical models* for these varieties. These are uniquely determined varieties over a specific number field, the *reflex field*, which underlie the given complex manifolds, and they have canonical, defining properties. For example, a "symplectic" embedding of a Shimura variety into Siegel space, which is the parameter space for principally polarized abelian varieties, gives the canonical model through the theory of moduli ([Del71]). The general case is due to Kazhdan, Borovoi, and others. See Chapter 10 for an example

where the higher dimensional theory is discussed (in a special case) and then applied to counting points on certain Shimura curves over totally real fields. A good place to learn the general theory is Milne's homepage (http://www.jmilne.org/math/) which contains a lot of material on Shimura varieties, much of it unpublished.

Shimura curves were first studied by Shimura ([Shi61, Shi67]) and then by Ihara ([Iha68b, Iha69]). One takes a quaternion algebra B over a totally real number field F, which is split at one infinite prime and ramified at all the others. This case is difficult if $F \neq \mathbb{Q}$, since the reflex field, which is F, is smaller than what the moduli theory can yield. In fact the curve case is most important since the existence of canonical models is by induction on dimension, with the curve case being the starting point (together with the even more important 0-dimensional case of special points).

The main subject of interest regarding Shimura varieties had been their Hasse-Weil L-functions over the reflex field or its extensions. These can frequently be proved to be automorphic, hence to have analytic continuation and functional equation. The first results, for modular curves, were obtained by Eichler (see Chapter 6), and there is currently a lot of work on more general cases. The Langlands philosophy in fact predicts that the L-functions thus obtained should be automorphic in all cases, and that they should cover a very large and important class of the good (=algebraic automorphic) L-functions. Following Deligne and Langlands, Carayol had used Shimura curves over totally real fields to prove the Langlands correspondence for Hilbert modular forms at the bad primes [Car86a, Car86b].

To compute the L-functions one needs to compute the reduction modulo primes of the canonical models. Then one counts the points on these reductions via the Lefschetz trace formula for étale cohomology, and one compares them to the automorphic trace formula. The good reduction of Shimura curves was studied by Morita (see the reference in Chapter 6). The bad reduction (see Chapters 3 and 4) was studied by Carayol ([Car86a]) and by Čerednik and Drinfel'd (see [BC91]). The reduction of Shimura varieties is a topic of much current interest (see e. g. [Var98a, Var98b, Rap90, RZ96]...).

The present book studies mainly Shimura curves over $\mathbb{Q}$. The theory is very close to the case of modular curves, but the absence

of cusps makes certain things easier to prove. On the other hand the very convenient tool of expanding a modular form around a cusp disappears, and hence explicit examples are harder to construct. Ihara was the first to write an equation of a Shimura curve, and his method has been generalized (see Chapter 8). Other ways have been devised by Elkies (see the reference in Chapter 8) and by Kurihara ([Kur94]). Another method is to intersect Hilbert modular surfaces in Siegel space (see e. g. [Run99]). This method permits to get the universal families of Kummer surfaces (the quotient of the universal family of abelian surfaces by ± 1), and even families of genus 2 fibrations whose jacobians give the abelian surfaces ([HM95]). Another method to give the universal Kummer families through special elliptic fibrations was developed jointly with Besser [Bes93, Bes95, Bes98, BL]. A closely related subject is the Picard-Fuchs equations of Shimura curves (see [BL]).

The real points of Shimura curves had been studied by Shimura (and also by Kudla), and the local points over p-adic fields jointly with Jordan and later by others. These local results have global applications to the Cassels-Tate pairing; see Chapter 7, [Bab01], and also [JLV03] for results for more general levels and fields. The global points were studied first by Jordan (see Chapter 7) and recently also by Skorobogatov and Yafaev (see [SY04]) using the local results.

To date, the most spectacular application of Shimura curves is in the proof of the Taniyama-Shimura-Weil modularity conjecture. This involves an interesting technical point: in the applications to L-functions, the cohomology of the Shimura varieties is taken with *rational* coefficients. Recently it has become more and more important to study finer invariants, coming from *integral* cohomology. In this regard a prominent role is played by the structure of the bad reduction of semistable type of Shimura varieties, especially of Shimura curves (see Chapters 3 and 4). This had first appeared in joint work with Jordan [JL86], and was further developed and applied by Ribet to prove that Fermat's Last Theorem follows from the modularity of elliptic curves over $\mathbb{Q}$ (see Chapter 9). It was also used in the proof of this modularity conjecture. Higher dimensional applications are as spectacular. Among several such are the proof of the local Langlands conjecture for GL_n by Harris and Taylor [HT01], and their forthcoming work.

Bibliografia

[Bab01] S. Baba, *Shimura curve quotients with odd Jacobian*, J. Number Theory **87** (2001), 96–108.

[BC91] J-F. Boutot, H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld*, Astérisque **196–197** (1991), 45–158, Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Bes93] A. Besser, *Universal families over shimura curves*, PhD thesis, Tel-Aviv University, 1993.

[Bes95] A. Besser, *CM cycles over Shimura curves*, J. Algebraic Geom. **4** (1995), num. 4, 659–691.

[Bes98] A. Besser, *Elliptic fibrations of $K3$ surfaces and QM Kummer surfaces*, Math. Z., **228** (1998) 283–308.

[BL] A. Besser, R. Livné, *Universal families of Kummer surfaces over Shimura curves*, in preparation.

[Car86a] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. **59** (1986), num. 2, 151–230.

[Car86b] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), num. 3, 409–468.

[Del71] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23 année 1970-71, exp. 389, 139–172, Lecture Notes in Math., vol. 244, Springer, 1971, pp. 123–165.

[Del79] P. Deligne, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, Automorphic forms, representations and L-functions, part 2, (Proc. Sympos. Pure Math., XXXIII, 1977), AMS, 1979, pp. 247–289.

[Elk98] N. Elkies, *Shimura curve computations*, Algorithmic number theory ANTS-3 (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, 1998, pp. 1–47.

[FK97] R. Fricke, F. Klein, *Vorlesungen über die Theorie der automorphen Funktionen*, Leipizig, 1897, Bibliotheca Mathematica Teubneriana, Johnson Reprint Corp., New York; B. G. Teubner Verlagsgesellschaft, Stuttgart 1965.

[HM95] K. Hashimoto, N. Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. **47** (1995), num. 2, 271–296.

[HT01] M. Harris, R. Taylor, *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, vol. 151, Princeton University Press, 2001.

[Iha68b] Y. Ihara, *On congruence monodromy problems. Vol. 1*, Lecture Notes, num. 1, Department of Mathematics, University of Tokyo, Tokyo, 1968.

[Iha69] Y. Ihara, *On congruence monodromy problems. Vol. 2*, Lecture Notes, num. 2, Department of Mathematics, University of Tokyo, Tokyo, 1969.

[JL86] B. Jordan, R. Livné, *On the Néron model of jacobians of Shimura curves*, Compositio Math. **60** (1986), num. 2, 227–236.

[JLV03] Bruce W. Jordan, Ron Livné, Yakov Varshavsky, *Local points of twisted Mumford quotients and Shimura curves*, Math. Ann. **327** (2003), num. 3, 409–428.

[Jor81] B. Jordan, *On the diophantine arithmetic of Shimura curves*, PhD thesis, Harvard University, 1981.

[Kur94] A. Kurihara, *On p-adic Poincaré series and Shimura curves*, Internat. J. Math. **5** (1994), 747–763.

[Rap90] M. Rapoport, *On the bad reduction of Shimura varieties*, Automorphic forms, Shimura varieties, and L-functions, Vol. II (Ann Arbor, MI, 1988), Perspect. Math., vol. 11, Academic Press, 1990, pp. 253–321.

[Run99] B. Runge, *Endomorphism rings of abelian surfaces and projective models of their moduli spaces*, Tohoku Math. J. (2) **51** (1999), num. 3, 283–303.

[RZ96] M. Rapoport, Th. Zink, *Period spaces for p-divisible groups*, Annals of Mathematics Studies, vol. 141, Princeton University Press, 1996.

[Shi61] G. Shimura, *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), num. 3, 275–331.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

[SY04] A. Skorobogatov, A. Yafaev, *Descent on certain Shimura curves*, Israel J. Math. **140** (2004), 319–332.

[Tak77a] K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), num. 1, 91–106.

[Tak77b] K. Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo, I.A. **24** (1977), 201–212.

[Var98a] Y. Varshavsky, *p-adic uniformization of unitary Shimura varieties*, Inst. Hautes Études Sci. Publ. Math. (1998), num. 87, 57–119.

[Var98b] Y. Varshavsky, *p-adic uniformization of unitary Shimura varieties. II*, J. Differential Geom. **49** (1998), num. 1, 75–113.

[vdG82] G. van der Geer, *On the geometry of a Siegel modular threefold*, Math. Ann. **260** (1982), num. 3, 317–350.

Capítol 1

Aritmètica d'àlgebres de quaternions

A. Rio

En aquest capítol s'inclouen les definicions i els resultats bàsics relatius a àlgebres de quaternions que permeten arribar a la definició de $X(D, N)$, que serà l'objecte d'estudi dels capítols posteriors. La referència bàsica per a aquest tema és [Vig80], on es troba desenvolupat de manera sistemàtica i extensa.

1.1 Definicions i exemples

1.1.1 Definicions. Sigui K un cos commutatiu.

Una $K-$**àlgebra** és una quaterna $(A, +, \cdot, \Lambda)$, on $(A, +, \cdot)$ és un anell unitari i Λ és una aplicació $K \times A \longrightarrow A$ tal que $(A, +, \Lambda)$ és un $K-$espai vectorial i es compleix $\Lambda(k, a \cdot b) = a \cdot \Lambda(k, b) = \Lambda(k, a)\, b$.

Una $K-$**àlgebra de divisió** és una $K-$àlgebra (no commutativa) on tot element diferent de zero és invertible.

Una $K-$àlgebra A és **simple** si no té altres ideals bilàters que 0 i A. Les àlgebres de divisió són, doncs, àlgebres simples.

Si A és una $K-$àlgebra i $Z(A)$ indica el seu centre, es compleix $K \simeq \Lambda(K, 1_A) \subseteq A$. Amb aquesta identificació es té $K \subseteq Z(A)$. Observem que si l'àlgebra és de divisió, llavors el seu centre és un cos (extensió de K).

Una $K-$àlgebra A és **central** si $K = Z(A)$.

1.1.2 Exemple. $A = \mathrm{M}(2, K)$ és una $K-$àlgebra central simple.

El cos K s'identifica amb el conjunt de les matrius $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

Si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(A)$, aleshores

$$\begin{aligned} \mathbf{0} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & a-d \\ 0 & c \end{pmatrix}, \\ \mathbf{0} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ -a+d & -b \end{pmatrix}. \end{aligned}$$

Per tant, $a = d,\ b = c = 0$. Així doncs,

$$Z(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in K \right\} \simeq K.$$

Sigui $J \neq 0$ és un ideal bilàter de A i $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J - \{\mathbf{0}\}$. Suposem que $a \neq 0$, aleshores

$$\begin{aligned} \alpha &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in J, \\ \beta &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \in J. \end{aligned}$$

$$\alpha + \beta \in J \Rightarrow J \text{ conté una unitat} \Rightarrow J = A.$$

1.1.3 Definició. Una $K-$**àlgebra de quaternions** és una $K-$àlgebra central i simple, de dimensió 4 sobre K.

1.1.4 Exemple. $\mathrm{M}(2, K)$ és una $K-$àlgebra de quaternions.

La teoria de $K-$àlgebres centrals i simples permet donar una altre definició (cf. [Pie82]), potser més operativa, d'àlgebra de quaternions.

Denotem $\mathcal{S}(K)$ el conjunt de les $K-$àlgebres centrals i simples, de dimensió finita sobre K.

El teorema de Wedderburn-Artin, que s'obté combinant el lema de Schur amb la forma matricial dels endomorfismes, dóna l'estructura general de les àlgebres semisimples. En particular, aquest teorema prova que una $K-$àlgebra simple és isomorfa a una àlgebra de matrius $M_n(D)$, on D és una $K-$àlgebra de divisió, determinada mòdul isomorfisme.

Els dos teoremes que citem a continuació són els considerats com a resultats fonamentals de la teoria de les àlgebres centrals i simples.

El primer teorema generalitza el fet que els únics automorfismes de $M_n(K)$ són els automorfismes interns (és a dir, els de "conjugació per una matriu").

1.1.5 Teorema. (Skolem-Noether) *Si $A \in \mathcal{S}(K)$, aleshores tenim* $\mathrm{Aut}(A) = \{\gamma_u(x) = uxu^{-1},\ u \in A^*\} = \mathrm{Inn}(A) \simeq A^*/K^*$.

1.1.6 Definició. Si A és una $K-$àlgebra i X és un subconjunt de A, llavors el **centralitzador de X en A** es defineix com

$$C_A(X) = \{a \in A \mid ax = xa\ \forall x \in X\}$$

En particular, $C_A(A) = Z(A)$. Si l'àlgebra és central, aleshores $C_A(C_A(A)) = C_A(K) = A$. El teorema següent generalitza això a les subàlgebres simples.

1.1.7 Teorema. (del doble centralitzador) *Si $A \in \mathcal{S}(K)$, B és una subàlgebra simple i $C_A(B)$ és el centralitzador de B en A, llavors:*

1. *$C_A(B)$ és simple.*
2. $\dim_K(B)\dim_K(C_A(B)) = \dim_K(A)$.
3. $C_A(C_A(B)) = B$.

1.1.8 Corol·lari. *Si $A \in \mathcal{S}(K)$ i F n'és un subcòs maximal, llavors* $C_A(F) \simeq M_n(F)$ *i* $\dim_K(A) = n^2\,[F:K]^2$.

DEMOSTRACIÓ: Prenent $B = F$ en el teorema anterior obtenim que $A' = C_A(F)$ és simple. A més, $F \subseteq A'$ n'és un subcòs maximal.

El teorema d'estructura (per a $F-$àlgebres simples) ens diu que $A' \simeq M_n(D)$, on D és una $F-$àlgebra de divisió. Si no fós $D = F$ podríem prendre $x \in D - F$ i $L = F[x]$ (polinomis a coeficients en F avaluats en x) seria un subcòs de D que contindria F estrictament. Identificant L amb les corresponents matrius escalars de $M_n(D)$ es contradiu la maximalitat de F en A'. Per tant, tindrem $D = F$ i $C_A(F) \simeq M_n(F)$.

La igualtat de dimensions es dedueix immediatament del segon apartat del teorema del doble centralitzador. □

Considerem el cas $\dim_K(A) = 4$ i fem ús d'aquest darrer resultat. Per a un subcòs maximal F tenim només dues possibilitats:

1. $F = K$. Aleshores, $A \simeq \mathrm{M}(2, K)$.

2. $F = K(i)$ és una extensió quadràtica de K.

   En aquest cas, atès que l'automorfisme $i \to -i$ és intern, existirà un element $j \in A$ tal que $j^{-1}ij = -i$.

Seguint aquesta línia de treball, s'arriba a la definició *clàssica*: si $\mathrm{car}(K) \neq 2$, una $K-$**àlgebra de quaternions** és una $K-$àlgebra de dimensió 4 sobre K amb una $K-$base $\{1, i, j, k\}$ tal que

$$i^2 = a \in K^*, \qquad j^2 = b \in K^*, \qquad ij = -ji = k.$$

Així doncs, l'operació d'elements de l'àlgebra de quaternions queda definida estenent per linealitat la multiplicació dels elements de la base, que es descriu a la taula següent:

xy	1	i	j	k
1	1	i	j	k
i	i	a	k	$-j$
j	j	$-k$	b	i
k	k	j	$-i$	$-ab$

Per designar aquesta àlgebra es fa servir la notació

$$H = (a, b)_K,$$

tot i que no és independent de la base:

$$\begin{array}{lcccl} \text{base } \{1, j, i, k\} & \Rightarrow & H & = & (b, a)_K, \\ \text{base } \{1, i, k, j\} & \Rightarrow & H & = & (a, -ab)_K, \\ \text{base } \{1, j, k, i\} & \Rightarrow & H & = & (b, -ab)_K, \\ \text{base } \{1, ci, j, k\} & \Rightarrow & H & = & (ac^2, b)_K. \end{array}$$

1.1.9 Observació. Si el cos fós de característica 2, es tindria una base $\{1, i, j, ij\}$, amb $i^2 + i = a,\ j^2 = b,\ ij = j(1 + i)$. Però aquest cas no el tractarem.

Tot seguit comprovem que, efectivament, $H = (a, b)_K$ és una $K-$àlgebra central i simple, fent servir l'operador de Lie

$$[x, y] = xy - yx.$$

- $H = (a, b)_K$ és central: si $x = x_0 + x_1\, i + x_2\, j + x_3\, k \in Z(H)$, aleshores

$$\begin{array}{rcrcrcl} 0 & = & [i, x] = & & 2\, a\, x_3\, j & & +2\, x_2\, k, \\ 0 & = & [j, x] = & & -2\, b\, x_3\, i & & -2\, x_1\, k. \end{array}$$

  Atès que $1, i, j, k$ són una $K-$base de H, es dedueix $x_1 = x_2 = x_3 = 0$. Aleshores, $x = x_0 \in K$.

- $H = (a, b)_K$ és simple: sigui $J \neq 0$ un ideal bilàter i $x \in J - \{0\}$. Si $x = x_0 \in K^*$, llavors $x \in H^*$ i $J = H$. Si $x \neq x_0$, alguna altra coordenada serà $\neq 0$. Atès que

$$\begin{array}{rcl} [j, [i, x]] & = & -4\, b\, x_2\, i \in J, \\ [k, [j, x]] & = & 4\, a\, b\, x_3\, j \in J, \\ [i, [k, x]] & = & -4\, a\, x_1\, k \in J, \end{array}$$

  J conté algun element invertible i, per tant, $J = H$.

1.1.10 Exemples. Prenent la base

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad k = ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

es té

$$\mathrm{M}(2, K) = (1, 1)_K.$$

De la igualtat

$$2\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a + d) + (a - d)i + (b + c)j + (b - c)k$$

s'obtenen les coordenades quaterniòniques d'una matriu.

Si el cos K és algebraicament tancat, aleshores no té extensions quadràtiques i $\mathrm{M}(2, K)$ és l'única àlgebra de quaternions sobre K.

Quaternions de Hamilton: $\mathbb{H} = (-1, -1)_{\mathbb{R}}$

Sobre $\mathbb{R}$, el subcòs maximal ha d'ésser $\mathbb{R}$ o $\mathbb{C}$ i les úniques àlgebres de quaternions són $\mathrm{M}(2, \mathbb{R})$ i $\mathbb{H}$.

1.1.11 Definicions. Considerem l'àlgebra de quaternions

$$H = (a, b)_K$$

i escrivim els seus elements $x = x_0 + x_1\, i + x_2\, j + x_3\, k$.

El conjunt dels **quaternions purs** és $H^+ = \{x \in H \mid x_0 = 0\}$. Es té la descomposició en suma directa

$$H = K \oplus H^+,$$

o sigui, tot element de H s'escriu de manera única com $x = x_0 + z$, amb $x_0 \in K$ i $z \in H^+$; és a dir, com a suma d'un escalar i un quaternió pur. Els quaternions purs es caracteritzen de forma invariant per isomorfismes mitjançant la condició següent:

$$x \in H - \{0\} \text{ és pur } \Leftrightarrow x^2 \in K \text{ i } x \notin K.$$

La **conjugació** és $x \longrightarrow \bar{x} = x_0 - x_1\, i - x_2\, j - x_3\, k = x_0 - z$. Es tracta d'un antiisomorfisme involutiu de H. La conjugació opera sobre els escalars com la identitat i sobre els quaternions purs com la multiplicació per -1.

La **traça reduïda** de x és $t(x) = x + \bar{x} = 2x_0 \in K$.

$(x, y) \longrightarrow t(xy)$ és una forma bilineal simètrica no degenerada.

La **norma reduïda** de x és $n(x) = x\bar{x} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \in K$.

$x \longrightarrow n(x)$ és un forma quadràtica. De fet, és la forma quadràtica associada a la forma bilineal $\frac{1}{2}t(x\bar{y})$.

Els elements invertibles de l'àlgebra són $H^* = \{x \mid n(x) \neq 0\}$. L'invers d'un element $x \in H^*$ és

$$x^{-1} = \bar{x}\, n(x)^{-1}.$$

La restricció $n : H^* \longrightarrow K^*$ és un morfisme de grups. El seu nucli el denotem H^1.

1.1.12 Exemple. Considerem $H = \mathrm{M}(2, K)$. La descomposició de

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$$

com a suma d'un escalar i un quaternió pur és

$$x = x_0 + z = \frac{1}{2}\begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} + \frac{1}{2}\begin{pmatrix} a-d & b \\ c & d-a \end{pmatrix}.$$

Els quaternions purs són les matrius de traça nul·la.

El conjugat de x és $\bar{x} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, és a dir, la matriu d'adjunts.

La traça de x és $t(x) = a + d$. La norma de x és $n(x) = \det(x)$.

1.2 Formes quadràtiques

Segons el teorema d'estructura de Wedderburn-Artin, una $K-$àlgebra de quaternions, o bé és una $K-$àlgebra de divisió o bé és isomorfa a l'àlgebra de matrius $\mathrm{M}(2, K)$. La distinció de casos pot expressar-se en termes de representabilitat de zero per una forma quadràtica de K (cf. [O'M00]).

1.2.1 Proposició. *Sigui $H = (a,b)_K$. Les condicions següents són equivalents:*

1. *H és una $K-$àlgebra de divisió.*
2. *Si $x \in H - \{0\}$, aleshores $n(x) \neq 0$.*
3. *La forma quadràtica $X_0^2 - aX_1^2 - bX_2^2 + abX_3^2$ és anisòtropa.*
4. *La forma quadràtica $X^2 - aY^2 - bZ^2$ és anisòtropa.*

Observem que la forma quadràtica ternària que apareix al darrer apartat de la proposició anterior prové de restringir la norma al subspai dels quaternions purs.

1.2.2 Exemple. Els quaternions de Hamilton $\mathbf{H} = (-1,-1)_{\mathbb{R}}$ són una àlgebra de divisió.

D'una banda, ja sabem que $\mathbf{H}$ i $\mathrm{M}(2,\mathbb{R})$ són les úniques àlgebres de quaternions sobre $\mathbb{R}$. D'altra banda, la forma quadràtica real $X^2+Y^2+Z^2$ és anisòtropa.

1.2.3 Proposició. *L'isomorfisme de $K-$àlgebres de quaternions es pot expressar com a equivalència de formes quadràtiques ternàries:*

$$\begin{array}{rcl} (a,b)_K & \simeq & (a',b')_K \\ & \Updownarrow & \\ aX_1^2 + bX_2^2 - abX_3^2 & \sim & a'X_1^2 + b'X_2^2 - a'b'X_3^2. \end{array}$$

1.2.4 Exemple. Si $a, b \in \mathbb{Z}$ són no nuls i lliures de quadrats, aleshores

$$(a,b)_{\mathbb{Q}} \simeq \mathrm{M}(2,\mathbb{Q}) \Leftrightarrow \left\{ \begin{array}{ll} a,b & \text{no són tots dos} < 0 \\ a & \text{és quadrat mod } b \\ b & \text{és quadrat mod } a \end{array} \right.$$

1.3 Grup de Brauer

Donades dues àlgebres $A, A' \in \mathcal{S}(K)$, sabem que $A \simeq M_n(D)$ i $A' \simeq M_{n'}(D')$, on D i D' indiquen $K-$àlgebres de divisió. Es defineix la *similaritat* entre àlgebres de la manera següent:

$$A \sim A' \text{ si } D \simeq D' \text{ (isomorfisme de } K-\text{àlgebres).}$$

Això és una relació d'equivalència a $\mathcal{S}(K)$ i el conjunt de classes

$$\mathrm{Br}(K) = \mathcal{S}(K)/\sim$$

s'anomena **grup de Brauer** de K. L'operació entre classes,

$$Cl(A)\,Cl(B) = Cl(A \otimes_K B)\,,$$

és associativa, té element neutre $Cl(K)(= Cl(M_n(K))\ \forall n)$ i l'invers de $Cl(A)$ és $Cl(A^*)$, on A^* és l'àlgebra oposada de A, és a dir, l'obtinguda en considerar en A la mateixa estructura d'espai vectorial però una nova estructura d'anell: la definida per $a * b = b \cdot a$.

El grup de Brauer actua com a classificador de les àlgebres de divisió centrals, ja que cadascun dels seus elements està representat per una àlgebra de divisió, única mòdul isomorfisme. Per això, la classe de Brauer també serveix per caracteritzar l'isomorfisme de $K-$àlgebres.

1.3.1 Proposició. *Si $A, B \in \mathcal{S}(K)$,*

$$A \simeq B \Leftrightarrow \begin{cases} Cl(A) = Cl(B) \\ i \\ \dim_K(A) = \dim_K(B). \end{cases}$$

1.3.2 Corol·lari. *En el cas particular d'àlgebres de quaternions,*

$$H \simeq H' \Leftrightarrow Cl(H) = Cl(H').$$

Per tal que l'operació del grup de Brauer es pugui restringir bé al conjunt d'àlgebres de quaternions cal una hipòtesi addicional.

1.3.3 Proposició. *Siguin H i H' dues $K-$àlgebres de quaternions. Si tenen un subcòs maximal isomorf, aleshores*

$$H \otimes H' \simeq H'' \otimes \mathrm{M}(2, K),$$

on H'' és una $K-$àlgebra de quaternions, única mòdul isomorfisme.

Si K és un cos local o global, l'existència de subcòs maximal isomorf és una condició que sempre es satisfà.

Alguns exemples d'àlgebres H, H', H'' que satisfan les condicions de la proposició són

- $(a,b)_K \otimes (a,c)_K \simeq (a,bc)_K \otimes \mathrm{M}(2,K)$,
- $H \otimes H \simeq \mathrm{M}(2,K) \otimes \mathrm{M}(2,K)$.

Aquest darrer exemple ens mostra que si H és una $K-$àlgebra de quaternions, aleshores la seva classe de Brauer o bé és trivial o bé té ordre 2, és a dir, es troba en la $2-$component del grup de Brauer:

$$Cl(H) \in \mathrm{Br}_2(K).$$

1.4 Extensió d'escalars

Si F/K és una extensió de cossos i H és una $K-$àlgebra de quaternions, llavors

$$H_F = H \otimes_K F$$

és una àlgebra de quaternions sobre F.

1.4.1 Exemple.

$$(a,b)_K \otimes_K F = (a,b)_F.$$

Donat un cos F, extensió de K, tenim una immersió

$$\begin{aligned} H &\hookrightarrow H_F \\ x &\to x \otimes 1. \end{aligned}$$

En particular, si prenem $F = K_s$, la clausura separable de K, llavors $H \hookrightarrow H_{K_s} = \mathrm{M}(2,K_s)$.

1.4.2 Definicions.

Un cos F, extensió de K, és **cos neutralitzador** de l'àlgebra de quaternions H si $H_F \simeq \mathrm{M}(2,F)$.

Si F és un cos, una $F-$**representació** de l'àlgebra de quaternions H és una representació matricial $H \hookrightarrow \mathrm{M}(2,F)$.

1.4.3 Exemple.

$$\begin{array}{rcl}(a,b)_K & \hookrightarrow & M_2\big(K(\sqrt{a},\sqrt{b}\,)\big)\\ x & \mapsto & \begin{pmatrix} x_0+x_1\sqrt{a} & \sqrt{b}\,(x_2+x_3\sqrt{a}) \\ \sqrt{b}\,(x_2-x_3\sqrt{a}\,) & x_0-x_1\sqrt{a}\end{pmatrix}\end{array}$$

Si ens restringim a extensions de grau 2, podem caracteritzar els cossos neutralitzadors de les àlgebres de quaternions.

1.4.4 Proposició. *Siguin F/K una extensió quadràtica i H una $K-$àlgebra de quaternions.*

F és cos neutralitzador de H si, i només si, F és isomorf a un subcòs maximal de H.

1.4.5 Exemple. L'aplicació

$$\begin{array}{rcl}(a,b)_K & \hookrightarrow & M_2\big(K(\sqrt{a}\,)\big)\\ x & \mapsto & \begin{pmatrix} x_0+x_1\sqrt{a} & x_2+x_3\sqrt{a} \\ b\,(x_2-x_3\sqrt{a}\,) & x_0-x_1\sqrt{a}\end{pmatrix}\end{array}$$

defineix una $K(\sqrt{a}\,)-$representació de l'àlgebra $(a,b)_K$.

1.5 Cas aritmètic. Ideals i ordres.

Siguin R un domini de Dedekind, K el cos de fraccions de R i H un àlgebra de quaternions sobre K.

1.5.1 Definicions.

Una $R-$**xarxa** de H és un $R-$submòdul finitament generat.

Un element $x \in H$ és $R-$**enter** si $R[x]$ és una $R-$xarxa de H.

1.5.2 Proposició. *Un element x és $R-$enter si, i només si, $t(x) \in R$ i $n(x) \in R$. Per tant, atès que $x^2 - t(x)x + n(x) = 0$, un element $R-$enter és arrel d'un polinomi mònic a coeficients en R.*

1.5.3 Remarca. Els elements enters de H no formen un anell.

1.5.4 Definicions.

Un **ideal** és una $R-$**xarxa completa**: $K \otimes_R I \simeq H$. És a dir, una $R-$xarxa que conté una $K-$base.

Un **ordre** de H és un ideal que té estructura d'anell. Equivalentment, $\mathcal{O} \supseteq R$ un anell d'enters tal que $K\mathcal{O} = H$. En particular, un ordre és un $R-$mòdul lliure de rang 4.

Un **ordre maximal** és un ordre maximal per la relació d'inclusió.

Un **ordre d'Eichler** és $\mathcal{O}_1 \cap \mathcal{O}_2$, amb els ordres $\mathcal{O}_i$ maximals.

Les **unitats** d'un ordre $\mathcal{O}$ formen un grup, que designem per $\mathcal{O}^*$. Es compleix

$$x \in \mathcal{O}^* \Leftrightarrow n(x) \in R^*,$$

ja que $x \in \mathcal{O},\ t(x) \in R \subseteq \mathcal{O} \Rightarrow \bar{x} \in \mathcal{O}$ i $x\bar{x} = n(x)$. Les **unitats de norma reduïda** 1 formen un subgrup, designat per $\mathcal{O}^1$.

En el conjunt dels ideals tenim les operacions

$$\begin{aligned} I^{-1} &= \{x \in H \mid IxI \subseteq I\} \\ IJ &= \{\sum xy\,, \quad x \in I,\ y \in J\}. \end{aligned}$$

D'altra banda, a cada ideal I s'associen dos ordres:

$$\begin{aligned} \mathcal{O}_e(I) &= \{x \in H \mid xI \subseteq I\} \\ \mathcal{O}_d(I) &= \{x \in H \mid Ix \subseteq I\}. \end{aligned}$$

Un ideal I és **bilàter** si $\mathcal{O}_e = \mathcal{O}_d$.

Un ideal I és **normal** si $\mathcal{O}_e$ i $\mathcal{O}_d$ són maximals.

Un ideal I és **enter** si $I \subseteq \mathcal{O}_e$. Equivalentment, $I \subseteq \mathcal{O}_d$.

Un ideal I és **principal** si $I = \mathcal{O}_e h = h\mathcal{O}_d$.

La **norma reduïda** d'un ideal I és l'ideal fraccionari de R generat per les normes reduïdes dels seus elements. El denotem per $n(I)$.

Com hem dit a la primera secció, si H és una $K-$àlgebra de quaternions i t designa la traça reduïda, aleshores

$$\begin{array}{rcl} H \times H & \longrightarrow & K \\ (x,y) & \mapsto & t(xy) = 2(x_0y_0 + ax_1y_1 + bx_2y_2 - abx_3y_3) \end{array}$$

és una forma bilineal simètrica no degenerada. Si $\mathcal{O}$ és un ordre, el seu **dual** és l'ideal bilàter enter

$$\widehat{\mathcal{O}} = \{x \in H \mid t(x\mathcal{O}) \subseteq R\}.$$

La **diferent** d'un ordre és l'ideal $\widehat{\mathcal{O}}^{-1}$.

El **discriminant reduït** d'un ordre és la norma de la seva diferent:

$$d(\mathcal{O}) = n(\widehat{\mathcal{O}}^{-1}).$$

Fixada una base, el quadrat del discriminant s'obté del determinant de la matriu de les traces, és a dir, si $\{e_i\}$ és una $R-$base de $\mathcal{O}$ i $M = \big(t(e_ie_j)\big)$, aleshores

$$d(\mathcal{O})^2 = R \det M.$$

1.5.5 Proposició. *Si $\mathcal{O}$ i $\mathcal{O}'$ són ordres d'una àlgebra de quaternions, aleshores*

$$\mathcal{O}' \subseteq \mathcal{O} \Rightarrow d(\mathcal{O}') \subseteq d(\mathcal{O})$$

amb igualtat si, i només si, $\mathcal{O}' = \mathcal{O}$.

1.6 Cas local

Tractem en aquesta secció el cas que K sigui un cos local. De fet, els casos arquimedians ja han estat completament descrits anteriorment:

- $K = \mathbb{C} \Rightarrow H = \mathrm{M}(2, \mathbb{C})$,
- $K = \mathbb{R} \Rightarrow H = \mathbb{H}$ (quaternions de Hamilton) o $H = \mathrm{M}(2, \mathbb{R})$.

1.6.1 Teorema. *Si K és un cos local no arquimedià, aleshores hi ha una única (mòdul isomorfisme) $K-$àlgebra de quaternions diferent de $\mathrm{M}(2,K)$.*

Si R és l'anell d'enters de K, π és un uniformitzant, F/K és l'única extensió quadràtica no ramificada i $\sigma \in \mathrm{Gal}(F/K)$ és l'element no trivial, aleshores la $K-$àlgebra de quaternions no trivial és

$$H = \left\{ \begin{pmatrix} u & v \\ \pi\sigma(v) & \sigma(u) \end{pmatrix} \mid u, v \in F \right\}.$$

S'obté $H \simeq (a,\pi)_K$ escrivint $F = K(\sqrt{a}\,)$ i prenent

$$i = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}.$$

1.6.2 Exemples. L'única $\mathbb{Q}_2-$àlgebra de quaternions no trivial és $(-3,2)_2$ i l'única $\mathbb{Q}_3-$àlgebra de quaternions no trivial és $(-1,3)_3$

Pel que hem vist abans sobre la relació entre àlgebres de quaternions i formes quadràtiques, per a un cos local no arquimedià tenim dues maneres diferents de definir un mateix caràcter quadràtic del grup $K^*/K^{*2} \times K^*/K^{*2}$:

Invariant de Hasse

$$\varepsilon(a,b) = \begin{cases} 1 & \text{si } (a,b)_K \simeq \mathrm{M}(2,K), \\ -1 & \text{altrament.} \end{cases}$$

Símbol de Hilbert

$$(a,b) = \begin{cases} 1 & \text{si } aX^2 + bY^2 - Z^2 \text{ representa } 0, \\ -1 & \text{altrament.} \end{cases}$$

En aquest cas local també es tenen perfectament caracteritzats els cossos neutralitzadors.

1.6.3 Proposició. *Siguin K un cos local no arquimedià, H una $K-$àlgebra de quaternions i F un cos extensió de K.*

1. *F és cos neutralitzador de H si, i només si, $[F:K]$ és parell.*

2. H té $F-$representació si, i només si, $[F:K]$ és parell.

Pel que fa als ordres, tractem aquí únicament el cas $K=\mathbb{Q}_p$. Per tenir els resultats sobre un altre cos local només cal substituir $\mathbb{Z}_p$ per l'anell d'enters i p per un uniformitzant.

1.6.4 Teorema. *Els ordres maximals de* $\mathrm{M}(2,\mathbb{Q}_p)$ *són* $\mathrm{M}(2,\mathbb{Z}_p)$ *i tots els seus conjugats.*

$$\mathcal{O}_{\underline{n}}=\mathrm{M}(2,\mathbb{Z}_p)\cap\begin{pmatrix}p^n & 0\\ 0 & 1\end{pmatrix}\mathrm{M}(2,\mathbb{Z}_p)\begin{pmatrix}p^n & 0\\ 0 & 1\end{pmatrix}^{-1}=\left\{\begin{pmatrix}a & b\\ p^n c & d\end{pmatrix}\right\}$$

s'anomena **ordre d'Eichler de nivell** $p^n\,\mathbb{Z}_p$.

Per a un ordre $\mathcal{O}$ de l'àlgebra $\mathrm{M}(2,\mathbb{Q}_p)$*, les condicions següents són equivalents:*

1. *$\mathcal{O}$ és ordre d'Eichler.*
2. *$\mathcal{O}$ s'escriu de manera única com a intersecció d'ordres maximals.*
3. *Existeix un únic n tal que $\mathcal{O}$ i $\mathcal{O}_{\underline{n}}$ són conjugats*
4. *$\mathcal{O}$ conté un subanell conjugat de*

$$\left\{\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\mid a,d\in\mathbb{Z}_p\right\}.$$

En les condicions anteriors, el discriminant reduït és $d(\mathcal{O})=p^n\mathbb{Z}_p$.

En el cas de les $\mathbb{Q}_p-$àlgebres de quaternions no trivials, l'estructura és molt més senzilla.

1.6.5 Teorema. *Si H és una $\mathbb{Q}_p-$àlgebra de quaternions tal que $H\not\simeq\mathrm{M}(2,\mathbb{Q}_p)$, aleshores $\tilde{v}(x)=v_p(n(x))$ és una valoració discreta de H, l'anell de la qual és*

$$\mathcal{O}=\{x\in H\mid n(x)\in\mathbb{Z}_p\}.$$

Tenim que:

1. $p\mathcal{O} = \wp^2$ *(p ramifica).*
2. $\mathcal{O}$ *és l'únic ordre maximal de* H*.*
3. $\mathcal{O}$ *és l'únic ordre d'Eichler. S'anomena* **ordre d'Eichler de nivell** $\mathbb{Z}_p$*.*
4. $d(\mathcal{O}) = p\,\mathbb{Z}_p$*.*

1.7 Cas global

Suposem ara que $K = \mathbb{Q}$ (o un cos global). Sigui, doncs, H una àlgebra de quaternions sobre $\mathbb{Q}$.

1.7.1 Definicions.

H és **ramificada a l'infinit** si $H_{\mathbb{R}} = H \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{H}$, l'àlgebra dels quaternions de Hamilton. És a dir,

$$H = (a, b)_{\mathbb{Q}}\,, \text{ amb } a < 0 \text{ i } b < 0.$$

H és **ramificada a un primer** p si $H_p = H \otimes_{\mathbb{Q}} \mathbb{Q}_p$ és $\mathbb{Q}_p$-àlgebra de divisió. És a dir, $H = (a, b)_{\mathbb{Q}}$ i el símbol de Hilbert en p és

$$(a, b)_p = -1.$$

Per a qualsevol $\mathbb{Q}-$àlgebra de quaternions H hi ha un nombre finit de places ramificades, el conjunt de les quals denotem per $\mathrm{Ram}(H)$. La llei de reciprocitat del símbol de Hilbert ens diu que $\prod_v (a, b)_v = 1$ i d'aquí es dedueix que el conjunt $\mathrm{Ram}(H)$ té cardinal parell.

Direm que H és **definida** si $\infty \in \mathrm{Ram}(H)$.

1.7.2 Exemple. Si $H = (-1, -1)_{\mathbb{Q}}$, llavors $\mathrm{Ram}(H) = \{\infty, 2\}$.

1.7.3 Proposició. *Sigui* H *una* $\mathbb{Q}-$*àlgebra de quaternions.*

H és indefinida si, i només si, $\mathbb{R}$ és cos neutralitzador de H.

En aquest cas, existeix una $\mathbb{R}-$*representació de* H *que es realitza en un cos quadràtic:*

$$H \hookrightarrow \mathrm{M}\left(2, \mathbb{Q}(\sqrt{a}\,)\right) \hookrightarrow \mathrm{M}(2, \mathbb{R})$$

1.7.4 Definició. El **discriminant reduït** d'una $\mathbb{Q}-$àlgebra de quaternions H és

$$d_H = \prod_{p \in \mathrm{Ram}(H)} p$$

Si substituim $\mathbb{Q}$ per un cos de nombres K, els discriminants reduïts són ideals enters de l'anell d'enters de K.

En el cas global, els discriminants classifiquen les àlgebres de quaternions.

1.7.5 Teorema. *Siguin H_1, H_2 àlgebres de quaternions sobre $\mathbb{Q}$.*

1. $H_1 \simeq H_2 \Leftrightarrow \mathrm{Ram}(H_1) = \mathrm{Ram}(H_2)$.
2. $H_1 \simeq H_2 \Leftrightarrow d_{H_1} = d_{H_2}$.

1.7.6 Teorema. *Sigui H una $\mathbb{Q}-$àlgebra de quaternions.*

1. $H \simeq \mathrm{M}(2, \mathbb{Q}) \Leftrightarrow H_p \simeq \mathrm{M}(2, \mathbb{Q}_p)\ \forall p \Leftrightarrow d_H = 1$.
2. *Sigui S un conjunt finit de places de $\mathbb{Q}$ (si K és un cos de nombres, cal excloure les places complexes), de cardinal parell. Mòdul isomorfisme, existeix una única $\mathbb{Q}-$àlgebra de quaternions H tal que* $\mathrm{Ram}(H) = S$.

   Donat $d \in \mathbb{Z}^+$ lliure de quadrats, es pot trobar explícitament $H/\mathbb{Q}$ tal que $d_H = d$.
3. *Sigui L un cos de nombres. Aleshores, L és cos neutralitzador de $H \Leftrightarrow L_\wp$ és cos neutralitzador de H_p per a tot $\wp \mid p$ de L.*

Així, per tractar el cas global cal tenir en compte que hi ha tota una sèrie de propietats locals:

- ésser ordre
- ésser ordre maximal
- ésser ordre d'Eichler
- ésser ideal
- ésser ideal enter
- ésser ideal bilàter
- norma reduïda d'un ideal
- discriminant reduït d'un ordre

que fan molt útil la tècnica de la adelització.

Si per a cada plaça v del cos es té un grup G_v i un subgrup C_v, en fixar un conjunt de places S es defineix el **grup adèlic**

$$\{(x_v) \in \prod G_v \mid x_v \in C_v \text{ per a tot } v \notin S \text{ llevat d'un nombre finit}\}.$$

1.7.7 Definicions. Suposem que K és un cos global i R és el seu anell d'enters.

Les **adeles** de K són el grup adèlic corresponent a

$$G_v = K_v \quad C_v = R_v \quad S = \infty,$$

és a dir,

$$\mathbf{A} = \{(x_v) \in \prod K_v \mid x_v \in R_v \ qpt \ v \text{ finita}\}.$$

Les **ideles** de K són el grup adèlic corresponent a

$$G_v = K_v^* \quad C_v = R_v^* \quad S = \infty,$$

és a dir, les unitats de les adeles:

$$\mathbf{A}^* = \{(x_v) \in \prod K_v^* \mid x_v \in R_v^* \ qpt \ v \text{ finita}\}.$$

Considerem H/K una àlgebra de quaternions. Per a cada plaça v de K posem $H_v = H \otimes_K K_v$. Fixem $S \neq \emptyset$ un conjunt finit de places de K tal que $S \supseteq \infty$.

L'anell

$$R_S = \bigcap_{v \notin S} (R_v \cap K)$$

és un anell de Dedekind. Si $\mathcal{O}$ és un R_S-ordre de H, posem

$$\mathcal{O}_v = \mathcal{O} \otimes_{R_S} R_v.$$

Considerem els grups adèlics corresponents a

- $G_v = H_v \qquad C_v = \mathcal{O}_v \qquad$ (**Adeles** $H_{\mathbf{A}}$),
- $G_v = H_v^* \qquad C_v = \mathcal{O}_v^* \qquad$ (Unitats $H_{\mathbf{A}}^*$),
- $G_v = H_v^1 \qquad C_v = \mathcal{O}_v^1 \qquad$ (Grup $H_{\mathbf{A}}^1$),

i definim

- la traça reduïda $t_{\mathbf{A}} : H_{\mathbf{A}} \longrightarrow \mathbf{A}$,
- la norma reduïda $n_{\mathbf{A}} : H^*_{\mathbf{A}} \longrightarrow \mathbf{A}^*$.

Els resultats següents s'obtenen utilitzant aquest tècnica d'adelització, que permet aprofitar l'estudi del cas local fet anteriorment.

1.7.8 Proposició. *Sigui H una àlgebra de quaternions sobre $\mathbb{Q}$.*

1. *Un $\mathbb{Z}-$ordre $\mathcal{O}$ és maximal si, i només si, $d(\mathcal{O}) = d_H$.*
2. *El* **nivell** *d'un ordre d'Eichler $\mathcal{O}$ és*

$$N = \prod_p N_p = \prod_{p \notin \mathrm{Ram}(H)} N_p = \prod_{p \nmid d_H} N_p.$$

1.7.9 Notació. $\mathcal{O}(D, N)$ indica un ordre d'Eichler de nivell N d'una àlgebra de quaternions de discriminant D i $\mathcal{O}(D, 1)$ un ordre maximal.

1.7.10 Teorema. *Sigui $\mathcal{O} = \mathcal{O}(D, N)$. Aleshores,*

1. $p \nmid ND \Rightarrow \mathcal{O}_p \simeq \mathrm{M}(2, \mathbb{Z}_p)$.
2. $p \mid D \Rightarrow \mathcal{O}_p \simeq$ *únic ordre maximal de H_p (que és $\not\simeq \mathrm{M}(2, \mathbb{Q}_p)$).*
3. $p \mid N \Rightarrow \mathcal{O}_p \simeq \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_p \right\}$.
4. $d(\mathcal{O}) = D\,N$.

1.7.11 Proposició. *Sigui H una $\mathbb{Q}-$àlgebra de quaternions de discriminant D. Aleshores*

1. *Un $\mathbb{Z}-$ordre d'Eichler és de nivell $N \Leftrightarrow d(\mathcal{O}) = D\,N$.*
2. *Per a tot N tal que $(N, D) = 1$, existeixen ordres d'Eichler de nivell N.*
3. $[\mathcal{O}(D, 1) : \mathcal{O}(D, N)] = N$.

1.8 Tipus i classes

De l'estudis fet pel cas local, sabem que tots els ordres d'Eichler $\mathcal{O}(D,N)$ són localment conjugats. Diem que són del mateix **tipus** si ho són globalment.

1.8.1 Notació. $t(D,N)$ indica el nombre de tipus d'ordres d'Eichler de nivell N en una àlgebra de quaternions de discriminant D.

Si $\mathcal{O}$ és un ordre d'una àlgebra de quaternions H, considerem els ideals I tals que $\mathcal{O}I = I$ (és a dir, $\mathcal{O} \subseteq \mathcal{O}_e(I)$) i en aquest conjunt definim la relació d'equivalència

$$I \sim J \text{ si existeix } x \in H^* \text{ tal que } I = Jx.$$

1.8.2 Notació. $h(\mathcal{O})$ indica el nombre de classes (laterals) d'aquesta relació i $h'(\mathcal{O})$ el nombre de classes de la relació restringida al conjunt dels ideals bilàters.

Si $\mathcal{O}_1$ i $\mathcal{O}_2$ són ordres d'Eichler de nivell N, la conjugació local implica que estan "lligats" per un ideal principal ($\mathcal{O}_1 x = x\mathcal{O}_2$). En aquest cas, els nombres de classes esmentats només depenen del parell (D,N) i es designen per $h(D,N)$ i $h'(D,N)$, respectivament.

1.8.3 Proposició. *Amb les notacions anteriors, es té* $h'(D,N) \leq h(D,N)$ *i* $t(D,N) \leq h(D,N)$.

Per obtenir resultats relatius a tipus i classes novament entra en joc l'adelització, ja que es tenen les correspondències bijectives següents:

$$\begin{aligned}
\text{Ideals} &\leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash H_{\mathbf{A}}^*, \\
\text{Ideals bilàters} &\leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash N(\mathcal{O}_{\mathbf{A}}), \\
\text{Classes d'ideals} &\leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash H_{\mathbf{A}}^* / H_K^*, \\
\text{Classes d'ideals bilàters} &\leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash N(\mathcal{O}_{\mathbf{A}}) / (H_K^* \cap N(\mathcal{O}_{\mathbf{A}})), \\
\text{Tipus d'ordres} &\leftrightarrow H_K^* \backslash H_{\mathbf{A}}^* / N(\mathcal{O}_{\mathbf{A}}).
\end{aligned}$$

on $N(\mathcal{O}_{\mathbf{A}})$ és el normalitzador de $\mathcal{O}_{\mathbf{A}}$ en $H^*_{\mathbf{A}}$.

1.8.4 Proposició. *El nombre de classes $h(D,N)$ és finit i s'obté sumant els nombres de classes d'ideals bilàters sobre un sistema de representants dels tipus:*

$$h(D,N) = \sum_{i=1}^{t(D,N)} h'_i(D,N).$$

1.8.5 Corol·lari. *Si $h'(D,N)$ no depèn del tipus, aleshores*

$$h(D,N) = t(D,N)h'(D,N).$$

Aquesta situació és la que es dóna quan H és indefinida.

1.8.6 Proposició. *Si $K = \mathbb{Q}$, llavors $h(D,N) = 1$ i $t(D,N) = 1$. En general, $h(D,N) = h$, el nombre de classes (restringit) del cos K.*

1.9 Interpretació modular

Sigui H una $\mathbb{Q}-$àlgebra de quaternions indefinida, és a dir, tal que

$$H \hookrightarrow H \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R}),$$

i de discriminant $d_H = D$.

Atès que hi ha un sol tipus, tots els $\mathcal{O}(D,N)$ són conjugats.

1.9.1 Notació.

$$\Gamma(D,N) = \{\gamma \in \mathcal{O}(D,N) \mid n(\gamma) = 1\} = \mathcal{O}(D,N)^1.$$

Tenim

$$\Gamma(D,N) \hookrightarrow H \hookrightarrow \mathrm{M}(2,\mathbb{R})$$

i, atès que la norma es correspon amb el determinant,

$$\mathrm{Im}(\Gamma(D,N)) \subseteq SL_2(\mathbb{R}).$$

Fent la identificació

$$SL_2(\mathbb{R})/\{\pm 1\} \simeq \mathrm{Aut}(\mathcal{H}),$$

resulta que $\Gamma(D, N)$ opera sobre el semiplà superior.

Denotem per $X(D, N)$ la corba tal que

$$\Gamma(D, N) \setminus \mathcal{H} \simeq X(D, N)(\mathbb{C})$$

Un teorema degut a Shimura garanteix que les corbes $X(D, N)$ tenen models definits sobre $\mathbb{Q}$.

Bibliografia

[Als00a] M. Alsina, *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura*, Tesi doctoral, Publ. Universitat de Barcelona, 2000.

[Eic55] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151.

[O'M00] O. O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer, Berlin, 2000, Reprint of the 1973 edition.

[Pie82] R. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer, New York, 1982, Studies in the History of Modern Science, 9.

[Vig80] M-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., num. 800, Springer, 1980.

[Wei67] A. Weil, *Basic number theory*, vol. 144, Grundl. math. Wiss., 1967.

Capítol 2

Superfícies abelianes amb multiplicació quaterniònica

V. Rotger

Introducció

Un ingredient molt important en l'estudi de la geometria i l'aritmètica de les corbes de Shimura és la seva interpretació modular. Sembla doncs molt interessant tenir un bon coneixement dels objectes que classifiquen aquestes corbes.

En efecte, les corbes de Shimura $X(D,N)$ són espais de moduli de superfícies abelianes amb multiplicació quaterniònica (per una àlgebra de quaternions racional de discriminant D) i estructura de nivell (de tipus $\Gamma_0(N)$).

En aquestes notes estudiarem aquestes varietats abelianes sobre el cos dels nombres complexos, cossos locals, cossos finits i cossos globals.

Introduïm primer les definicions i notacions que utilitzarem al llarg d'aquests apunts.

Sigui k un cos i sigui A/k una varietat abeliana sobre k de dimensió $g \geq 1$.

Notem $\mathrm{End}_k(A)$ l'anell d'endomorfismes definits sobre el cos k de la varietat abeliana A. $\mathrm{End}_k(A)$ és una $\mathbb{Z}$-àlgebra de rang finit. Sigui $\mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes \mathbb{Q}$.

Una varietat abeliana A/k és k-simple si A no conté subvarietats abelianes pròpies definides sobre k. Dues varietats abelianes de la mateixa dimensió són isògenes si existeix un morfisme finit d'una en l'altra.

Una polarització en una varietat abeliana A és un feix invertible ample L en A.

Finalment, una àlgebra associativa D és simple si no admet ideals bilàters no trivials. D és semisimple si és suma directa d'àlgebres simples. Una àlgebra simple és una àlgebra de divisió si tots els elements no nuls són invertibles.

La motivació fonamental per a l'estudi de les superfícies abelianes amb multiplicació quaterniònica parametritzades per les corbes de Shimura són els següents teoremes sobre l'estructura de l'àlgebra d'endomorfismes d'una varietat abeliana.

2.0.2 Teorema. (de descomposició de Poincaré) *Sigui A/k una varietat abeliana definida sobre un cos k. Aleshores A és k-isògena a un producte de varietats abelianes k-simples: $A \sim \Pi A_i^{n_i}$ per a certes A_i/k varietats abelianes k-simples no isògenes entre si, $n_i \geq 1$.*

En aquest cas, $\mathrm{End}_k^0(A) \cong \oplus \mathrm{M}(n_i, D_i)$, 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.

2.0.3 Teorema. (de classificació) *Sigui (A, L) una varietat abeliana polaritzada i simple sobre un cos k, $k = \bar{k}$, de dimensió g.*

Sigui $\mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes \mathbb{Q}$ l'àlgebra de divisió dels endomorfismes d'A i sigui K el centre de $\mathrm{End}_k^0(A)$.

Sigui $K_0 = \{f \in K, f = f^*\}$, el subcòs de K fix per la involució de Rosati $* = *_L$ associada a L.

Notem $e = [K : \mathbb{Q}]$, $e_0 = [K_0 : \mathbb{Q}]$, $d^2 = [\mathrm{End}_k^0(A) : K]$.

Aleshores

a) K_0 *és un cos totament real.*

b) $K = K_0$ *o bé* K *és un cos CM sobre* K_0. *En el primer cas* $e = e_0$ *i en el segon* $e = 2e_0$.

c) $\mathrm{End}_k^0(A)$ *és una àlgebra de divisió isomorfa a una de les àlgebres següents :*

I) $\mathrm{End}_k^0(A) = K = K_0$ *i* $*_L = Id_K$.

En aquest cas, necessàriament $e|g$.

II) $K = K_0$ *és un cos totalment real.* $\mathrm{End}_k^0(A)$ *és una àlgebra de quaternions sobre* K *totalment indefinida. És a dir, per a tot homomorfisme* $\sigma : K \to \mathbb{R}$, $\mathrm{End}_k^0(A) \otimes_\sigma \mathbb{R} \cong \mathrm{M}(2, \mathbb{R})$.

En aquest cas, necessàriament $2e|g$.

III) $K = K_0$ *és un cos totalment real.* $\mathrm{End}_k^0(A)$ *és una àlgebra de quaternions totalment definida sobre* K.

És a dir, per a tot homomorfisme $\sigma : K \to \mathbb{R}$, $\mathrm{End}_k^0(A) \otimes_\sigma \mathbb{R} \cong \mathbb{H}$, *on* $\mathbb{H}$ *denoten els quaternions de Hamilton.*

En aquest cas, necessàriament $2e|g$ *si car* $k = 0$; $e|g$ *si car* $k = p > 0$.

IV) K *és un cos CM, extensió quadràtica de* K_0, *un cos totalment real.* $\mathrm{End}_k^0(A)$ *és una àlgebra de divisió sobre* K.

Necessàriament $e_o d^2|g$ *si car* $k = 0$; $e_0 d|g$ *si car* $k = p > 0$.

Si $(A,\ L)/k$ és una varietat abeliana polaritzada de dimensió g i simple sobre un cos k no necessàriament algebraicament tancat, aleshores el teorema anterior no és cert per a l'àlgebra $\mathrm{End}_k^0(A)$. Sigui $\bar{k}$ la clausura algebraica de k. Del teorema anterior, l'única informació que obtenim és que $\mathrm{End}_k^0(A) \subset \mathrm{End}_{\bar{k}}^0(A)$ és una subàlgebra simple.

Si especialitzem aquests resultats a les superfícies abelianes obtenim el següent resultat.

2.0.4 Corol·lari. *Sigui* A, L *una superfície abeliana polaritzada no*

necessàriament simple definida sobre un cos k. Aleshores $\mathrm{End}_{\bar{k}}^0(A)$ *és isomorfa a una de les següents àlgebres:*

1. $\mathbb{Q}$
2. *Un cos quadràtic real.*
3. *Un cos CM sobre un cos quadràtic real.*
4. *Una àlgebra de quaternions indefinida B sobre $\mathbb{Q}$.*
5. *(Si car $k = p > 0$) Una àlgebra de quaternions B totalment definida sobre $\mathbb{Q}(\sqrt{d})$, $d > 0$, un cos quadràtic real.*
6. *(Si car $k = p > 0$) Una àlgebra de quaternions B sobre $\mathbb{Q}(\sqrt{-d})$, $d > 0$, un cos quadràtic imaginari.*
7. $\mathbb{Q}\times\mathbb{Q}$, $\mathbb{Q}\times\mathbb{Q}(\sqrt{-d})$, $\mathbb{Q}(\sqrt{-d})\times\mathbb{Q}(\sqrt{-d})$, $\mathrm{M}(2,\mathbb{Q})$, $\mathrm{M}(2,\mathbb{Q}(\sqrt{-d}))$ *on $d > 0$.*
8. *(Si car $k = p > 0$)* $\mathbb{Q} \times D_p$, $\mathbb{Q}(\sqrt{-d}) \times D_p$, $D_p \times D_p$, $\mathrm{M}(2, D_p)$ *on D_p és l'àlgebra de quaternions sobre $\mathbb{Q}$ de discriminant p.*

Els dos darrers casos es produeixen si i només si A és isògena a un producte de corbes el·líptiques sobre $\bar{k}$.

Notem també que el teorema 2.0.3 de classificació en principi no presenta cap obstrucció perquè un cos quadràtic imaginari o una àlgebra de quaternions definida sobre $\mathbb{Q}$ es realitzin com a àlgebra d'endomorfismes d'una superfície abeliana.

En canvi, aquests dos casos han estat exclosos en la llista de possibilitats per a l'àlgebra d'endomorfismes $\mathrm{End}_{\bar{k}}^0(A)$ d'una superfície abeliana. Això es deu a què una anàlisi detallada (deguda a Shimura) mostra que aquestes dues possibilitats no es donen mai ([Shi63c], [BL92]).

És convenient també remarcar de nou que aquest teorema descriu l'àlgebra dels endomorfismes d'A definits sobre la clausura algebraica $\bar{k}$ de k i que en general tan sols tenim una inclusió $\mathrm{End}_k^0(A) \subset \mathrm{End}_{\bar{k}}^0(A)$. A partir d'ara ens concentrarem en les superfícies abelianes amb multiplicació quaterniònica.

Per a poder precisar què entenem per *multiplicació quaterniònica*, introduïm la següent data inicial (cf. Rio, capítol 1).

Sigui B una àlgebra de quaternions sobre $\mathbb{Q}$ de discriminant D. Suposem a més que B és indefinida, és a dir,

$$B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}(2, \mathbb{R}).$$

Sota aquesta assumpció, podem escollir una immersió

$$\Psi : B \hookrightarrow \mathrm{M}(2, \mathbb{R})$$

que, pel teorema de Skolem-Noether (cf. Rio, capítol I), és única llevat de conjugació per elements de $\mathrm{GL}_2(\mathbb{R})$.

Pels teoremes d'Eichler (cf. [Als00a], [Vig80], cap. V), tots els anells maximals d'enters de B són conjugats entre si. Triem $\mathcal{O} \subset B$ un ordre maximal d'enters en aquesta única classe de conjugació. $\mathcal{O}$ és un anell principal: tots els ideals laterals són principals (cf. Rio, capítol 1).

Diem que una (anti-)involució $\phi : B \to B$ és positiva (respecte a la traça reduïda) si per a tot $b \in B$, $b \neq 0$, $\mathrm{tr}(b \cdot \phi(b)) > 0$. De nou degut al teorema de Skolem-Noether, totes les involucions positives en B són de la forma $\phi(b) = v^{-1} \cdot \bar{b} \cdot v$ on $v \in B$ satisfà $v^2 + d = 0$, $d \in \mathbb{Q}^*$, $d < 0$. D'altra banda, pels teoremes d'Eichler sobre immersions d'ordres quadràtics en ordres quaterniònics (cf. [Vig80], [Als00a]), existeix un element $u \in \mathcal{O}$ tal que $u^2 + Disc(B) = 0$. Fixant-ne un, obtenim una involució positiva en B que denotarem

$$\begin{array}{rccc} * : B & \to & & B \\ b & \mapsto & b^* = u^{-1} \cdot b \cdot u. & \end{array}$$

2.1 Superfícies abelianes amb multiplicació quaterniònica sobre un cos k qualsevol

Fixem la data inicial (B, $\mathcal{O}$, $\Psi : B \hookrightarrow \mathrm{M}(2, \mathbb{R})$, $b \to b^*$) tal com hem descrit anteriorment.

2.1.1 Definició. Una superfície abeliana amb multiplicació quaterniònica (QM) sobre un cos k és un parell (A, i) on

- A és una varietat abeliana de dimensió 2,
- $i : \mathcal{O} \hookrightarrow \mathrm{End}_k(A)$ és una immersió de l'ordre d'enters $\mathcal{O}$ en l'anell de k-endomorfismes d'A.

En aquest cas es diu que A té QM per $\mathcal{O}$. Una ullada al corol·lari 2.0.4 mostra que si A té QM i car $k = 0$, aleshores necessàriament $\mathrm{End}_k^0(A)$ és del tipus 4 ó 7. $\mathrm{M}_2(\mathbb{Q}(\sqrt{-d}))$.

En cas que car $k = p > 0$, aleshores poden donar-se els tipus 4, 6, 7. $\mathrm{M}_2(\mathbb{Q}(\sqrt{-d}))$ i 8.

Una superfície abeliana polaritzada amb multiplicació quaterniònica sobre k és una tripleta (A, i, L) on

- (A, i) és una superfície abeliana amb QM sobre k i
- L és una polarització definida sobre k tal que *la involució de Rosati* $*_L : \mathrm{End}_k^0(A) \to \mathrm{End}_k^0(A)$ *restringida a* B *via la immersió* i *coincideix amb la involució positiva* $*$ *de* B *que hem fixat abans.*

És a dir, per a tot $b \in \mathcal{O}$, $i(b^*) = \phi_L \cdot i(\hat{b}) \cdot \phi_L^{-1}$, on ϕ_L denota la isogènia entre A i la superfície abeliana dual $\hat{A}$ induïda per L (cf. [GL00]).

Recordem que una polarització L està definida sobre un cos k si i només si és el feix invertible associat a una corba $C \subset A$ definida sobre k.

Les superfícies abelianes polaritzades amb QM (A, i, L) a vegades s'anomenen *corbes el·líptiques falses* perquè, tal com veurem, s'assemblen en molts aspectes al quadrat d'una corba el·líptica $E^2 = E \times E$. De fet, si E és una corba el·líptica, aleshores $A = E^2$ és una superfície abeliana amb una immersió natural $i : \mathrm{M}_2(\mathbb{Z}) \hookrightarrow \mathrm{End}(A)$. Com $\mathrm{M}_2(\mathbb{Z})$ és un ordre d'enters maximal de l'àlgebra de quaternions escindida $\mathrm{M}_2(\mathbb{Q})$, (A, i) esdevé l'exemple bàsic de superfícies abelianes amb QM.

Tal com hem dit a la introducció, la motivació principal per a estudiar aquestes superfícies és que les corbes de Shimura $X(D) =$

$X(D,1)$ de nivell trivial parametritzen les classes d'isomorfisme de tripletes $(A,\, i,\, L)$ on $\mathcal{O}$ és l'ordre maximal d'enters d'una àlgebra de quaternions B de discriminant D. Les corbes de Shimura $X(D,N)$ de nivell N classifiquen llevat d'isomorfisme les quadrupletes $(A,\, i,\, L,\, \langle P\rangle)$ on $(A,\, i,\, L)$ són superfícies abelianes polaritzades amb QM per l'ordre $\mathcal{O}$ maximal d'enters i on $\langle P\rangle \in A[N]$ és un grup cíclic de N-torsió invariant per l'acció d'$\mathcal{O}$ (cf. [Cla03]).

És important observar que les superfícies abelianes parametritzades per les corbes $X(D,N)$ tenen multiplicació per $\mathcal{O}$ un ordre maximal i no per un ordre d'Eichler.

Superfícies abelianes amb QM i CM

2.1.2 Definició. Una varietat abeliana A de dimensió g definida sobre un cos k té multiplicació complexa sobre k si existeixen un cos CM F de grau $2g$ sobre $\mathbb{Q}$ i una immersió $j : F \hookrightarrow \mathrm{End}_k^0(A)$.

És convenient aclarir que una varietat abeliana A pot tenir multiplicació complexa per diferents (i fins i tot infinits) cossos CM. Aquest fet contrasta amb el que succeeix en corbes el·líptiques amb CM: el cos de multiplicació complexa és únic.

Sigui ara $(A,\, i)$ una superfície abeliana amb multiplicació quaterniònica sobre un cos k.

Aleshores, d'acord amb la definició anterior, A té multiplicació complexa sobre una extensió k' de k si existeix un cos CM F de grau 4 sobre $\mathbb{Q}$ i una immersió $j : F \hookrightarrow \mathrm{End}_{k'}^0(A)$. En aquest cas direm que A (o potser millor la tripleta (A, i, j)) té QM i CM simultàniament.

Podem donar la següent caracterització de les superfícies abelianes amb QM i CM sobre un cos de característica 0.

2.1.3 Teorema. *Sigui $(A,\, i)$ una superfície abeliana amb QM sobre k, $\mathrm{car}\, k = 0$, per un ordre maximal d'enters $\mathcal{O}$ en l'àlgebra de quaternions B. Identifiquem B amb una subàlgebra de $\mathrm{End}_k^0(A)$ via i.*

Aleshores són equivalents:

i) A té multiplicació complexa sobre k'.

ii) el commutador

$$\mathrm{End}_B^0(A/k') = \{\phi \in \mathrm{End}_{k'}^0(A) : \phi \cdot b = b \cdot \phi \quad \forall b \in B\}$$

és un cos quadràtic imaginari K que escindeix B, és a dir, $B \otimes K \cong \mathrm{M}(2, K)$ o, equivalentment, $K \subset B$.

iii) $\mathrm{End}_{k'}^0(A) \cong \mathrm{M}(2, K)$ *on K és un cos quadràtic imaginari K que escindeix B.*

iv) A és k'-isògena al quadrat $E \times E$ d'una corba el·líptica E/k' amb multiplicació complexa sobre k' per un cos quadràtic imaginari K que escindeix B.

Prova: Observem primer que iii) i iv) són clarament equivalents pel teorema 2.0.3.

i)⇒iii), iv): Si A té multiplicació complexa per un cos CM F de grau 4 aleshores $\mathrm{End}_{k'}^0(A)$ inclou estrictament B i pel teorema 2.0.3 A no pot ser k'-simple. Només pot donar-se el cas que A és k' isògena al quadrat d'una corba el·líptica E/k' amb multiplicació complexa per un cos quadràtic imaginari K tal que $B \otimes K \cong \mathrm{M}(2, K)$. Necessàriament $K \subset B$ (cf. Rio, capítol 1) o, equivalentment (cf. Rio, capítol 1), K escindeix B.

iii)⇒ii): Segueix del següent teorema clàssic de bicommutativitat de R-àlgebres associatives: sigui R un anell commutatiu i siguin B_1,B_2 dues àlgebres associatives sobre R. Sigui $B = B_1 \otimes_R B_2$. Aleshores el commutador de B_1 en B és B_2 i viceversa.

ii)⇒i): Sigui L un cos quadràtic real que escindeix B i l'identifiquem amb un subcos de B. L'existència d'L la garanteix el fet que B és indefinida ([Als00a], [Vig80]). Identificant de nou ara L amb un subcòs d'$\mathrm{End}_{k'}^0(A)$ via la immersió i, la composició $L \cdot \mathrm{End}_B^0(A/k')$ és un subcòs d'$\mathrm{End}_{k'}^0(A)$ isomorf a $L \cdot K$, de grau $4 = 2\dim(A)$ sobre $\mathbb{Q}$. Per tant, A té CM sobre k'. □

Com a conseqüència d'aquest teorema, observem que si una superfície amb QM (A, i) té multiplicació complexa, aleshores en realitat (A, i) té multiplicació complexa per a infinits cossos CM quàrtics F.

De tota manera, de les caracteritzacions anteriors queda clar que si (A, i) té multiplicació complexa sobre un cos k', aleshores hi ha un

cos *quadràtic* imaginari distingit i únicament determinat: el commutador $K = \mathrm{End}_B^0(A/k')$. És natural aleshores fer la següent definició, que tan sols està ben motivada en aquest cas particular de les superfícies abelianes amb QM.

2.1.4 Definició. Sigui $(A, i)/k$ una superfície abeliana amb QM. Si a més (A, i) té multiplicació complexa sobre un cos k', diem que (A, i) té CM pel cos quadràtic $K = \mathrm{End}_B^0(A/k'))$.

2.1.5 Observació. Podem descriure millor la multiplicació complexa de (A, i) precisant l'ordre quadràtic $\mathrm{End}_{\mathcal{O}}(A/k') \subset K$. Tenim que $\mathrm{End}_{\mathcal{O}}(A/k') = R_f$ és un ordre d'enters de conductor f en l'ordre maximal $R_1 = R_K$.

2.1.6 Observació. És un resultat clàssic de Tate que *totes* les varietats abelianes definides sobre un cos finit tenen CM. Això contrasta amb el que succeeix sobre un cos de característica 0, on una varietat abeliana genèrica no té multiplicació complexa. Més endavant tractarem aquests punts amb més detall.

2.2 Superfícies abelianes amb multiplicació quaterniònica sobre $\mathbb{C}$

Sobre el cos dels nombres complexos $\mathbb{C}$, una superfície abeliana $A/\mathbb{C}$ és isomorfa, com a varietat analítica, a un tor complex:

$$\mathbb{C}^2/\Lambda \cong A(\mathbb{C}).$$

És natural preguntar-se si podem construir explícitament xarxes de períodes Λ tals que el tor complex $\mathbb{C}^2/\Lambda$ és una superfície abeliana amb multiplicació quaterniònica. Recordem [GL00] que si $\Lambda \subset \mathbb{C}$ és una xarxa qualsevol, $\mathbb{C}^2/\Lambda$ no és necessàriament una superfície abeliana perquè sovint aquesta varietat analítica no és algebraica. De fet, aquest és el cas genèric.

Sigui $D = p_1 \cdot \ldots \cdot p_{2r}$ un enter positiu lliure de quadrats, producte d'un nombre parell de primers. Sigui B l'àlgebra de quaternions indefinida sobre $\mathbb{Q}$ de discriminant D. Triem un ordre maximal d'enters $\mathcal{O}$ i fixem una immersió $\Psi : B \hookrightarrow \mathrm{M}(2, \mathbb{R})$. Per a completar la data

inicial ens cal triar una involució positiva en B i per a fer-ho considerem un element $\mu \in \mathcal{O}$ tal que $\mu^2 + D = 0$. L'existència d'aquest element és garantida pels teoremes d'immersions optimals d'Eichler (cf. [Als00a], [Vig80]).

L'element $\mu \in \mathcal{O}$ defineix una (anti-)involució en l'àlgebra B:

$$\begin{array}{rccc} * : B & \mapsto & B \\ \beta & \mapsto & \beta^* := \mu\bar{\beta}\mu^{-1} \end{array} ,$$

No és difícil veure que la involució * és positiva respecte a la traça reduïda $tr_{B/\mathbb{Q}}$, és a dir, $tr_{B/\mathbb{Q}}(\beta \cdot \beta^*) > 0$, per tot $\beta \in B$.

Donada la data inicial (B, $\mathcal{O}$, $\Psi : B \hookrightarrow \mathrm{M}(2, \mathbb{R})$, $b \to b^*$), volem trobar xarxes $\Lambda \subset \mathbb{C}$ tals que:

i) Existeix una forma bilineal alternada $E_\Lambda : \Lambda \times \Lambda \to \mathbb{Z}$ tal que E_Λ és la part imaginària Im H d'una forma hermítica definida positiva $H_\Lambda : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}$.

ii) Existeix una immersió $i : \mathcal{O} \subset \mathrm{End}(\Lambda)$

La primera condició garanteix que $\mathbb{C}^2/\Lambda$ és una superfície abeliana polaritzada amb la forma de Riemann E_Λ. La segona condició fa que $\mathbb{C}^2/\Lambda$ tingui QM. De fet, veurem que la tripleta ($\mathbb{C}^2/\Lambda$, i, E_Λ) és, segons la convenció que hem adoptat, una *superfície abeliana polaritzada amb multiplicació quaterniònica sobre* $\mathbb{C}$.

Sigui $\tau \in \mathcal{H} = \{a + bi, a \in \mathbb{R}, b \in \mathbb{R}_{>0}\}$. Construirem una xarxa Λ_τ com la que volem per a cada element τ en el semiplà superior de Poincaré. El mètode és similar a la construcció clàssica $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ de corbes el·líptiques sobre $\mathbb{C}$. Observem primer de tot que la immersió $\Psi : B \hookrightarrow \mathrm{M}(2, \mathbb{R})$ indueix una acció natural de l'ordre d'enters maximal $\mathcal{O}$ en $\mathbb{C}^2$: $\forall \beta \in \mathcal{O}$, $v = \binom{v_1}{v_2} \in \mathbb{C}^2$, $\beta(v) = \Psi(\beta)(v)$ és el producte natural d'una matriu per un vector.

2.2.1 Definició. $\Lambda_\tau := \mathcal{O}\binom{\tau}{1} = \{v \in \mathbb{C}^2$ tals que existeix $\beta \in \mathcal{O}$ amb $v = \beta(v)\}$.

Notem que Λ_τ és una xarxa completa de $\mathbb{C}^2$ degut a què $\mathcal{O}$ és un $\mathbb{Z}$-mòdul de rang 4.

A més, la multiplicació per l'esquerra indueix una acció natural d'$\mathcal{O}$ en Λ_τ sense punts fixos i per tant una immersió $i_\tau : \mathcal{O} \hookrightarrow$

$\mathrm{End}(\Lambda_\tau)$. Aquesta xarxa admet la següent forma de Riemann:

$$\begin{aligned} E_\tau : \ \mathcal{O}\tbinom{\tau}{1} \times \mathcal{O}\tbinom{\tau}{1} &\to \mathbb{Z} \\ (\alpha\tbinom{\tau}{1}, \beta\tbinom{\tau}{1}) &\mapsto \mathrm{tr}(\mu\alpha\bar{\beta}) \end{aligned}$$

per a tot α, $\beta \in \mathcal{O}$.

Així, Λ_τ i E_τ defineixen la varietat abeliana complexa polaritzada $(A_\tau = \mathbb{C}^2/\Lambda_\tau,\ E_\tau)$. De fet, és un resultat de Jordan [Jor81] que E_τ és la forma de Riemann d'una polarització *principal* d'A_τ, és a dir, E_τ indueix un isomorfisme $A_\tau \cong \hat{A}_\tau$ entre A_τ i la varietat abeliana dual $\hat{A}_\tau$.

D'altra banda, la polarització principal E_τ defineix la (anti-)involució de Rosati $*_E$ en $\mathrm{End}^0(A)$ ([GL00]) i per tant restringeix a una involució en B via la immersió $\Psi : B \hookrightarrow \mathrm{End}^0(A)$. Perquè $(A_\tau = \mathbb{C}^2/\Lambda_\tau,\ i_\tau,\ E_\tau)$ sigui una superfície abeliana polaritzada amb QM, tan sols resta comprovar que les dues involucions $b \to b^* = \mu^{-1}\bar{b}\mu$ i $*_E$ coincideixen en B.

Ho recollim tot plegat en el següent teorema fonamental per a la interpretació modular de les corbes de Shimura.

2.2.2 Teorema. *1.* (**Shimura**) *$A_\tau = \mathbb{C}^2/\Lambda_\tau$, i_τ, E_τ és una superficie abeliana principalment polaritzada amb QM. En particular, $* = *_E : B \to B$.*

2. (**Milne**) *$E = E_\tau$ és l'*única *polarització principal tal que la involució de Rosati $*_E$ coincideix amb la involució positiva $*$.*

3. (**Shimura**) *Sigui $(A,\ i,\ E)$ una superfície principalment polaritzada amb QM per la data $(B,\ \mathcal{O},\ \Psi : B \hookrightarrow \mathrm{M}(2,\mathbb{R}),\ b \to b^*)$. Aleshores existeix un element del semiplà superior $\tau \in \mathcal{H}$ tal que $(A,\ i,\ E) \cong (A_\tau,\ i_\tau,\ E_\tau)$.*

4. (**Shimura**) *Siguin $\tau_1,\ \tau_2 \in \mathcal{H}$. Aleshores $(A_{\tau_1},\ i_{\tau_1},\ E_\tau) \cong (A_{\tau_2},\ i_{\tau_2},\ E_{\tau_2}) \quad \Leftrightarrow$ existeix $\gamma \in \Gamma(D,1) = \mathcal{O}^1 := \{\gamma \in \mathcal{O}, n(\gamma) = 1\}$ tal que $\gamma\tau_1 = \tau_2$.*

Com a conseqüència d'aquests teoremes de Shimura, podem interpretar els punts complexos de la superfície de Riemann com a classes d'isomorfisme de superfícies abelianes principalment polaritzades amb

QM per $\mathcal{O}$. Relativitzant aquest argument sobre una base arbitrària s'obté un resultat més profund:

2.2.3 Teorema. (Shimura) *Existeix una corba algebraica projectiva $X(D,1)/\mathbb{Q}$ definida sobre $\mathbb{Q}$ que resol (grollerament) el problema de moduli (sobre $\mathbb{Q}$) de classificació de superfícies abelianes principalment polaritzades amb QM per $(B,\ \mathcal{O},\ \Psi,\ b \to b^*)$.*

A més,

$$\mathcal{O}^1\backslash\mathcal{H} = X(D,1)(\mathbb{C}).$$

Aquest model racional distingit s'anomena el *model canònic de Shimura* i està caracteritzat de manera única pel fet que els punts CM o punts de Heegner en $X(D,1)/\mathbb{Q}$ generen certs cossos de classes ([Shi67], M. Alsina, capítol 7, V. Rotger, capítol 8).

Superfícies abelianes amb QM i CM sobre $\mathbb{C}$

El teorema anterior planteja la següent qüestió. Sigui $\tau \in \mathcal{H}$. Podem determinar quan (A_τ, i_τ, E_τ) té multiplicació complexa? Veurem que la resposta té una forta analogia amb el cas de les corbes el·líptiques.

La xarxa $\Lambda_\tau := \mathcal{O}\binom{\tau}{1}$ és estable per l'acció natural per l'esquerra de l'ordre de quaternions $\mathcal{O}$. Si tenim en compte les caracteritzacions que hem donat de superfícies abelianes amb QM i CM, cal estudiar el cos $K = \mathrm{End}_B^0(A_\tau/\mathbb{C})$, el commutador de B en $\mathrm{End}^0(A_\tau)$.

Pot comprovar-se que només poden donar-se dues possibilitats:

O bé $K = \mathbb{Q}$ o bé K és un cos quadràtic imaginari.

En el primer cas, $(A_\tau,\ i_\tau,\ E_\tau)$ és una superfície abeliana amb QM que *no* té CM.

En el segon cas, K és un cos quadràtic que escindeix l'àlgebra B i (A_τ, i_τ, E_τ) té multiplicació complexa per K.

Estudiem ara la qüestió des d'un altre punt de vista: sigui K un cos quadràtic imaginari que escindeix B i sigui $R_f \subset K$ un ordre d'enters de conductor f. Fixem, en cas que existeixi, una immersió optimal $j : R_f \hookrightarrow \mathcal{O}$. Això vol dir que $j(K) \cap \mathcal{O} = j(R_f) \subset B$.

Els teoremes d'Eichler (cf. [Als00a], [Vig80]) determinen completament quan existeix una immersió optimal $j : R_f \hookrightarrow \mathcal{O}$.

En composar amb $\Psi : B \hookrightarrow \mathrm{M}(2,\mathbb{R})$, obtenim una immersió $\Psi \circ j : R_f \setminus \{0\} \hookrightarrow B^* \hookrightarrow \mathrm{GL}_2^+(\mathbb{R})$. Així $R_f \setminus \{0\}$, via j, actua en el semiplà superior de Poincaré per transformacions de Möbius i pot comprovar-se que ho fa amb un únic punt fix que anomenem $\tau_{R_f,j}$.

2.2.4 Teorema. (Shimura) *1. Sigui $j : R_f \hookrightarrow \mathcal{O}$ una immersió optimal i sigui $\tau = \tau_{R_f,j} \in \mathcal{H}$ l'únic punt fix de (R_f, j) tal com hem descrit abans. Aleshores $\mathrm{End}_B^0(A_\tau) = K$, $\mathrm{End}_{\mathcal{O}}(A_\tau) = R_f$ i per tant $(A_\tau,\, i_\tau,\, E_\tau)$ és una superfície abeliana principalment polaritzada amb QM per $\mathcal{O}$ i CM per R_f.*

2. Siguin $j_1, j_2 : R_f \hookrightarrow \mathcal{O}$ immersions optimals. Obtenim els mateixos punts fixos $\tau_1 = \tau_{R_f,j_1} = \tau_2 = \tau_{R_f,j_2}$ si i només si existeix una unitat $u \in \mathcal{O}^*$ tal que $j_1 = u \cdot j_2 \cdot u^{-1}$.

3. Sigui $(A,\, i,\, E)$ una superfície abeliana principalment polaritzada amb QM i CM per un ordre quadràtic $R_f \subset K$. Aleshores existeix una immersió optimal $j : R_f \hookrightarrow \mathcal{O}$ tal que $(A,\, i,\, E) \cong (A_\tau,\, i_\tau,\, E_\tau)$ on $\tau = \tau_{R_f,j}$.

Aquest teorema dóna una descripció exhaustiva de les superfícies abelianes amb QM i CM sobre el cos dels nombres complexos. Tenint en compte la interpretació modular que hem comentat anteriorment, aquestes superfícies corresponen a punts especials en la corba de Shimura $X(D,1)$. Aquests punts s'anomenen punts de multiplicació complexa o punts de Heegner. El conjunt de punts de multiplicació complexa per un ordre quadràtic R_f en $X(D,1)$ es denota $\mathrm{CM}(R_f)$.

Si no existeixen immersions optimals de R_f en $\mathcal{O}$ aleshores es té que $\mathrm{CM}(R_f) = \emptyset$. Donat un ordre quadràtic R_f podem preguntarnos quin és el cardinal de $\mathrm{CM}(R_f)$. En el cas clàssic de les corbes el·líptiques sabem que $\mathrm{card}(\mathrm{CM}(R_f)) = h(R_f)$, on $h(R_f)$ denota el nombre de classes de l'ordre R_f. Cal esperar doncs una fórmula similar en el nostre cas.

Pel teorema anterior, hi ha tants punts de multiplicació complexa per R_f en $X(D,1)$ com classes de $\mathcal{O}^*$-conjugació d'immersions optimals $j : R_f \hookrightarrow \mathcal{O}$. Les fórmules d'Eichler ([Als00a], [Vig80]) compten

aquestes classes d'immersions, que sempre n'hi ha en un nombre finit.

En el cas més senzill, quan el conductor de l'ordre quadràtic és trivial ($f = 1$), obtenim el següent resultat.

2.2.5 Teorema. (Eichler)

$$\mathrm{cardCM}(R_K) = h(R_K) \cdot \prod_{p|D} \left(1 - \left(\frac{\mathrm{disc}(R_K)}{p}\right)\right).$$

Observem que quan $D = 1$, $\mathrm{CM}(R_K) = h(R_K)$, tal com calia esperar del fet que $X(1,1) = \mathbb{C}j$ és la recta afí j.

2.3 Superfícies abelianes amb multiplicació quaterniònica sobre un cos finit

En aquesta secció estudiem superfícies abelianes amb QM definides sobre un cos finit $k = \mathbb{F}_q$, on $q = p^r$ és la potència d'un nombre primer p. Aquestes superfícies poden interpretar-se com els punts sobre cossos finits de la reducció mod p del model de Morita-Drinfeld de les corbes de Shimura $X(D,1)$.

Sigui A/k una superfície abeliana tal que $\mathrm{End}_k^0(A)$ conté una àlgebra de quaternions B indefinida de discriminant $D = \Pi_{i=1}^{2r} p_i$.

El fet que $B \subset \mathrm{End}_k^0(A)$ imposa moltes restriccions en l'àlgebra $\mathrm{End}_k^0(A)$. El teorema de classificació d'àlgebres d'endomorfismes de varietats abelianes que hem donat a la primera secció, juntament amb els teoremes de Tate sobre varietats abelianes sobre cossos finits, conclouen que tan sols tenim tres possibilitats:

1. A és k-simple i $\mathrm{End}_k^0(A)$ és una àlgebra de quaternions de centre un cos quadràtic imaginari K. En aquest cas, tenint en compte els teoremes de Tate, podem assegurar que p descompon totalment en K i l'àlgebra de quaternions $\mathrm{End}_k^0(A)$ ramifica exactament en els dos primers $\wp$, $\bar{\wp}$ a sobre de p.
2. A/k és k-isògena al quadrat $E^2 = E \times E$ d'una corba el·líptica E/k ordinària i per tant $\mathrm{End}_k^0(A) \cong \mathrm{M}(2,K)$ on K és un cos quadràtic imaginari.

3. A/k és k-isògena al quadrat $E^2 = E \times E$ d'una corba el·líptica E/k supersingular i per tant $\mathrm{End}_k^0(A) \cong \mathrm{M}(2, D_p)$ on D_p és l'àlgebra de quaternions definida sobre $\mathbb{Q}$ ramificada en p i ∞.

En el primer cas, tot i que A és k-simple, descompon també com el quadrat d'una corba el·líptica sobre una extensió finita de k.

Denotem $\pi_A \in \mathrm{End}_k^0(A)$ l'endomorfisme de Frobenius de A/k. Sigui ℓ un primer diferent de $p =$car k. Weil va provar que l'acció de π_A en el mòdul de Tate $T_\ell(A)$ té per polinomi característic $f_A = det(\pi_A - tId)$ un polinomi mònic de grau $2g$ que té tots els seus coeficients enters i no depèn del nombre primer ℓ triat.

En qualsevol cas, el centre d'$\mathrm{End}_k^0(A)$ és sempre un cos quadràtic imaginari (casos 1 i 2) o bé el cos dels nombres racionals $\mathbb{Q}$ (cas 3). Sabem (Tate) que $\mathbb{Q}(\pi_A) =$ centre $(\mathrm{End}_k^0(A))$ i per tant $f_A = (f_A^0)^2$ per a algun polinomi $f_a^0 \in \mathbb{Z}[t]$ de grau 2. De fet, degut a les conjectures de Weil, podem assegurar que $f_a^0 = t^2 + at \pm q$ on $a \in \mathbb{Z}$, $-2\sqrt{q} \leq a \leq 2\sqrt{q}$.

Hi ha una forta relació entre el polinomi característic $f_A = (f_A^0)^2$ i l'àlgebra d'endomorfismes $\mathrm{End}_k^0(A)$. Aquesta relació l'estableix la teoria d'Honda-Tate que en el nostre cas es tradueix en el següent teorema (cf. [Jor86]). Donada A/k una varietat abeliana sobre k, notem A^0 la classe de k-isogènia d'A.

2.3.1 Teorema. (Honda-Tate) *Considerem d'una banda el conjunt de classes de k-isogènia de superfícies abelianes tals que* $\mathrm{End}_k^0(A)$ *conté una àlgebra de quaternions racional indefinida.*

D'altra, considerem el conjunt format pels polinomis quadràtics $t^2 + at + q \in \mathbb{Z}[t]$ amb $q = p^r$, $a \in \mathbb{Z}$, $-2\sqrt{q} \leq a \leq 2\sqrt{q}$ que satisfan alguna de les següents condicions:

1. $(a, p) = 1$.
2. $a = 0$.
3. *r és parell i* $a = \pm\sqrt{q}$, $a = \pm 2\sqrt{q}$.
4. *r és senar i* $p = 2$ *o* 3, $a = \pm^{r+1/2}$.

Aleshores, la correspondència $A^0 \longleftrightarrow f_A^0$ *és una correspondència bijectiva entre aquests dos conjunts. En cada cas, pot precisar-se quina és l'àlgebra d'endomorfismes* $\mathrm{End}_k^0(A)$*:*

1. $\mathrm{End}_k^0(A) = \mathrm{M}(2, \mathbb{Q}(\sqrt{a^2 - 4q}))$.
2. *Si* r *és parell,* $p = 2$ *o* $p \equiv 3(mod 4)$: $\mathrm{End}_k^0(A) = \mathrm{M}(2, \mathbb{Q}(i))$. *Si* r *és parell,* $p \equiv 1(mod\ 4)$: $\mathrm{End}_k^0(A) =$ *àlgebra de quaternions sobre* $\mathbb{Q}(i)$ *ramificada exactament als dos primers a sobre de* p*. Si* r *és senar,* $\mathrm{End}_k^0(A) = \mathrm{M}(2, \mathbb{Q}(\sqrt{-p}))$.
3. *Si* $a = \pm 2\sqrt{q}$, $\mathrm{End}_k^0(A) = \mathrm{M}(2, D_p)$. *Si* $a = \pm\sqrt{q}$, $p = 3$ *o* $p \equiv 2(mod 3)$: $\mathrm{End}_k^0(A) = \mathrm{M}(2, \mathbb{Q}(\sqrt{-3}))$. *I si* $p \equiv 1(mod 3)$: $\mathrm{End}_k^0(A)$ *és l'àlgebra de quaternions sobre* $\mathbb{Q}(\sqrt{-3})$ *ramificada als primers a sobre de* p*.*
4. *Si* $p = 2$: $\mathrm{End}_k^0(A) = \mathrm{M}(2, \mathbb{Q}(i))$. *Si* $p = 3$: $\mathrm{End}_k^0(A) = \mathrm{M}(2, \mathbb{Q}(\sqrt{-3}))$.

2.3.2 Observació. Sigui p un nombre primer. L'invariant de Hasse d'una superfície abeliana A definida sobre un cos k de característica p és $i(A) = \dim_{\mathbb{F}_p}(A[p])$, que pot ser 0, 1 o 2. No varia en fer extensions del cos on la superfície A està definida i també és invariant per isogènies.

Dels resultats anteriors observem que si la superfície A té multiplicació quaterniònica, aleshores $i(A) = 0$ o 2. En el primer cas A és $\bar{k}$-isògena al quadrat d'una corba el·líptica supersingular i direm que A és supersingular. En el segon cas A és k-isògena al quadrat d'una corba el·líptica ordinària i es diu que A és ordinària.

2.3.3 Observació. Si A/k té multiplicació quaterniònica per una àlgebra de quaternions B de discriminant D, pot comprovar-se que si $p = \mathrm{car}\ k \mid D$, aleshores A és supersingular (cf. [Jor81]).

2.4 Superfícies abelianes amb multiplicació quaterniònica sobre un cos de nombres

Cossos de definició i cossos de moduli

Les superfícies abelianes amb multiplicació quaterniònica definides sobre un cos de nombres poden interpretar-se com a punts racionals en les corbes de Shimura.

Sigui (A, i, L) una superfície abeliana polaritzada amb QM sobre un cos de nombres $k \subset \bar{\mathbb{Q}}$, on $\bar{\mathbb{Q}}$ és una clausura algebraica fixada de $\mathbb{Q}$. Diem que (A, i, L) admet un model sobre un cos $k' \subset \bar{\mathbb{Q}}$ si existeix (A', i', L') una superfície abeliana polaritzada amb QM sobre k' tal que és $\bar{\mathbb{Q}}$-isomorfa a (A, i, L).

2.4.1 Definició. Sigui (A, i, L) una superfície abeliana polaritzada amb QM sobre k. El cos de moduli k_0 de $(A,\ i,\ L)$ és el mínim subcòs de k tal que per tot $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$, $(A^\sigma,\ i^\sigma,\ L^\sigma)$ és isomorfa sobre $\bar{\mathbb{Q}}$ a (A, i, L).

En altres paraules, sigui $H \subset \mathrm{Gal}(k/\mathbb{Q})$ el subgrup format pels elements $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ tals que $(A^\sigma,\ i^\sigma,\ L^\sigma)$ és isomorfa sobre $\bar{\mathbb{Q}}$ a $(A,\ i,\ L)$. Aleshores el cos de moduli k_0 és el subcòs de k fix per H.

Si $P \in X(D,1)(\overline{\mathbb{Q}})$ denota el punt en la corba de Shimura associat a una superfície $(A,\ i,\ L)$, el cos de moduli k_0 és el cos de nombres $\mathbb{Q}(P)$ que generen les coordenades de P en el model canònic de Shimura $X(D,1)/\mathbb{Q}$. És a dir: $\mathbb{Q}(P) = k_0$.

No sempre existeix un model de la superfície abeliana polaritzada amb QM $(A,\ i,\ L)$ sobre el seu cos de moduli k_0. En qualsevol cas, k_0 sempre està contingut en els possibles cossos de definició de la superfície. Jordan [Jor86] va estudiar aquest problema i va obtenir el següent

2.4.2 Teorema. (Jordan) *Sigui k un cos de característica 0 que conté el cos de moduli k_0 d'una superfície abeliana polaritzada $(A,\ i,\ L)$ amb QM per una àlgebra de quaternions B. Aleshores $(A,\ i,\ L)$ admet un model sobre k si i només si k escindeix B.*

Exemples:

1. Si A és una corba el·líptica definida sobre un cos k, aleshores el cos de moduli 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 la interpretació modular de Shimura de la corba $S_{\mathbb{Q}}$:

$$S_{\mathbb{Q}}(k_0) \longleftrightarrow \{(A, i, L) \text{ amb cos de moduli } k_0\}$$

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 amb multiplicació quaterniònica (A,ι,L) amb $\mathbb{Q}(\sqrt{-7})$ com a cos de moduli.

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 $B(6)$.

Representacions de Galois sobre la torsió de les superfícies abelianes amb QM

Sigui $(A,\ i,\ L)$ definida sobre un cos de nombres k. Per cada primer ℓ, el grup de Galois absolut $\mathrm{Gal}(\overline{k}/k)$ actua sobre la ℓ-torsió $A[\ell]$ de la superfície abeliana A. Ho fa de manera compatible amb els morfismes naturals $A[\ell^{n+1}] \xrightarrow{\cdot\ell} A[\ell^n]$ i per tant $\mathrm{Gal}(\overline{k}/k)$ descriu una acció contínua sobre el mòdul de Tate $T_\ell(A)$. D'aquesta manera s'indueix una representació:

$$\rho_\ell : \mathrm{Gal}(\overline{k}/k) \to GL_4(\mathbb{Z}_\ell).$$

D'altra banda A també té multiplicació quaterniònica definida sobre k: $\mathcal{O} \hookrightarrow \mathrm{End}_k(A)$. Això indueix una representació de l'ordre maximal de quaternions

$$i_\ell : \mathcal{O} \hookrightarrow \mathrm{End}_k(T_\ell(A)).$$

L'acció de $\mathrm{Gal}(\overline{k}/k)$ sobre $T_\ell(A))$ ha de commutar amb la d'$\mathcal{O}$:

$$\rho_\ell : G(\overline{k}/k) \to \mathrm{Aut}_{\mathcal{O}}(T_\ell(A))$$

on $\mathrm{Aut}_{\mathcal{O}}(T_\ell(A)) \cong$

$$\cong \{\alpha \in \mathrm{GL}_4(\mathbb{Z}_\ell) \text{ tals que } \alpha\beta = \beta\alpha \text{ per a tot } \beta \in \mathcal{O}\} \cong (\mathcal{O} \otimes \mathbb{Z}_\ell)^*.$$

Notem $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$. Obtenim aleshores una representació natural

$$\rho_\ell : \mathrm{Gal}(\overline{k}/k) \to \mathcal{O}_\ell^*$$

Notem que l'isomorfisme $\mathrm{End}_{\mathcal{O}}(T_\ell(A)) \cong \mathcal{O}_\ell^*$ s'obté aplicant el teorema de bicommutativitat citat anteriorment aplicat a l'isomorfisme de $\mathbb{Z}_\ell$-mòduls $\mathcal{O}_\ell \otimes \mathcal{O}_\ell \cong \mathrm{M}(4, \mathbb{Z}_\ell)$.

Aquesta representació del grup de Galois absolut en el grup d'unitats de l'ordre maximal és molt coneguda quan especialitzem a l'àlgebra de quaternions $B = \mathrm{M}(2, \mathbb{Q})$ de discriminant 1. En aquest cas les superfícies abelianes amb multiplicació per l'ordre maximal d'enters $\mathrm{M}(2, \mathbb{Z})$ són isomorfes al quadrat d'una corba el·líptica: $A = E^2$. Si E és definida sobre el cos k, aleshores la tripleta natural $(E^2, i : \mathrm{M}(2, \mathbb{Z}) \hookrightarrow \mathrm{End}_k(E^2), L^{\otimes 2})$, on L és l'única polarització principal en E, també és definida sobre k.

En aquest cas, la representació de Galois que obtenim és la representació clàssica del grup de Galois actuant en el mòdul de Tate de la corba el·líptica E:

$$\rho_\ell : \mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

Recordem els teoremes de Serre que estudien la imatge d'aquestes representacions en el cas clàssic de les corbes el·líptiques:

2.4.3 Teorema. (Serre, Deuring) *Sigui E una corba el·líptica definida sobre un cos de nombres k.*

1. *Si E no té multiplicació complexa, aleshores la imatge de la representació*
$$\rho : \mathrm{Gal}(\overline{k}/k) \to \Pi_\ell \, \mathrm{GL}_2(\mathbb{Z}_\ell)$$
és un obert dens per la topologia ℓ-àdica, és a dir, un subgrup d'índex finit.

2. *Si E té multiplicació complexa, aleshores la imatge de la representació ρ és subgrup abelià de $\Pi_\ell \, \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Ohta [Oht74], tal com suggereix (però no publica) Serre, demostra que la situació és molt semblant en el cas general d'una superfície

abeliana amb QM no necessàriament simple. Pot considerar-se com una altra motivació per anomenar aquestes superfícies *falses corbes el·líptiques*.

2.4.4 Teorema. (Ohta) *Sigui* $(A,\ i : \mathcal{O} \hookrightarrow \mathrm{End}_k(A),\ L)$ *definida sobre un cos de nombres* k*. Per simplicitat suposarem que* $\mathcal{O}$ *és un ordre (maximal) en una àlgebra de quaternions de divisió, és a dir,* $disc(B) \neq 1$*. Aquest cas ja està cobert pels teoremes de Serre anteriors.*

Aleshores:

1. *Si* A *no té multiplicació complexa (és a dir* A *és* k*-simple o, equivalentment, el monomorfisme* i *és un isomorfisme (cf. teorema 2.0.3)), aleshores la imatge de la representació*

$$\rho : \mathrm{Gal}(\overline{k}/k) \to \Pi_\ell \mathcal{O}_\ell^*$$

és un obert dens per la topologia ℓ*-àdica, és a dir, un subgrup d'índex finit.*

En altres paraules, les representacions $\rho_\ell : \mathrm{Gal}(\overline{k}/k) \to \mathcal{O}_\ell^*$ *són exhaustives llevat d'un nombre finit de primers, on la imatge pot ser un subgrup d'índex finit.*

2. *Si* A *té multiplicació complexa (és a dir,* A *és* k*-isògena al producte de dues corbes el·líptiques o, equivalentment, i és una inclusió estricta), aleshores la imatge de la representació* ρ *és subgrup abelià de* $\Pi_\ell \mathcal{O}_\ell^*$*.*

Reducció d'una superfície abeliana amb QM

Finalment, exposem breument uns resultats sobre la reducció de les superfícies abelianes amb multiplicació quaterniònica.

2.4.5 Teorema. (de la bona reducció potencial) *Sigui* $(A,\ i,\ L)$ *una superfície abeliana polaritzada amb QM sobre un cos de nombres* k*. Aleshores existeix una extensió finita* L/k *sobre la qual* A *té bona reducció en tots els primers.*

Molt breument, la idea de la demostració és la següent: pel teorema de la reducció semiestable de Grothendieck, existeix una extensió finita L/k on la superfície abeliana A té reducció semiestable. Si A no tingués bona reducció en totes les places de L, aleshores la reducció del model de Néron de A sobre una plaça de mala reducció descompondria en una part tòrica no trivial i una part abeliana. Però això és incompatible amb l'acció quaterniònica que pressuposem en A.

Com a corol·lari dels resultats de la secció anterior sobre cossos finits obtenim el següent

2.4.6 Teorema. *Sigui (A, i, L) definida sobre un cos de nombres k. Sigui v una plaça finita de k de bona reducció d'A. Posem $k_v = \mathbb{F}_q$. Aleshores la superfície abeliana reduïda A_v/k_v descompon (sobre $\overline{k_v}$) en el producte de dues corbes el·líptiques.*

De fet pot precisar-se que si v és una plaça ordinària (i aquesta és la situació més habitual) aleshores la descomposició es produeix sobre k_v. Si v és una plaça supersingular, es pot assegurar que es produeix sobre $\mathbb{F}_{q^{12}}$.

Es produeix el fenomen curiós que A sovint és absolutament simple (aquest és el cas genèric si $\mathrm{disc}(B) \neq 1$) però totes les reduccions descomponen. Això dóna una altra motivació per a anomenar les superfícies abelianes amb QM *falses corbes el·líptiques*.

Bibliografia

[Als00a] M. Alsina, *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura*, Tesi doctoral, Publ. Universitat de Barcelona, 2000.

[BL92] C. Birkenhake, H. Lange, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer, 1992.

[GL00] J. Guàrdia, J. C. Lario (eds.), *Varietats abelianes amb multiplicació complexa*, Notes del Seminari de teoria de nombres (UB-UAB-UPC), vol. 6, STNB, Barcelona, 2000.

[JL85] B. Jordan, R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985), num. 2, 235–248.

[Jor81] B. Jordan, *On the diophantine arithmetic of Shimura curves*, Tesi doctoral, Harvard University, 1981.

[Jor86] B.W. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92-114.

[Mil79] J. Milne, *Points on Shimura varieties mod p*, Automorphic forms, representations and L-functions, Proc. XXXII Sympos. Pure Math. (1977), Amer. Math. Soc., 1979, pp. 165–184.

[Mor92] A. Mori, *Explicit period matrices of abelian surfaces with quaternionic multiplications*, Boll. Un. Mat. Ital. A (7) **6** (1992), num. 2, 197–208.

[Mum70] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research, Bombay, Oxford University Press, 1970.

[Oht74] M. Ohta, *On ℓ-adic representations of Galois groups obtained from certain two dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo **21** (1974), 299–308.

[Shi63c] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. **78** (1963), num. 1, 149–192.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

[ST61] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[ST68] J-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[Vig80] M-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., num. 800, Springer, 1980.

Capítol 3

Uniformització p-àdica de corbes de Shimura

X. Xarles

Introducció

Les idees per investigar la versió p-àdica de la uniformització clàssica (sobre $\mathbb{C}$) de les corbes van començar amb el treball de John Tate [Tat71] del 1962 (treball que no va ser publicat fins al 1971), on va demostrar que les corbes el·líptiques sobre un cos p-àdic amb reducció multiplicativa *split* poden ser uniformitzades analíticament pel grup multiplicatiu si s'utilitza una noció adequada de geometria analítica p-àdica, la geometria analítica rígida. D'altra banda, les corbes el·líptiques amb bona reducció no poden en principi ser p-àdicament uniformitzades, ja que són simplement connexes (com a varietats rígides analítiques).

El 1972, David Mumford [Mum72] va aconseguir estendre el resultat de Tate a les corbes de gènere més gran que 1. Com en el cas complex, l'espai uniformitzador passa a ser el "semiplà superior de Poincaré p-àdic", i el "grup fonamental"ja no és un grup abelià discret sinó un cert subgrup del grup de les matrius 2×2. D'altra banda, com en el cas de les corbes el·líptiques, no totes les corbes poden ser p-àdicament uniformitzades: sols les que tenen reducció "total-

ment degenerada *split*", anomenades actualment corbes de Mumford. De fet, Mumford no va utilitzar el llenguatge de la geometria rígida analítica, sinó el llenguatge equivalent de la geometria formal; posteriorment L. Gerritzen i M. van der Put [GvdP80] van traduir aquests resultats a la geometria rígida analítica i van estendre els resultats a qualsevol cos complet respecte a un valor absolut no arquimedià.

El 1976, I. V. Čerednik [Čer76] va observar que les corbes de Shimura amb discriminant múltiple de p són de fet corbes de Mumford (sobre una certa extensió finita de $\mathbb{Q}_p$), i va construir explícitament (en funció de l'àlgebra de quaternions) aquesta uniformització. El mateix any 1976, V. G. Drinfeld [Dri76] va aclarir i millorar aquests resultats de Čerednik dotant d'una interpretació de moduli al semiplà superior de Poincaré p-àdic. A la vegada va donar una formulació de la uniformització p-àdica però ara sobre $\mathbb{Q}_p$, perfectament anàloga a la uniformització complexa.

En aquesta presentació farem una breu ullada a tots aquests resultats, des de les corbes de Mumford i la seva uniformització rígida analítica, el semiplà superior de Poincaré p-àdic i formal juntament amb la seva interpretació de moduli, i, finalment, la uniformització de les corbes de Shimura.

3.1 Corbes de Mumford

Sigui K un cos complet respecte a una valoració discreta, i sigui $C = \widehat{\overline{K}}$ la completació de la clausura algebraica de K. Sigui R l'anell d'enters de K, k el cos residual de R, π un uniformitzant de R i $|\ \ |$ el valor absolut de K i la seva extensió a C.

3.1.1 Definició. Una corba $\mathcal{X}$ sobre R amb fibra genèrica llisa i projectiva s'anomena *estable* si és pròpia i plana sobre R i la seva fibra sobre k és geomètricament reduïda, connexa, amb singularitats que siguin punts dobles ordinaris i tal que cada component racional interseca les altres en, com a màxim, tres punts (fet que implica que el gènere de $\mathcal{X}$ és més gran que 1).

Una corba estable $\mathcal{X}$ sobre R té reducció totalment degenerada *split* si tots els components de (la normalització de) la seva reducció

són isomorfs a $\mathbb{P}^1$ i tots els punts dobles són k-racionals.

Finalment, si X és una corba irreductible, llisa i projectiva sobre K, direm que és una *corba de Mumford* si té un model estable $\mathcal{X}$ sobre R amb reducció totalment degenerada *split*.

Les corbes de Mumford són l'equivalent a les corbes el·líptiques de Tate per a gènere més gran que 1.

3.1.2 Teorema. *Sigui X una corba irreductible, llisa i projectiva sobre K. Si X és una corba de Mumford, aleshores*

1. *La jacobiana $Jac(X)$ té reducció tòrica split, o sigui que la reducció del component connex del model de Néron és isomorf a ${\mathbb{G}_m}^g$.*
2. *La jacobiana $Jac(X)$ és isomorfa com a varietat rígida analítica a ${\mathbb{G}_m}^g$ mòdul una xarxa.*
3. *Si ℓ és un nombre primer diferent de la característica de k, aleshores el primer grup de cohomologia étale verifica que*

$$\dim_{\mathbb{Q}_\ell} H^1(X_{et}, \mathbb{Q}_\ell)(1)^{G_K} = g,$$

on G_K és el grup de Galois absolut de K, i (1) és el twist de Tate (o sigui és el producte tensorial amb $\mathbb{Q}_\ell(1) := (\lim \mu_{\ell^n}(\bar{K})) \otimes \mathbb{Q}_\ell$).

A més a més, totes les condicions anteriors són equivalents.

La demostració d'aquest teorema es basa en diversos resultats: que les corbes de Mumford verifiquen 1 és conseqüència de la seva uniformització no arquimediana i es pot consultar en el llibre de Gerritzen i Van der Put [GvdP80] o bé en els articles de Bosch i Lütkebohmert [BL85] i [BL84]; que 2 i 3 són equivalents a 1 és una conseqüència de la uniformització rígida analítica de les varietats abelianes (vegeu per exemple l'article de Bosch i Lütkebohmert [BL91]).

3.1.3 Exemple. Les corbes $X_0(p)$, on p és un nombre primer, són corbes de Mumford sobre $\mathbb{Q}_{p^2}$, l'única extensió quadràtica no ramificada de $\mathbb{Q}_p$. No ho són sobre $\mathbb{Q}_p$ ja que les singularitats de la seva

reducció (per a un model adequat) són definides sobre $\mathbb{F}_{p^2}$ ja que es corresponen (via la interpretació de moduli) a certes corbes el·líptiques supersingulars que estan definides sobre $\mathbb{F}_{p^2}$.

El nostre objectiu és veure que les corbes de Mumford tenen una uniformització rígida analítica similar a la uniformització complexa. Abans cal que definim l'objecte que jugarà el paper del semiplà superior de Poincaré.

3.2 El semiplà superior no arquimedià

Com abans, sigui K un cos complet respecte a una valoració discreta, i sigui $C = \widehat{\overline{K}}$ la completació de la clausura algebraica de K. Sigui R l'anell d'enters de K, k el cos residual de R que suposarem **finit**, π un uniformitzant de R i $|\ |$ el valor absolut de K i la seva extensió a C. Molts dels resultats d'aquesta secció són vàlids amb lleugers canvis si el cos residual no és finit (vegeu la remarca 3.2.9).

3.2.1 Definició. El *semiplà superior no arquimedià* (associat a K) és el conjunt $\Omega := \mathbb{P}^1_C(C) \setminus \mathbb{P}^1_K(K) = C \setminus K$, amb l'estructura de varietat rígida analítica sobre K que definirem seguidament.

3.2.2 Observació. L'anàleg arquimedià de Ω és l'espai $\Omega := \mathbb{P}^1_{\mathbb{C}} \setminus \mathbb{P}^1_{\mathbb{R}}$; aquest espai és no connex i per això agafem normalment el semiplà superior. En el cas no arquimedià Ω és connex, i per tant ens hem de quedar amb tot Ω.

Per poder definir una estructura de varietat rígida analítica a Ω hem d'estudiar primer l'arbre de $\mathrm{PGL}(2, K)$, també anomenat arbre de Bruhat-Tits.

Anomenarem xarxa de K^2 un sub-R-mòdul lliure de K^2 de rang 2. Direm que dues xarxes M_1 i M_2 són (homotèticament) equivalents si existeix un $\lambda \in K$ tal que $M_2 = \lambda M_1$. Designarem amb la notació $[M]$ les classes mòdul homotècia de xarxes en K^2.

El graf $\mathcal{T}$ de $\mathrm{PGL}(2, K)$ és definit per les dades següents:

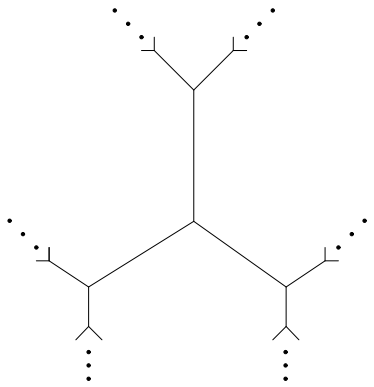

Figura 3.1: Arbre $\mathcal{T}$ per a $\mathbb{Q}_2$.

(i) els vèrtexs de $\mathcal{T}$ són les classes mòdul homotècia de xarxes de K^2.

(ii) dos vèrtexs s i s' estan units per una aresta si i només si existeixen $M_1 \in s$ i $M_2 \in s'$ tals que $\pi M_2 \subsetneq M_1 \subsetneq M_2$, o, equivalentment, $M_1/M_2 \cong k$.

3.2.3 Proposició. *El graf $\mathcal{T}$ és un arbre. Fixat un vèrtex s, tenim una correspondència entre el conjunt d'arestes amb origen s i els punts de $\mathbb{P}^1_k(k)$.*

3.2.4 Exemple. Suposem que $K = \mathbb{Q}_p$ amb $p = 2$. Aleshores cada vèrtex de l'arbre $\mathcal{T}$ té tres arestes que surten d'ell, i és infinit (però localment finit). Vegeu la figura 3.1.

3.2.5 Observació. El grup $\mathrm{PGL}(2, K)$ actua de manera natural en $\mathcal{T}$ de la manera següent. Si A és una matriu de $\mathrm{GL}(2, K)$,

(i) per a tot vèrtex $[M]$ de $\mathcal{T}$, $A[M] := [AM]$;

(ii) si tenim dos vèrtexs s i s' units per una aresta $[s, s']$, aleshores $A[s, s'] := [As, As']$.

És senzill comprovar que aquesta acció està ben definida.

Finalment observem que els "punts límit"de l'arbre $\mathcal{T}$ són els punts de $\mathbb{P}^1_K(K)$.

3.2.6 Observació. Definim *semilínies* de $\mathcal{T}$ les successions infinites de vèrtexs $\{s_n\}$ sense repetició tals que s_i està connectada a s_{i-1} per a tot i. Aleshores el conjunt de semilínies de $\mathcal{T}$ (amb la relació d'equivalència natural tal que dues semilínies son equivalents si difereixen en un nombre finit de vèrtexs) és correspon de manera natural als punts de $\mathbb{P}^1_K(K)$.

En efecte, només hem de prendre un representant M_i de s_i per a cada i i considerar el subespai $\bigcap_i M_i \otimes_R K \subset K^2$; aquest subespai ens determina el punt buscat.

Per definir una estructura d'espai rígid analític a Ω el que farem serà identificar $\mathcal{T}$ amb el graf dual de la reducció d'un cert model formal de Ω sobre R. Recordem que els espais rígids analítics són sempre la "fibra genèrica"d'esquemes formals (sota unes certes condicions de finitud). En general no tenim un model formal canònic d'un espai rígid analític; en el nostre cas, però, en construirem un.

Observem que donar una xarxa M de K^2 mòdul homotècia és equivalent a donar un esquema X sobre R isomorf a la recta projectiva $\mathbb{P}^1_R$ amb fibra genèrica $\mathbb{P}^1_K$,

$$\mathbb{P}(M) := \mathbf{Proj}(\mathrm{Sym}(\mathrm{Hom}_R(M, R))).$$

Els punts R-racionals de $\mathbb{P}(M)$ es corresponen aleshores als morfismes com a R-mòduls $M \to R$. Tenim que dues xarxes M i M' són equivalents mòdul homotècia si i només si l'isomorfisme canònic entre les fibres genèriques de $\mathbb{P}(M)$ i $\mathbb{P}(M')$ puja a un isomorfisme entre $\mathbb{P}(M)$ i $\mathbb{P}(M')$.

Ara, donada una aresta $[s, s']$ de $\mathcal{T}$, escollim $M \in s$ i $M' \in s'$ tal que $\pi M \subsetneq M' \subsetneq M$. Els morfismes exhaustius $M \to M/M' \cong k$ i $M' \to M'/\pi M \cong k$ ens determinen punts $p \in \mathbb{P}(M)$ i $p' \in \mathbb{P}(M')$. Considerem l'esclatament (*blowing up*) $B_p(\mathbb{P}(M))$ de $\mathbb{P}(M)$ en el punt p i igualment $B_{p'}(\mathbb{P}(M'))$; aquests dos esquemes són canònicament isomorfs i el designarem mitjançant $\mathbb{P}(M, M')$.

3.2.7 Observació. La fibra en k de l'esquema $\mathbb{P}(M, M')$ és isomorfa a dues rectes projectives que es tallen en un punt.

3.2.8 Observació. Es pot donar una descripció més explícita de $\mathbb{P}(M, M')$ de la següent forma: si escollim com abans $M \in s$ i $M' \in s'$ tal que $\pi M \subsetneq M' \subsetneq M$ i prenem e_0, e_1 una base de M tal que e_0, πe_1 sigui una base de M', aleshores tenim que

$$\mathbb{P}(M) \cong \mathbf{Proj}(R[X_0, X_1]))$$

$$\mathbb{P}(M') \cong \mathbf{Proj}(R[Y_0, Y_1])$$

$$\mathbb{P}(M, M') \cong \text{ la clausura de } Y_0X_1 - \pi X_0Y_1 = 0 \text{ a}$$

$$\mathbf{Proj}(R[X_0Y_0, X_0Y_1, X_1Y_0, X_1Y_1]),$$

on $X_i : M \to R$ donats per $X_i(e_j) = \delta_{ij}$, i $Y_i : M \to R$ donats per $Y_i(e_0) = \delta_{i0}$ i $Y_i(\pi e_1) = \delta_{i1}$.

Ara, donat un vèrtex s de $\mathcal{T}$, sigui Ω_s l'esquema $\mathbb{P}(M) \setminus \mathbb{P}(M)(k)$ i $\widehat{\Omega_s}$ la completació de Ω_s al llarg de la fibra tancada. I, donada una aresta $[s, s']$ designarem mitjançant $\Omega_{[s,s']}$ l'esquema $\mathbb{P}(M, M')$ menys els seus punts k-racionals i mitjançant $\widehat{\Omega_{[s,s']}}$ la seva completació al llarg de la fibra tancada.

Tenim que els esquemes formals $\widehat{\Omega_s}$ i $\widehat{\Omega_{s'}}$ són de manera natural subesquemes formals oberts de $\widehat{\Omega_{[s,s']}}$. Això ens permet d'anar enganxant els diferents esquemes formals $\widehat{\Omega_{[s,s']}}$ per a totes les arestes de $\mathcal{T}$ fins a obtenir l'esquema formal $\widehat{\Omega}$.

3.2.9 Remarca. De fet aquest procediment no el podem fer a menys que l'arbre $\mathcal{T}$ sigui localment finit, o sigui que a cada vèrtex li arriben sols un nombre finit d'arestes. Per exemple, si el cos residual k és finit, aleshores $\mathcal{T}$ és localment finit.

En el cas que el nostre cos residual no és finit, l'únic que podem aconseguir és construir un semiplà superior de Poincaré no arquimedià per a qualsevol subarbre localment finit.

3.2.10 Observació. La fibra especial de $\widehat{\Omega}$ és l'arbre de rectes projectives sobre k intersecant-se en els punts k-racionals. El seu graf associat és $\mathcal{T}$ (o sigui que $\mathcal{T}$ és el graf dual de la fibra especial de $\widehat{\Omega}$).

Finalment ens cal veure que la fibra genèrica de $\widehat{\Omega}$ es pot identificar amb Ω. En fer-ho obtindrem de pas un recobriment per oberts afinoides de Ω que ens definirà la seva estructura rígida analítica.

Comencem per identificar qui és la fibra genèrica de $\widehat{\Omega_s}$ i de $\widehat{\Omega_{[s,s']}}$.

3.2.11 Lema. *La fibra genèrica de $\widehat{\Omega_s}$ és isomorfa al subconjunt de C*

$$\{\xi \in C \,|\, |\xi| \leq 1\} \;\setminus \bigcup_{\substack{a \in R \\ \bmod \pi R}} \{\xi \in C \,|\, |\xi - a| \leq 1\}.$$

3.2.12 Lema. *La fibra genèrica de $\widehat{\Omega_{[s,s']}}$ és isomorfa al subconjunt de C*

$$\{\xi \in C \,|\, |\xi| \leq 1\} \;\setminus \bigcup_{\substack{a \in R \\ \bmod \pi R}} \{\xi \in C \,|\, |\xi - a| < 1\}$$

$$\setminus \bigcup_{\substack{b \in \pi R \\ \bmod \pi^2 R}} \{\xi \in C \,|\, |\xi - a| < |\pi|\}$$

on la fibra genèrica de $\widehat{\Omega_s}$ s'identifica amb el conjunt definit al lema anterior i la fibra genèrica de $\widehat{\Omega_{s'}}$ s'identifica amb

$$\{\xi \in C \,|\, |\xi| \leq |\pi|\} \;\setminus \bigcup_{\substack{b \in \pi R \\ \bmod \pi^2 R}} \{\xi \in C \,|\, |\xi - a| < |\pi|\}.$$

La demostració d'aquests lemes és senzilla; per demostrar el segon cal identificar $\mathbb{P}(M, M')$ amb l'esclatament $B_p(\mathbb{P}(M))$ de $\mathbb{P}(M)$ en el punt $p : M \to M/M' \cong k$. Vegeu la figura 3.2 de l'obert del lema anterior en el cas $K = \mathbb{Q}_2$.

Tampoc és difícil de comprovar que cadascun d'aquests conjunts són varietats rígides analítiques afinoides. Podeu consultar per exemple l'excel·lent article de Boutot i Carayol [BC91].

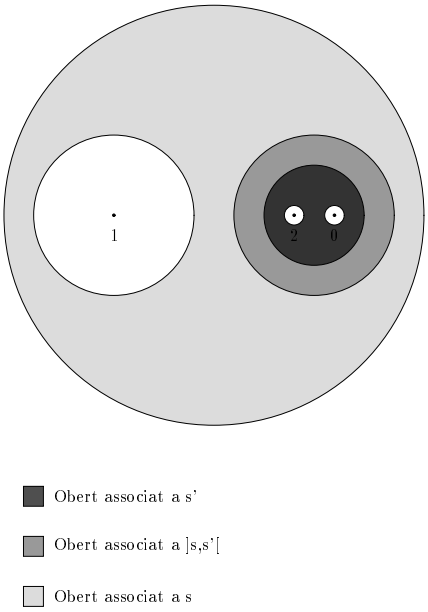

Figura 3.2: Fibra genèrica de $\widehat{\Omega_{[s,s']}}$ per a $\mathbb{Q}_2$.

Ara s'han d'identificar aquests conjunts amb subconjunts de Ω. És clar que només és necessari fer-ho per a la fibra genèrica de $\widehat{\Omega_{[s,s']}}$.

Escollim com abans $M \in s$ i $M' \in s'$ tal que $\pi M \subsetneq M' \subsetneq M$ i prenem e_1, e_2 una base de M tal que e_1, πe_2 sigui una base de M'. Aleshores $e_1 = (e_1^1, e_1^2) \in K^2$ i $e_2 = (e_2^1, e_2^2) \in K^2$, i podem identificar Ω amb $C \setminus K$ mitjançant l'aplicació que a cada $[a : b] \in \Omega = \mathbb{P}^1_C \setminus \mathbb{P}^1_K$ li associa

$$\begin{array}{rcl} \Omega & \longrightarrow & C \setminus K \\ [a:b] & \longmapsto & \frac{ae_1^1+be_1^2}{ae_2^1+be_2^2}. \end{array}$$

Utilitzem aquest morfisme per identificar la fibra genèrica de $\widehat{\Omega_{[s,s']}}$ amb un subconjunt de Ω.

3.2.13 Proposició. *La construcció anterior ens dóna un recobriment de Ω per a varietats rígides analítiques afinoides que ens determina una estructura de varietat rígida analítica sobre K de Ω.*

La reducció d'aquesta varietat respecte a aquest recobriment és el graf infinit de rectes projectives que es tallen en els seus punts k-racionals.

La demostració d'aquest fet és estàndard. Per a reduccions de varietats rígides analítiques respecte a recobriments podeu consultar el llibre [BGR84] o bé el llibre [GvdP80].

3.3 Uniformització de corbes de Mumford

Situem-nos a partir d'ara en el cas que K és una extensió finita de $\mathbb{Q}_p$; aquest és, de fet, el cas que necessitem per estudiar les corbes de Shimura i ens simplificarà alguns dels resultats. La teoria general es pot consultar per exemple en el llibre [GvdP80] o bé de forma molt resumida en l'article [Sch00].

El resultat de Mumford es basa a associar a cada corba de Mumford X — tal com les hem definit en la primera secció — un cert subgrup Γ de $\mathrm{PGL}(2, K)$ i demostrar que X és de fet isomorfa a $\Gamma\backslash\Omega'$, per a una certa subvarietat analítica rígida de Ω.

La idea és senzilla: considerem el graf associat a la reducció de X (si es vol el graf dual de la reducció de X) i el seu recobriment universal G. Es pot veure que el recobriment universal és de fet un subarbre (localment finit) $\mathcal{T}'$ de l'arbre $\mathcal{T}$ de Bruhat-Tits. El grup de transformacions Γ d'aquest recobriment universal és el grup buscat. Observeu que és un grup lliure amb g generadors, on g és el nombre de "llaços"del graf. Construïm aleshores el subespai $\Omega' := \Omega_{\mathcal{T}'}$ de Ω associat a $\mathcal{T}'$ (vegeu la remarca 3.2.9).

Tenim aleshores un morfisme recobridor de la reducció de Ω' a la reducció de X amb grup de transformacions Γ. Aquest morfisme puja a un morfisme d'esquemes formals de $\widehat{\Omega}'$ a la completació formal respecte a la fibra especial del model de X escollit, que ens dóna un isomorfisme entre aquesta completació formal i $\Gamma\backslash\widehat{\Omega}'$ Finalment aquest Γ es pot identificar amb un subgrup de $\mathrm{PGL}(2, K)$, grup de transformacions de la recta projectiva sobre K.

3.3.1 Definicions. Un subgrup Γ de $\mathrm{PGL}(2, K)$ diem que és un subgrup de Schottky si és discret, lliure de torsió i lliure amb dos o més generadors.

Donat un subgrup de Schottky Γ, sigui Σ_Γ és conjunt de punts de $\mathbb{P}^1_K$ que són fixos per algun element de Γ diferent de la identitat. Tenim que $\Sigma_\Gamma \subset \mathbb{P}^1(K)$ i que és infinit (ja que Γ té dos o més generadors).

Ara, donat un subconjunt infinit $\Sigma \subset \mathbb{P}^1(K)$, definim el subgraf $\mathcal{T}_\Sigma$ de $\mathcal{T}$ que té com a vèrtexs

$$Ver(\mathcal{T}_\Sigma) := \{[s(x_0, x_1, x_2)] \mid (x_0, x_1, x_2) \in \Sigma^3\},$$

on $[s((x_0, x_1, x_2))]$ és l'únic vèrtex de $\mathcal{T}$ intersecció de les tres semilínies associades a cada un dels x_i (vegeu 3.2.6), i com a arestes totes les arestes entre els vèrtexs donats.

Finalment, denotem per Ω_Γ el subespai rígid analític de Ω associat a l'arbre $\mathcal{T}_\Sigma$ per a $\Sigma = \Sigma_\Gamma$, i per $\widehat{\Omega_\Gamma}$ el subesquema formal de Ω associat.

El següent teorema va ser demostrat per David Mumford [Mum72].

3.3.2 Teorema. (Mumford) *Sigui K una extensió finita de $\mathbb{Q}_p$ amb anell d'enters R. Aleshores,*

(i) *Donat Γ un grup de Schottky de $\mathrm{PGL}(2,K)$ existeix una corba estable $\mathcal{X}_\Gamma$ sobre R amb reducció totalment degenerada split tal que la seva completació formal respecte a la fibra especial és isomorfa a $\Gamma\backslash\widehat{\Omega_\Gamma}$.*

(ii) *Donada una corba estable $\mathcal{X}$ sobre R amb reducció totalment degenerada split existeix un subgrup de Schottky Γ de $\mathrm{PGL}(2,K)$ i un isomorfisme entre $\mathcal{X}$ i $\mathcal{X}_\Gamma$.*

Del teorema es dedueix fàcilment la següent versió rígida analítica.

3.3.3 Teorema. *Sigui K una extensió finita de $\mathbb{Q}_p$. Aleshores*

(i) *Donat Γ un grup de Schottky de $\mathrm{PGL}(2,K)$ existeix una corba de Mumford X_Γ sobre K que és isomorfa a $\Gamma\backslash\Omega_\Gamma$ com a varietat rígida analítica.*

(ii) *Donada una corba de Mumford X sobre K existeix un subgrup de Schottky Γ de $\mathrm{PGL}(2,K)$ i un isomorfisme entre X i X_Γ.*

Per a veure una generalització a cossos complets respecte a un valor absolut no arquimedià podeu consultar [GvdP80].

3.3.4 Exemple. Ja hem dit que les corbes $X_0(p)$, on p és un nombre primer, són corbes de Mumford sobre $\mathbb{Q}_{p^2}$, l'única extensió quadràtica no ramificada de $\mathbb{Q}_p$. No es coneix, però, una interpretació aritmètica del subgrup de Schottky associat.

3.4 El teorema de Čerednik-Drinfeld

Recordem primer algunes notacions per a les corbes de Shimura (vegeu A. Rio, capítol 1, secció 8).

3.4.1 Notació. Sigui B una àlgebra de quaternions indefinida de discriminant $D > 1$, i sigui $N \geq 1$ un nombre enter coprimer amb

D. Fixem $\mathcal{O}(D,N)$ un ordre d'Eichler de conductor N a B, i $\mathcal{O}(D)$ un ordre maximal. Sigui $X(D,N)$ la corba de Shimura associada a $\mathcal{O}(D,N)$. Sabem, gràcies a Shimura, que $X(D,N)$ té un model projectiu i de tipus finit a $\mathbb{Z}[1/N]$, interpretant-la com la corba associada a un cert problema de moduli (vegeu V. Rotger, capítol 2, teorema 2.2.3 i r. Re, capítol 4).

3.4.2 Notació. Sigui $\mathbb{C}_p$ la completació de la clausura algebraica de $\mathbb{Q}_p$. Si K és una extensió finita de $\mathbb{Q}_p$, designarem mitjançant Ω_K el semiplà superior no arquimedià associat a K; o sigui,

$$\Omega_K := \mathbb{P}^1_{\mathbb{C}_p}(\mathbb{C}_p) \setminus \mathbb{P}^1_K(K),$$

amb l'estructura d'espai rígid analític definida a la secció 3.2. Per a simplificar la notació, quan $K = \mathbb{Q}_p$ utilitzarem Ω. Igualment $\widehat{\Omega_K}$ i $\widehat{\Omega}$ seran els esquemes formals associats. Finalment, designarem per $\mathbb{Q}_{p^2}$ a l'extensió quadràtica no ramificada de $\mathbb{Q}_p$.

Fixem p un primer que divideixi D (i no divideixi N), i considerem $X(D,N)$ sobre $\mathbb{Q}_p$ i sobre $\mathbb{Z}_p$. El teorema de Čerednik-Drinfeld ens diu que $X(D,N)$ és de fet una corba de Mumford sobre $\mathbb{Q}_{p^2}$, i a més ens determina quin grup de Schottky hem de prendre. De fet, el teorema ens dóna també una mena d'uniformització de $X(D,N)$ sobre $\mathbb{Q}_p$: és la torçada del quocient d'una corba de Mumford.

La idea bàsica prové de la següent construcció de Čerednik, anomenada l'intercanvi d'invariants locals.

3.4.3 Definició. Sigui B una àlgebra de quaternions indefinida de discriminant $D > 1$, i p un nombre primer dividint D. Aleshores l'àlgebra de quaternions $B^{(p)}$ obtinguda a partir de B intercanviant els invariants locals p i ∞ és l'àlgebra de quaternions definida amb discriminant D/p.

3.4.4 Lema. *Sigui $\mathcal{O}(D,N)^{(p)}$ un ordre d'Eichler de conductor N a $B^{(p)}$ (cf. Rio, capítol 1). Sigui*

$$\widetilde{\Gamma} := \mathcal{O}(D,N)^{(p)}[1/p]^* \subset (B^{(p)} \otimes \mathbb{Q}_p)^* \cong \mathrm{GL}(2,\mathbb{Q}_p)$$

i

$$\widetilde{\Gamma}_+ = \{\gamma \in \widetilde{\Gamma} \mid v_p(\det(\gamma)) \cong 0 \mod 2\}.$$

Aleshores, la imatge Γ_+ *de* $\widetilde{\Gamma}_+$ *dins de* $\mathrm{PGL}(2,\mathbb{Q}_{p^2})$ *és un subgrup de Schottky.*

Observem que Γ, la imatge de $\widetilde{\Gamma}$ a dins de $\mathrm{PGL}(2,\mathbb{Q}_p)$, no és un grup de Shottky, ja que no és lliure de torsió. Tot i així podem considerar $\Gamma\backslash\Omega$, que és una corba però no és $X(D,N)$. Per obtenir $X(D,N)$ ens cal fer una construcció una mica més elaborada.

Sigui $\mathbb{Z}_{p^\infty}$ l'anell de Witt de la clausura algebraica de $\mathbb{F}_p$ (o l'anell d'enters de la màxima extensió no ramificada de $\mathbb{Q}_p$). Considerem l'acció de Γ a $\mathbb{Z}_{p^\infty}$ donada a través del Frobenius:

$$\gamma(\lambda) = \mathrm{Frob}^{n(\gamma)}(\lambda)$$

$\forall\lambda \in \mathbb{Z}_{p^\infty}$ i $\forall\gamma \in \Gamma$, on $n(\gamma) := v_p(\det(\gamma))$ i Frob és el Frobenius de $\mathbb{Z}_{p^\infty}$.

Podem fer operar així Γ a $\widehat{\Omega}\widehat{\otimes}\mathbb{Z}_{p^\infty}$, que considerem com a esquema formal sobre $\mathbb{Z}_p$. Tenim aleshores el teorema següent.

3.4.5 Teorema. (Čerednik-Drinfeld) *La completació formal respecte a la fibra especial de la corba* $X(D,N)$ *sobre* $\mathbb{Z}_p$ *és canònicament isomorfa a l'esquema formal*

$$\Gamma\backslash\left(\widehat{\Omega}\widehat{\otimes}\mathbb{Z}_{p^\infty}\right).$$

Aquest teorema de fet es pot explicitar una mica més. Tenim que l'acció de Γ a Ω factoritza a través de Γ_+, d'on

$$\Gamma_+\backslash\left(\Omega\widehat{\otimes}\mathbb{Z}_{p^\infty}\right) \cong \left(\Gamma_+\backslash\Omega\right)\widehat{\otimes}\mathbb{Z}_{p^2}.$$

3.4.6 Corol·lari. $X(D,N)\otimes\mathbb{Q}_{p^2} \cong \Gamma_+\backslash\Omega_{\mathbb{Q}_{p^2}}$ *com a varietats rígides analítiques sobre* $\mathbb{Q}_{p^2}$.

Finalment podem veure que de fet la corba de Shimura $X(D,N)$ és una torçada de $\Gamma_+\backslash\Omega$.

3.4.7 Corol·lari. *Si designem* $W := \Gamma/\Gamma_+$, *aleshores* W *és un grup d'ordre 2, generat per* w *operant a* $\Omega_{\mathbb{Q}_{p^2}}$ *via el Frobenius, i tenim*

$$X(D,N)\otimes\mathbb{Q}_p \cong W\backslash\left(\Gamma_+\backslash\Omega_{\mathbb{Q}_{p^2}}\right).$$

Aquests dos corol·laris són conseqüències més o menys directes del teorema. Per donar una idea de com es demostra aquest teorema necessitem veure la interpretació de moduli que dóna Drinfeld del semiplà superior formal.

Ens podem preguntar com és que hem de fer el procés d'intercanviar invariants locals. Una idea sobre aquest fet ens la pot donar la següent proposició, conseqüència dels resultats de Serre i Tate sobre varietats abelianes sobre cossos finits.

3.4.8 Proposició. *Hi ha una única classe mòdul isogènia de parelles (A, i), on A és una superfície abeliana sobre $k := \overline{\mathbb{F}}_p$ i*

$$i : \mathcal{O}(D) \hookrightarrow \mathrm{End}_k(A)$$

és una acció de $\mathcal{O}(D)$ a A. A més, A és isògena al producte de dues corbes el·líptiques supersingulars.

Finalment, tenim un isomorfisme natural entre $B^{(p)}$ i

$$\mathrm{End}_{\mathcal{O}(D)}((A, i)) \otimes \mathbb{Q}.$$

Com hem dit, la demostració de Drinfeld del teorema anterior es basa en una interpretació del semiplà superior p-àdic com a espai de moduli: és essencialment l'espai de moduli dels grups formals de pes 4 amb acció quaterniònica amb certes condicions de rigidificació. O sigui, els grups formals que es comporten com el grup formal associat a la varietat abeliana determinada en la proposició anterior. Aquest és el pas més difícil de la demostració, on s'utilitzen tècniques de grups formals i de mòduls de Dieudonné (vegeu l'article [BC91] per a una exposició més detallada).

3.4.9 Teorema. (Drinfeld) *Sigui A una superfície abeliana sobre $\overline{\mathbb{F}}_p$ amb acció de $\mathcal{O}(D)$. Sigui Φ el grup formal associat a A.*

Donada una $\mathbb{Z}_{p^\infty}$-àlgebra B on p és nilpotent, designem per $F(B)$ el conjunt de classes d'isomorfisme de parelles (X, ρ) on X és un esquema formal sobre B de dimensió 2 i alçada 4 amb acció de $\mathcal{O}(D)$ i ρ és una quasi-isogènia d'alçada 0

$$\rho : \Phi_{B/pB} \to X_{B/pB}.$$

Aleshores el functor F és representat per l'esquema formal sobre $\mathbb{Z}_{p^\infty}$ donat per $\widehat{\Omega}\widehat{\otimes}\mathbb{Z}_{p^\infty}$.

Bibliografia

[BC91] J-F. Boutot, H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld*, Astérisque **196–197** (1991), 45–158, Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[BGR84] S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 261, Springer, Berlin, 1984, A systematic approach to rigid analytic geometry.

[BL84] S. Bosch, W. Lütkebohmert, *Stable reduction and uniformization of abelian varieties. II*, Invent. Math. **78** (1984), num. 2, 257–297.

[BL85] S. Bosch, W. Lütkebohmert, *Stable reduction and uniformization of abelian varieties. I*, Math. Ann. **270** (1985), num. 3, 349–379.

[BL91] S. Bosch, W. Lütkebohmert, *Degenerating abelian varieties*, Topology **30** (1991), num. 4, 653–698.

[Čer76] I. Čerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(k_w)$ *with compact quotients*, Math. USSR Sb. **29** (1976), num. 1, 55–78.

[Dri76] V. G. Drinfeld, *Coverings of p-adic symmetric regions*, Funct. Anal. Appl. **10** (1976), 107–115.

[GvdP80] L. Gerritzen, M. van der Put, *Schottky groups and Mumford curves*, Lecture Notes in Math., vol. 817, Springer, Berlin, 1980.

[Kur79] A. Kurihara, *On some exemples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Tokyo **25** (1979), num. 3, 277–300.

[Mum72] D. Mumford, *An analytic construction of degenerating curves over complete local rings*, Compositio Math. **24** (1972), 129–174.

[Sch00] T. Schmechta, *Mumford-Tate curves*, Courbes semistables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., vol. 187, Birkhäuser, Basel, 2000, pp. 111–119.

[Tat71] J. Tate, *Rigid analytic spaces*, Invent. Math. **12** (1971), 257–289.

Capítol 4

Integral models of Shimura curves (after K. Buzzard)

R. Re

4.1 The functorial point of view on Shimura curves

The present report is a brief summary of the author's talk at the seminar of the Number Theory group of the University of Barcelona of year 2001. It consists of an exposition of the results contained in the article [Buz97], by K. Buzzard. The author of these notes heartly thanks prof. Pilar Bayer for her invitation to participate to this seminar, and the Department of Mathematics of the University of Barcelona for the hospitality.

False elliptic curves

Let D be an indefinite nonsplit quarternion algebra over $\mathbb{Q}$, $\mathcal{O}_D$ a fixed maximal order of D and $d = \mathrm{disc}(D)$. Let S be a scheme on

which d is invertible. A *false elliptic curve* over S is a pair $(A/S, i)$ where A/S is an abelian surface over S and $i : \mathcal{O}_D \to \mathrm{End}_S(A)$ is an injective ring homomorphism.

A false elliptic curve always admits a *canonical principal polarization*, whose associated Rosati involution in $\mathrm{End}(A_s)$, for any $s \in S$, induces the involution on $\mathcal{O}_D$ given by $x \mapsto t^{-1}\bar{x}t$, where $t \in \mathcal{O}_D$ is such that $t^2 = -d$.

Isogenies

Isogenies π of false elliptic curves (A, i) and (B, j) are defined as the isogenies compatible with the structure maps i, j. Their transposed $\pi^t : B \to A$ are defined in terms of the canonical pricipal polarization defined above. The *false degree* of an isogeny is the integer number $n = \pi^t\pi$.

Level structures

A *naïve full level M-structure* on a f.e.c. $(A/S, i)$ is an isomorphism of schemes $\alpha : (\mathcal{O}_D \otimes \mathbb{Z}/M\mathbb{Z})_S \to A[M]$, where by $A[M]$ we mean the M-torsion points of A (as group scheme over S.) This isomorphism is required to preserve the left action of $\mathcal{O}_D$.
There is the following generalization of this to the concept of a *naïve H-structure* on $(A/S, i)$, for a subgroup $H \subseteq (\mathcal{O}_D \otimes \mathbb{Z}/M\mathbb{Z})^*$:
a *naïve H-structure* is a full M-structure on A_{U_i} for each open set U_i of an (étale) open covering of S such that two of these are related by the left multiplication by an element in H on $U_i \times_S U_j$. In other words a global section of a suitable sheaf in the étale topology.
If we denote by $\mathcal{O}_{D,f}$ the inverse limit of the rings $\mathcal{O}_D \otimes \mathbb{Z}/M\mathbb{Z}$, that is $\mathcal{O}_D \otimes \hat{\mathbb{Z}}$, and calling $U \subseteq \mathcal{O}_{D,f}^*$ the preimage of H, we may also speak of level $U-$ structure, since a $H-$ structure lifts to any M' divisible by M. In particular one may consider the following cases:

- $U = V_0(M)$ the preimage of

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) \mid c = 0 \right\}$$

under the natural surjection $u_M : \mathcal{O}_{D,f}^* \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) \cong (\mathcal{O}_D \otimes \mathbb{Z}/M\mathbb{Z})^*$.

- $U = V_1(M)$ the preimage of

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/M\mathbb{Z}) \mid c = 0 \text{ and } d = 1 \right\}.$$

Shimura curves as algebraic stacks

Let U be a compact open subgroup of $\mathcal{O}_{D,f}^*$ with the following three properties:

1. $\det(U) = \hat{\mathbb{Z}}^*$.
2. U is maximal at primes dividing d that is $U = (\mathcal{O}_D \otimes \mathbb{Z}_p)^* \times U'$ for any $p \not| d$.
3. $U \subseteq V_1(N)$ for some $N \geq 4$ prime to d.

One defines M_U as the smallest positive integer M prime to d and such that $\ker u_M \subseteq U$.

Then one defines the category $X^D(U)$ as follows: an object of $X^D(U)$ is a f.e.c. $(A/S/\mathbb{Z}[1/M_U d], i_A)$ equipped with a level $U-$ structure; a morphism is a morphism of f.e.c. compatible with all the given structures in the natural sense. There is a morphism of $X^D(U)$ in the category of $\mathrm{Spec}(\mathbb{Z}[1/M_U d])-$schemes given by sending $(A/S, i)$ to S. With all this set we can state the following theorems.

4.1.1 Theorem. *If (1) and (2) hold then $X^D(U)$ is an algebraic stack over $\mathbb{Z}[1/M_U d]$. Moreover the morphism*

$$X^D(U) \to \mathrm{Spec}(\mathbb{Z}[1/M_U d])$$

is proper of relative codimension one.
If also (3) holds then $X^D(U)$ is associated to a scheme, and $X^D(U) \to$

$\mathrm{Spec}(\mathbb{Z}[1/M_U d])$ *is projective. Moreover its fibres are geometrically irreducible.*

The reader may look [CF90] for the basic definitions and results on algebraic stacks.

New structures at l

One can add new structures to the algebraic stack $X^D(U)$.

- A $\Gamma_0(l)$-*structure* on a f.e.c. A/S is an isogeny π of f.e.c's $\pi : A/S \to B/S$ of false degree l. Equivalently, a $\Gamma_0(l)$-*structure* can be thought as a finite subgroup scheme $K \subset A[l]$ of rank l^2 which is $\mathcal{O}_D$-invariant, interpreted as the kernel of an isogeny of false degree l. If one considers the isomorphism of $\mathcal{O}_D$ with $M_2(\mathbb{F}_l)$ then by taking $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, one sees that $K \cong K_1 \oplus K_2$ where $K_1 = \ker(e)$ and $K_2 = \ker(1-e)$. Moreover $K_1 \cong K_2$ via the action of the element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and therefore K_1 alone is sufficient to determine K and therefore a $\Gamma_0(l)$-*structure*.
- A $\Gamma_1(l)$-*structure* on $(A/S, i)$ is a $\Gamma_0(l)$-*structure*, plus a generator P of K_1.
- A *balanced* $\Gamma_1(l)$-*structure* is a $\Gamma_0(l)$-*structure* plus also a generator P' of K_1', which is the kernel of $e^* : K' \to K'$ where K' is the kernel of the dual isogeny.
- A *canonical balanced* $\Gamma_1(l)$-*structure* is as above plus the condition that $\langle P, P' \rangle = \omega_l$, where $\langle P, P' \rangle$ is the canonical pairing between $\ker \pi$ and $\ker \pi^t$ and ω_l is a fixed primitive $l-$th root of unity.

The results on the new structures are the following.

4.1.2 Theorem. *Let U be a compact group satisfying (1)-(3) as above and suppose that l does not divide $M_U d$. Then the functors*

from $\mathbb{Z}[1/M_U d]$-schemes to sets, which send S to the sets of isomorphism classes of f.e.c. over S equipped with a level U- structure and a $\Gamma_0(l)$-structure , or a canonical balanced $\Gamma_1(l)$-structure are representable by schemes $X^D(U, \Gamma_0(l))$ and $X^D(U, Bal.can\Gamma_1(l))$ respectively.

The following theorem analyzes the structure of these schemes more closely.

4.1.3 Theorem. *One has the following:*

1. *$X^D(U, \Gamma_0(l))$ is smooth over $\mathbb{Z}[1/M_U d]$ away from the supersingular points in characteristic l.*
2. *$X^D(U, \Gamma_0(l))/\mathbb{Z}[1/M_U d]$ is proper.*
3. *The forgetful map $c : X^D(U, \Gamma_0(l)) \to X^D(U)$ is finite. Moreover c is flat and $X^D(U, \Gamma_0(l))$ is a regular scheme.*
4. *The fibre $X^D(U, \Gamma_0(l))_{\mathbb{F}_l}$ of $X^D(U, \Gamma_0(l))$ is composed of two irreducible components, both isomorphic to $X^D(U)_{\mathbb{F}_l}$, which intersect transversely at the supersingular points.*

A similar theorem also holds for $X^D(U, Bal.can.\Gamma_1(l))$ as a scheme over $\mathrm{Spec}(\mathbb{Z}[1/M_U d][\omega_l])$. Here the role of $X^D(U)$ is played by a covering of it, the scheme $X^D(U, Ig(l))$ representing the functor of isomorphism classes of f.e.c. plus *Igusa structures*. We will not discuss this case in more detail.
The proof of these results follows similar techniques to those in [KM85], and the results themselves are clear analogues of those holding for modular curves.

Bibliografia

[Bou79] J-F. Boutot, *Le problème de modules en inégale caractéristique*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 43–62.

[Buz97] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), num. 3, 591–612.

[CF90] C. Chai, G. Faltings, *Degenerations of abelian varieties*, vol. 22, Ergeb. Math. Grenzgeb., num. 3, Springer, 1990.

[KM85] N. M. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

Capítol 5

Operadors de Hecke. Fórmula de les traces

A. Arenas

En aquestes notes introduïm l'àlgebra de Hecke respecte del grup de les unitats de norma 1 d'un ordre d'Eichler d'una $\mathbb{Q}$-àlgebra de quaternions indefinida. Això permet considerar sense ambigüitat els operadors de Hecke i justificar la seva acció sobre les formes parabòliques amb caràcter. L'objectiu final d'aquestes notes és arribar a la fórmula de les traces d'aquests operadors, així com oferir una panoràmica general dels mètodes i prerequisits emprats.

5.1 Operadors de Hecke

Un subgrup Γ de $\mathrm{SL}(2,\mathbb{R})$ s'anomena *fuchsià de primera espècie* si és discret i $\Gamma\backslash\mathcal{H}^*$ és compacte; on $\mathcal{H}^* = \mathcal{H} \cup \{ \text{ puntes de } \Gamma\}$ i $\mathcal{H}$ denota l'hiperplà superior de Poincaré. Per un teorema de Siegel ([Sie45]), un subgrup de $\mathrm{SL}(2,\mathbb{R})$ és fuchsià de primera espècie si i només si el volum de $\Gamma\backslash\mathcal{H}^*$ és finit. L'exemple més conegut és el del grup modular $\mathrm{SL}(2,\mathbb{Z})$ i els seus subgrups de congruència. En aquestes notes ens interessarem pel grup fuchsià de primera espècie

$$\Gamma(\mathcal{O}) = \{\gamma \in \mathcal{O} | N_B(\gamma) = 1\},$$

de les unitats de norma 1 d'un ordre $\mathcal{O}$ d'una $\mathbb{Q}$-àlgebra de quaternions indefinida $\mathbf{B}$. Per a provar que $\Gamma(\mathcal{O})$ és fuchsià de primera espècie cal fer primer un estudi previ detallat dels ordres de $\mathbf{B} \bigotimes \mathbb{Q}_p$ (veure ([Wei67a]) i, si denotem per $\mathbb{A}_{\mathbb{Q}}$ les adèles de $\mathbb{Q}$, globalitzar després els resultats obtinguts en l'idelitzat $(\mathbf{B} \bigotimes \mathbb{A}_{\mathbb{Q}})^*$ de $\mathbf{B}$. Així doncs, és gairebé essencial pensar aquest grup adèlicament:

$$\Gamma(\mathcal{O}) = (\mathbf{GL}^+(2,\mathbb{R}) \times \Pi_p \mathcal{O}_p^*) \cap \mathbf{B}^*,$$

on $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$.

En el cas en què $\mathbf{B}$ sigui una $\mathbb{Q}$-àlgebra de quaternions indefinida de discriminant D i $\mathcal{O}(D,N)$ un ordre d'Eichler de nivell N de $\mathbf{B}$, denotarem per $\Gamma(D,N)$ el corresponent grup d'unitats de norma 1.

Si $\mathbf{B}$ és una àlgebra de divisió, aleshores $\Gamma\backslash\mathcal{H}$ és compacte i per tant $\Gamma(\mathcal{O})$ no té puntes.

Si $D = 1$ podem suposar $\mathbf{B} = \mathbf{M}(2,\mathbb{Q})$, aleshores es recuperen el grup modular i els seus subgrups de congruència. En particular, si

$$\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M}(2,\mathbb{Z}) | c \equiv 0 \mod N \right\},$$

es té $\Gamma(\mathcal{O}) = \Gamma_0(N)$.

Pel fet que $\Gamma(\mathcal{O})$ és un grup fuchsià de primera espècie tenim que $\Gamma(\mathcal{O})\backslash\mathcal{H}^*$ és una superfície de Riemann compacta que dóna lloc a la *corba de Shimura* $X(\Gamma(\mathcal{O}))$:= relativa al grup $\Gamma(\mathcal{O})$. Si $\mathcal{O}(D,N)$ és un ordre d'Eichler de discriminant D i de nivell N, denotarem per $\mathbf{X}(D,N)$ la corresponent corba de Shimura i observem que en el cas $\Gamma(\mathcal{O}) = \Gamma_0(N)$, obtenim la corba modular $X_0(N)$.

Donem ara un recull de les definicions habituals de formes automorfes i d'operadors de Hecke introduïts a partir de classes laterals dobles (cf. [Shi71]).

Si f és una funció a valors complexos definida sobre $\mathcal{H}$ i $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ és un element de $\mathrm{GL}^+(2,\mathbb{R})$, aleshores l'acció, de pes $k \in \mathbb{Z}$, de α sobre f ve donada per:

$$(f|_k\alpha)(z) = (det\alpha)^{\frac{k}{2}}(cz+d)^{-k} f(\alpha(z)).$$

Si $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$ és un grup fuchsià de primera espècie i χ és un caràcter de Γ d'ordre finit, una funció $f : \mathcal{H} \to \mathbb{C}$ s'anomena *forma automorfa* de pes k respecte de Γ amb caràcter χ quan es compleixen les condicions següents:

(i) f és meromorfa en $\mathcal{H}$,

(ii) $f|_k\gamma = \chi(\gamma)f$, per a tot $\gamma \in \Gamma$,

(iii) f és meromorfa a les puntes de Γ.

$\mathcal{A}_k(\Gamma,\chi)$ denotarà el conjunt de formes automorfes de pes k respecte de Γ amb caràcter χ.

Anàlogament es defineix el conjunt $\mathcal{G}_k(\Gamma,\chi)$ de *formes enteres* de pes k respecte de Γ amb caràcter χ, és a dir, $f \in \mathcal{G}_k(\Gamma,\chi)$ si $f : \mathcal{H} \to \mathbb{C}$, és holomorfa, $f|_k = \chi(\gamma)f, \forall\gamma \in \Gamma$, i f és holomorfa a les puntes de Γ. En el cas en què $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ sigui un subgrup de congruència, $\mathcal{G}_k(\Gamma,\chi)$ s'anomena espai de formes modulars. Per $\mathcal{S}_k(\Gamma,\chi)$ es denotarà l'espai de *formes parabòliques*, és a dir el format per les formes enteres que s'anul.len a les puntes de Γ. Òbviament, si Γ no té puntes els $\mathbb{C}$-espais vectorials $\mathcal{G}_k(\Gamma,\chi)$ i $\mathcal{S}_k(\Gamma,\chi)$ coincideixen.

Donades dues formes enteres f,g amb almenys una d'elles parabòlica, es defineix el *producte escalar de Petersson*:

$$< f, g >= \int_{\Gamma\backslash\mathcal{H}} f(z)g(z)y^{k-2}dxdy,$$

amb $z = x + iy$.

Aquest producte és hermític a l'espai de formes parabòliques.

Dos subgrups Γ, Γ' d'un mateix grup $\mathbf{G}$ s'anomenen *commensurables*, i això ho denotarem $\Gamma \approx \Gamma'$, si $[\Gamma : \Gamma\cap\Gamma'] < \infty$ i $[\Gamma' : \Gamma\cap\Gamma'] < \infty$. El subgrup de $\mathbf{G}$

$$\widetilde{\Gamma} = \{g \in \mathbf{G} | g\Gamma g^{-1} \approx \Gamma\}$$

s'anomena el *commensurador* de Γ.

Per a tot $\alpha \in \widetilde{\Gamma}$ considerarem la *classe lateral doble* $\Gamma\alpha\Gamma$ de α respecte de Γ. Es té

$$\Gamma\alpha\Gamma = \sqcup\Gamma\alpha_i,$$

on $\alpha_i = \alpha\gamma_i$, i on $\{\gamma_1, ..., \gamma_n\}$ és un conjunt de representants de $(\Gamma \cap \alpha^{-1}\Gamma\alpha)\backslash\Gamma$. Si Γ és un subgrup de $\mathbf{G}$, $\Delta \subset \mathbf{G}$ és un semigrup de $\mathbf{G}$ tal que $\Gamma \subset \Delta \subset \widetilde{\Gamma}$, i considerem elements α, $\beta \in \Delta$ amb les seves corresponents classes laterals dobles $\Gamma\alpha\Gamma = \sqcup\Gamma\alpha_i$, i $\Gamma\beta\Gamma = \sqcup\Gamma\beta_j$, es pot definir el següent producte:

$$(\Gamma\alpha\Gamma).(\Gamma\beta\Gamma) = \sum_{\gamma} c_\gamma \ \Gamma\gamma\Gamma,$$

amb

$$c_\gamma = \#\{(i,j)|\Gamma\alpha_i\beta_j = \Gamma\gamma\}.$$

Es pot comprovar que aquesta definició no depèn dels representants triats. Estenent per bilinealitat s'obté així l'anomenada *àlgebra de Hecke*, que denotarem $\mathbb{T}(\Gamma, \Delta)$, formada per les combinacions lineals formals $\sum_{\alpha\in\Delta} a_\alpha \Gamma\alpha\Gamma$ amb $a_\alpha \in \mathbb{Z}$, $a_\alpha = 0$ per a quasi tot α. Els elements de $\mathbb{T}(\Gamma, \Delta)$ s'anomenen (per abús del llenguatge) operadors de Hecke.

Donada una forma automorfa $f \in \mathcal{A}_k(\Gamma, \chi)$, es defineix l'acció d'una classe doble $\Gamma\alpha\Gamma$ sobre una forma automorfa $f \in \mathcal{A}_k(\Gamma, \chi)$ de la següent manera:

$$(f|\Gamma\alpha\Gamma)(z) = \sum_{j=1}^{n} \det(\alpha_j)^{\frac{k}{2}-1}\overline{\chi(\alpha_j)}(f|\alpha_j)(z).$$

Aquesta definició és independent dels representants triats.

Sigui $\mathbf{B}$ una $\mathbb{Q}$-àlgebra de quaternions indefinida de discriminant D. Ara esbrinarem l'estructura de l'àlgebra de Hecke associada al grup $\Gamma = \Gamma(N, D)$ de les unitats de norma 1 d'un ordre d'Eichler $\mathcal{O} = \mathcal{O}(N, D)$ de nivell N de l'àlgebra $\mathbf{B}$ que, de fet, veurem que es redueix a la de les corresponents àlgebres de Hecke locals. Denotem per $\mathbf{B}_A = \mathbf{B} \otimes \mathbb{Q}_A$ l'adelitzat de $\mathbf{B}$ i considerem els següents conjunts

$$\mathbf{U} = \mathbf{GL}^+(2, \mathbb{R}) \times \Pi_p \mathcal{O}_p^*$$

$$\text{i} \quad \mathbf{D} = (\mathbf{GL}^+(2, \mathbb{R}) \times \Pi_p \mathbf{D}_p) \cap \mathbf{B}_A^*,$$

on

$$\mathbf{D}_p = \begin{cases} \{g \in \mathcal{O}_p | N_{\mathbf{B}_p}(g) \neq 0\}, & \text{si } p \nmid N \\ \left\{ \begin{pmatrix} a & b \\ p^e c & d \end{pmatrix} \in \mathcal{O}_p |\ a \in \mathbb{Z}_p^*, ad - p^e bc \neq 0 \right\}, & \text{si } p \mid N \end{cases}$$

i el semigrup $\Delta = \mathcal{O} \cap \mathbf{D}$.

La següent proposició permetrà considerar les àlgebres de Hecke: $\mathbb{T}(\mathcal{O}_p^*, \mathbf{D}_p)$, $\mathbb{T}(\mathbf{U}, \mathbf{D})$, $\mathbb{T}(\Gamma, \Delta)$.

5.1.1 Proposició. $\mathbf{U}$ *és un subgrup de* $\mathbf{B}_A^*$ *i* $\mathbf{D}$ *és un semigrup de* $\mathbf{B}_A^*$. $\mathcal{O}_p^*$ *és un subgrup de* $\mathbf{B}_p^*$ *i* $\mathbf{D}_p$ *és un semigrup de* $\mathbf{B}_p^*$. $\mathbf{\Gamma}$ *és un subgrup de* $\mathbf{B}^*$ *i* Δ *és un semigrup de* $\mathbf{B}^*$. *A més es tenen les inclusions:* $\mathcal{O}_p^* \subset \mathbf{D}_p \subset \widetilde{\mathcal{O}_p^*}$, $\mathbf{U} \subset \mathbf{D} \subset \widetilde{\mathbf{U}}$, $\mathbf{\Gamma} \subset \Delta \subset \widetilde{\mathbf{\Gamma}}$.

El teorema següent permet reduir l'estudi de l'estructura de l'àlgebra de Hecke $\mathbb{T}(\Gamma, \Delta)$ al cas local.

5.1.2 Teorema. (i) *L'aplicació*

$$\Gamma\alpha\Gamma \mapsto \mathbf{U}\alpha\mathbf{U}$$

indueix un isomorfisme

$$\mathbb{T}(\Gamma, \Delta) \cong \mathbb{T}(\mathbf{U}, \mathbf{D}).$$

(ii) *L'aplicació*

$$\mathbf{U}g\mathbf{U} \mapsto \mathcal{O}_p^* g_p \mathcal{O}_p^*,$$

on $g = (g_v)$, *indueix un isomorfisme*

$$\mathbb{T}(\mathbf{U}, \mathbf{D}) \cong \bigotimes_p \mathbb{T}(\mathcal{O}_p^*, \mathbf{D}_p).$$

L'estructura de l'àlgebra de Hecke local $\mathbb{T}(\mathcal{O}_p^*, \mathbf{D}_p)$ és donada pel següent:

5.1.3 Teorema. *Per a tot primer* p, *la* $\mathbb{Z}$*-àlgebra* $\mathbb{T}(\mathcal{O}_p^*, \mathbf{D}_p)$ *és commutativa, i es satisfà:*

(i) $\mathbb{T}(\mathcal{O}_p^*, \mathbf{D}_p) = \mathbb{Z}[T'(1,p), T'(p,p)]$, *si* $p \nmid ND$,
amb $T'(1,p)$ *i* $T'(p,p)$ *algebraicament independents, on*

$$T'(1,p) = \mathcal{O}_p^* \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \mathcal{O}_p^*,$$

$$T'(p,p) = \mathcal{O}_p^* \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \mathcal{O}_p^*.$$

Els seus elements satisfan:

$$T'(1,p)T'(1,p) = T'(1,p^2) + (p+1)T'(p,p);$$
$$T'(1,p)T'(1,p^e) = T'(1,p^{e+1}) + pT'(p,p)T'(1,p^{e-1}),\ \textit{si } e>1;$$
$$T'(p,p)T'(p^e,p^f) = T'(p^{e+1},p^{f+1}),\ \textit{per a qualssevol } e,f\in\mathbb{Z}^+.$$

(ii) $\mathbb{T}(\mathcal{O}_p^*,\mathbf{D}_p) = \mathbb{Z}[T'(1,p)]$, *si* $p|N$,
amb $T'(1,p)$ *algebraicament independent, i es té*

$$T'(1,p)T'(1,p^e) = T'(p^{e+1}),$$

per a tot $e\in\mathbb{Z}^+$.

(iii) $\mathbb{T}(\mathcal{O}_p^*,\mathbf{D}_p) = \mathbb{Z}[\mathcal{O}_p^*\pi_p\mathcal{O}_p^*]$, *si* $p|D$,
amb π_p *un element primer de* $\mathbf{B}_p$, *i amb les relacions*

$$\mathcal{O}_p^*\pi_p^2\mathcal{O}_p^* = \mathcal{O}_p^*p\mathcal{O}_p^*$$

i

$$(\mathcal{O}_p^*\pi_p\mathcal{O}_p^*)(\mathcal{O}_p^*\pi_p^e\mathcal{O}_p^*) = \mathcal{O}_p^*\pi_p^{e+1}\mathcal{O}_p^*,$$

per a tot $e\in\mathbb{Z}^+$.

5.1.4 Definició.

$$T(n) := \sum \Gamma\alpha\Gamma,$$

amb les condicions $n\in\mathbb{Z}^+$, $\alpha\in\Delta$, $\mathbf{N}_{\mathbf{B}}(\alpha) = n$.

$$T(n,n) := \Gamma n\Gamma,\ \textit{si } (n,N)=1.$$

Tenint en compte que $\mathbb{T}(\mathcal{O}_p^*,D_p)$ és un subanell de $\bigotimes_p \mathbb{T}(\mathcal{O}_p^*,D_p)$ i que aquest últim és isomorf a $\mathbb{T}(\Gamma,\Delta)$ es té:

5.1.5 Proposició. (i) *Si* $p\nmid ND$, *aleshores l'operador* $T(p^m)$ *correspon a* $\sum \mathcal{O}_p^*\begin{pmatrix}p^r & 0\\ 0 & p^s\end{pmatrix}\mathcal{O}_p^*$, *amb la suma estesa a les parelles* (r,s) *satisfent* $r+s=m$, $0\le r\le s$. *A més, l'operador de Hecke* $T(p,p)$ *correspon a* $\mathcal{O}_p^*p\mathcal{O}_p^*$.

(ii) *Si* $p|N$, *aleshores* $T(p^m)$ *correspon a* $\mathcal{O}_p^*\begin{pmatrix}1 & 0\\ 0 & p^m\end{pmatrix}\mathcal{O}_p^*$.

(iii) *Si $p|D$, aleshores $T(p^m)$ correspon a $\mathcal{O}_p^*\pi_p^m\mathcal{O}_p^*$.*

Els resultats anteriors permeten de donar l'estructura de l'àlgebra de Hecke $\mathbb{T}(\Gamma,\Delta)$ respecte del grup d'unitats de norma 1 d'un ordre d'Eichler $\mathcal{O}(D,N)$ d'una $\mathbb{Q}$-àlgebra de quaternions indefinida de discriminant D.

5.1.6 Teorema. *L'àlgebra de Hecke $\mathbb{T}(\Gamma,\Delta)$ és commutativa i*

$$\mathbb{T}(\Gamma,\Delta)=\mathbb{Z}[T(p),T(p,p),T(q)],$$

amb els $T(p)$, $T(p,p)$ i $T(q)$ algebraicament independents, de manera que $p\nmid ND$, $q|ND$.

Amb les següents lleis de multiplicació:

$$\begin{array}{ll} T(nm)=T(n)T(m) & (n,m)=1,\\ T(p^r)T(p)=T(p^{r+1})+pT(p,p)T(p^{r-1}) & p\nmid ND,\\ T(q^r)T(q)=T(q^{r+1}) & q|ND.\end{array}$$

El teorema anterior és equivalent a dir que la sèrie formal de Dirichlet $\sum T(n)n^{-s}$ té producte d'Euler:

$$\sum T(n)n^{-s}=\prod_{p\nmid ND}(1-T(p)p^{-s}+pT(p,p)p^{-2s})^{-1}$$
$$\times\prod_{q|ND}(1-T(q)q^{-s})^{-1}.$$

5.1.7 Remarques. (i) Tot caràcter χ de Dirichlet mòdul N indueix un caràcter a $\Gamma(D,N)$. (ii) $\mathbb{T}(\Gamma,\Delta)$ opera a l'espai $\mathcal{G}_k(\Gamma,\chi)$ de formes modulars enteres i, en particular, a l'espai $\mathcal{S}_k(\Gamma,\chi)$ de formes modulars parabòliques.

Tenint en compte les propietats anteriors i treballant anàlogament al cas modular s'obté el següent:

5.1.8 Teorema. *Sigui $\Gamma=\Gamma(N,D)$ i sigui χ un caràcter de Dirichlet mòdul N, aleshores*

$$\langle f|_kT(n),g\rangle=\langle f,g|_k\overline{\chi(n)}T(n)\rangle,$$

per a f, $g \in \mathcal{S}_k(\Gamma, \chi)$.

L'espai $\mathcal{S}_k(\Gamma, \chi)$ *té una base de funcions pròpies respecte de tots els operadors de Hecke* $T(n)$ *amb* $(n, N) = 1$.

5.2 Fórmula de les traces

L'origen de la recerca d'una fórmula que permeti calcular les traces dels operadors de Hecke es troba en el treball de E. Hecke [Hec40] per tal de calcular nombres de representacions d'enters per formes quadràtiques enteres. M. Eichler ([Eic55a], [Eic57]) dóna una fórmula explícita per a la traça dels operadors $T(n)$ actuant a $\mathcal{S}_k(\Gamma_0(N))$ amb nivell N lliure de quadrats i pes $k \geq 2$. H. Shimizu ([Shi63b], [Shi63a]) generalitza la fórmula per a formes modulars de Hilbert, però mantenint la condició de nivell N lliure de quadrats i, per qüestions tècniques, per a pes $k \geq 3$. M. Yamauchi [Yam71] considera nivell $4N$, amb N imparell i lliure de quadrats. H. Hijikata [Hij74] dóna una fórmula explícita de la traça de $T(n)$ que actuen sobre $\mathcal{S}_k(\Gamma_0(N), \chi)$ per a nivell N qualsevol i pes $k \geq 2$ i per a la traça de $T(n)$ actuant sobre $\mathcal{S}_k(\Gamma, \chi)$, on Γ és el grup d'unitats de norma 1 d'un ordre d'Eichler dins una $\mathbb{Q}$-àlgebra de quaternions indefinida de discriminant $D > 1$. La fórmula de les traces s'aplica per a l'obtenció de dimensions d'espais de formes parabòliques, polinomis característics d'operadors de Hecke i bases d'espais de formes parabòliques (cf. [Miy76], [Wad71], [Wad73]).

Cal recordar que $\mathcal{S}_k(\Gamma, \chi)$ és un espai de Hilbert de dimensió finita i per tant té la funció nucli

$$K_k(z_1, z_2) = \sum_{i=1,\ldots,d} f_i(z_1)\overline{f_i(z_2)}, \qquad \forall z_1, z_2 \in \mathcal{H},$$

on $\{f_1, ..., f_d\}$ és una base ortonormal de $\mathcal{S}_k(\Gamma, \chi)$. A més, es té la notable propietat

$$K_k(z_1, z_2) = \varepsilon^{-1} \sum_{\gamma \in \Gamma} \overline{\chi(\gamma)} K(\gamma(z_1), z_2) j(\gamma, z_1)^{-k},$$

on

$$K(\gamma(z_1), z_2) = \frac{k-1}{4\pi} \left(\frac{z_1 - \overline{z}_2}{2i} \right)^{-k}$$

i $\varepsilon = 2, 1$ segons $-I$ sigui o no un element de Γ.

5.2.1 Notació. Denotarem per T l'operador de Hecke $T(n)$ definit per la suma de totes les classes laterals dobles distintes $\Gamma\beta\Gamma$ amb $\beta \in \Delta$ i $N(\beta) = n$. A més a més, denotarem per $\alpha \in T$ la condició $\alpha \in \Gamma\beta\Gamma$, on $\beta \in \Delta, N(\beta) = n$, i observem que si $\alpha \in T$, aleshores $\alpha \in \mathbf{B}^*$.

5.2.2 Remarca. Si $\{f_1, ..., f_d\}$ és una base ortonormal de $\mathcal{S}_k(\Gamma, \chi)$ aleshores la traça $\mathrm{tr}(T)$ de $T(n)$ actuant sobre $\mathcal{S}_k(\Gamma, \chi)$ és donada per

$$\mathrm{tr}(T) = \sum_{i=1,...d} \langle f_i | T, f_i \rangle.$$

Ara aplicant successivament les definicions de producte escalar de Petersson, d'acció d'un operador de Hecke sobre una forma parabòlica i el valor de la funció nucli de $\mathcal{S}_k(\Gamma, \chi)$ s'obté

$$\mathrm{tr}(T) = \varepsilon^{-1} \int_{\Gamma\backslash\mathcal{H}} \sum_{\alpha \in T} \kappa(z, \alpha) y^{-2} dxdy.$$

Com que Γ actúa sobre $\mathbf{B}$ per conjugació, podem considerar, en particular, el grup d'isotropia

$$\Gamma(\alpha) = \{\gamma \in \Gamma | \gamma\alpha\gamma^{-1} = \alpha\},$$

dels elements $\alpha \in T$ i denotarem per $T//\Gamma$ el conjunt de classes de conjugació.

La integral i la suma involucrades en el càlcul de la traça es poden invertir tenint en compte l'acció de Γ sobre T per conjugació:

$$\mathrm{tr}(T) = \varepsilon^{-1} \sum_{\alpha \in T//\Gamma} \int_{\Gamma(\alpha)\backslash\mathcal{H}} \kappa(z, \alpha)\ y^{-2} dxdy.$$

Distingint ara segons l'element $\alpha \in T$ sigui un múltiple de $\pm I$, $(\alpha \in T^o)$; una transformació elúlíptica, $(\alpha \in T^e)$; una transformació hiperbòlica, $(\alpha \in T^h)$; o una transformació parabòlica, $(\alpha \in T^p)$; i donat que el tipus de α es respecta per conjugació, la suma precedent que expressa la traça de T es pot descompondre en quatre sumands:

$$\mathrm{tr}(T) = t_o + t_e + t_h + t_p\ ,$$

amb

$$t_* = \varepsilon^{-1} \sum_{\alpha \in T^*//\Gamma} \int_{\Gamma(\alpha)\backslash\mathcal{H}} \kappa(z,\alpha)\ y^{-2} dxdy.$$

(l'estrella * pot designar o, e, h, p).

En el cas de $\alpha \in T^o$ és fàcil fer els càlculs. Es té

$$\alpha = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \qquad \Gamma(\alpha) = \Gamma$$

i aleshores

$$\int_{\Gamma(\alpha)\backslash\mathcal{H}} \kappa(z,\alpha) y^{-2} dxdy$$

$$= \det(\alpha)^{k-1} \overline{\chi}(\alpha) \frac{k-1}{4\pi} \int_{\Gamma\backslash\mathcal{H}} \left(\frac{z-\overline{z}}{2i}\right)^{-k} a^{-k} y^{k-2} dxdy$$

$$= \det(\alpha)^{k-1} \overline{\chi}(\alpha) \frac{k-1}{4\pi} a^{-k} \int_{\Gamma\backslash\mathcal{H}} \left(\frac{2iy}{2i}\right)^{-k} y^{k-2} dxdy$$

$$= \operatorname{sgn}(\alpha)^k \det(\alpha)^{\frac{k}{2}-1} \overline{\chi}(\alpha) \frac{k-1}{4\pi} \operatorname{vol}(\Gamma\backslash\mathcal{H}).$$

Els càlculs involucrats en els altres sumands són tediosos, però esdevenen relativament senzills si prèviament es consideren els punts fixos de les transformacions que hi surten. Concretament, cal remarcar en el cas hiperbòlic que si $\alpha \in T^h$ té almenys un punt fix que sigui punta de Γ, aleshores l'altre punt fix també és una punta de Γ. Si $\alpha \in T^h$ és tal que cap dels seus dos punts fixos és una punta de Γ, aleshores

$$\int_{\Gamma(\alpha)\backslash\mathcal{H}} \kappa(z,\alpha)\ y^{-2} dxdy = 0,$$

i, en el cas parabòlic, que el seu punt fix és necessàriament una punta de Γ. En definitiva, resulta el següent:

5.2.3 Teorema.

$$t_o = \frac{k-1}{4\pi} \varepsilon^{-1} \operatorname{vol}(\Gamma\backslash\mathcal{H}) \sum_{\alpha \in T^0} \overline{\chi}(\alpha) \operatorname{sgn}(\alpha)^k \det(\alpha)^{\frac{k}{2}-1},$$

$$t_e = -\sum_{\alpha \in T^e//\Gamma} \overline{\chi}(\alpha) k(\alpha) l(\alpha),$$

$$t_h = -\sum_{\alpha\in T^h//\Gamma} \overline{\chi}(\alpha)k(\alpha)l(\alpha),$$

$$t_p = -\lim_{s\to 0^+} \sum_{\alpha\in T^p//\Gamma} \overline{\chi}(\alpha)k(\alpha)l(\alpha),$$

on

$$k(\alpha) = \begin{cases} \dfrac{\eta_\alpha^{k-1} - \zeta_\alpha^{k-1}}{\eta_\alpha - \zeta_\alpha}, & \alpha \in T^e, \\ \dfrac{\min\{|\zeta_\alpha|, |\eta_\alpha|\}^{k-1}}{|\zeta_\alpha - \eta_\alpha|}\mathrm{sgn}(\alpha)^k, & \alpha \in T^h, \\ \dfrac{s}{4}\mathrm{sgn}(\alpha)^k \det(\alpha), & \alpha \in T^p, \end{cases}$$

$$\mathrm{sgn}(\alpha) = \mathrm{sgn}(\zeta_\alpha),$$

$$l(\alpha) = \begin{cases} (2\varepsilon)^{-1}, & \alpha \in T^e, \\ \varepsilon^{-1}, & \alpha \in T^h, \\ \varepsilon^{-1}|m(\alpha)|^{s+1}, & \alpha \in T^p, \end{cases}$$

on $m(\alpha)$ s'expressa bàsicament en termes de l'arrel ζ_α (cf. [Miy76], chap. 6).

Observem que si $\Gamma\backslash\mathcal{H}$ és compacte, aleshores $t_p = t_h = 0$. Per tal de calcular les sumes que surten al teorema anterior, considerem l'acció de $\mathbf{B}^*$ sobre T per conjugació. Sigui $\alpha \in \mathbf{B}^* \cap \mathcal{O}, \alpha \notin \mathbb{Q}$, denotem per $C(\alpha)$ l'òrbita de α

$$C_{\mathbf{B}^*}(\alpha) = \{\delta\alpha\delta^{-1} | \delta \in \mathbf{B}^*\}.$$

Si $\alpha \in T$, aleshores $\alpha \in \mathbf{B}^* \cap \mathcal{O}$, ja que $\Gamma \subset \Delta = \mathcal{O} \cap \mathbf{D}$ i $\det \alpha = n > 0$.

Denotem $S = T^e, T^h, T^p$. Aleshores:

$S \cap C(\alpha) = T \cap C(\alpha)$, la qual cosa permet unificar notacions. Per tal de calcular

$$\sum_{\alpha\in S//\Gamma} \overline{\chi(\alpha)}k(\alpha)l(\alpha),$$

trencarem aquesta expressió en tres sumes.

La funció $k(\alpha), \alpha \in S$, és invariant respecte de la conjugació respecte d'elements de $\mathbf{B}^*$:

$$k(\alpha) = k(\delta\alpha\delta^{-1}), \quad \forall \delta \in \mathbf{B}^*.$$

Per tant:

$$\sum_{\alpha \in S//\Gamma} \overline{\chi(\alpha)} k(\alpha) l(\alpha) = \sum_{\alpha \in S//\mathbf{B}^*} k(\alpha) \sum_{\beta \in (T \cap C(\alpha))//\Gamma} \overline{\chi(\beta)} l(\beta).$$

Si $\alpha \in T, \alpha \notin \mathbb{Q}$, considerem la $\mathbb{Q}$-àlgebra $\mathbb{Q}[\alpha]$. Si $\alpha \in T^e \cup T^h \cup T^p$, tenim:

$$\mathbb{Q}[\alpha] \cong \begin{cases} \mathbb{Q}(\sqrt{d}), & d < 0, \alpha \in T^e, \\ \mathbb{Q} \times \mathbb{Q}, & \alpha \in T^h, \\ \mathbb{Q}[\varepsilon], \varepsilon^2 = 0, & \alpha \in T^p. \end{cases}$$

Aquest últim resultat ve d'observar que el discriminant del polinomi característic de α coincideix amb el discriminant de l'equació de punts fixos de α.

5.2.4 Remarca. Si $\beta := \delta\alpha\delta^{-1} \in T \cap C(\alpha)$, aleshores $\mathbb{Q}[\alpha] \cap \delta^{-1}\mathcal{O}\delta$ és un ordre r_β de $\mathbb{Q}[\alpha]$ que conté $\mathbb{Z}[\alpha]$. Si $r_{\beta'} = r_\beta$, es té $l(\beta') = l(\beta)$ i es denota per $l(r)$. Tenint aquests resultats en consideració, s'obté:

$$\sum_{\alpha \in S//\Gamma} \overline{\chi(\alpha)} k(\alpha) l(\alpha)$$

$$= \sum_{\alpha \in S//\mathbf{B}^*} k(\alpha) \sum_{\mathbb{Z}[\alpha] \subset r} l(r) \sum_{\beta \in (T \cap C(\alpha, r))//\Gamma} \overline{\chi(\beta)},$$

on

$$C(\alpha, r) = \{\delta\alpha\delta^{-1} \mid \delta \in \mathbf{B}^*, \mathbb{Q}[\alpha] \cap \delta^{-1}\mathcal{O}\delta = r\}.$$

5.2.5 Notació.

$$\mathbb{Z}_{\mathbf{A}} = \mathbb{R} \times \prod_p \mathbb{Z}_p, \ \mathcal{O}_{\mathbf{A}} = \mathcal{O} \otimes \mathbb{Z}_{\mathbf{A}},$$

$$r_{\mathbf{A}} = r \otimes \mathbb{Z}_{\mathbf{A}},$$

$$C_{\mathbf{A}}(\alpha) = \{h\alpha h^{-1} \mid h \in \mathbf{B}_{\mathbf{A}}^*\},$$

$$C_{\mathbf{A}}(\alpha, r) = \{h\alpha h^{-1} \mid h \in \mathbf{B}_{\mathbf{A}}^*, \mathbb{Q}_{\mathbf{A}}[\alpha] \cap h^{-1}\mathcal{O}_{\mathbf{A}} h = r_{\mathbf{A}}\}.$$

5.2.6 Propietats.

$$C(\alpha) \subset C_{\mathbf{A}}(\alpha), \qquad C(\alpha, r) \subset C_{\mathbf{A}}(\alpha, r).$$

L'aplicació natural $C(\alpha)//\Gamma \to C_{\mathbf{A}}(\alpha)//U$ és epijectiva i el cardinal de la preimatge de cada element és el nombre de classes $h(r)$ de l'ordre r corresponent. A més:

$$\sum_{\beta \in (T \cap C(\alpha,r))//\Gamma} \overline{\chi(\beta)} \quad = \quad h(r) \sum_{g \in (T_{\mathbf{A}} \cap C_{\mathbf{A}}(\alpha,r))//U} \overline{\chi(g)}.$$

Tenint en compte que $\chi_v(g_v) = 1$, si $v = \infty$ o bé $v \nmid N$ es té:

$$\sum_{g \in (T_{\mathbf{A}} \cap C_{\mathbf{A}}(\alpha,r))//U} \overline{\chi(g)} \quad = \quad \prod_v \sum_{g_v \in (T_v \cap C_v(\alpha,r))//\mathcal{O}_v^*} \overline{\chi_v(g_v)}.$$

Aquestes observacions ens permeten en essència reduir els càlculs de les sumes precedents al cas de les idèles o, dit en altres paraules, als corresponents càlculs en totes les localitzacions. Els detalls d'aquestes reduccions es fan un xic llargs, però finalment s'arriba a provar el següent:

5.2.7 Teorema. (Eichler, Selberg, Shimizu, Miyake). *Sigui* $\mathbf{B}$ *una* $\mathbb{Q}$*-àlgebra de quaternions indefinida de discriminant* D*, i sigui* $\mathcal{O} \subset \mathbf{B}$ *un ordre d'Eichler de nivell* $N = \prod_p p^\nu$ *amb la condició* $(D, N) = 1$*. Sigui*

$$\Gamma = \{\gamma \in \mathcal{O}^* | N_{\mathbf{B}}(\gamma) = 1\}$$

el grup de les unitats de norma 1 *de* $\mathcal{O}$*. Sigui* χ *un caràcter de Dirichlet mòdul* N *de conductor* $m_\chi = \prod_p p^e$ *i considerem l'operador de Hecke*

$$T(n) = \sum \Gamma\beta\Gamma,$$

amb $\beta \in \Delta, N_{\mathbf{B}}(\beta) = n$ *i l'espai de formes parabòliques de pes* $k \geq 2$*,* $\mathcal{S}_k(\Gamma, \chi)$*. Aleshores, es té la fórmula següent:*

$$tr(T(n)) = tr(T(n)|\mathcal{S}_k(\Gamma, \chi))$$

$$= \chi(\sqrt{n}) \frac{k-1}{12} n^{\frac{k}{2}-1} N \prod_{p|N} (1 + p^{-1}) \prod_{p|D} (p - 1)$$

$$-\sum_t a(t)\sum_f b(t,f)c(t,f)+\delta_2(N,n),$$

amb $\chi(\sqrt{n})=0$ *si* n *no és un quadrat i per a certes funcions* a, b, c, δ_2, *explicitades, per exemple, en* ([Miy76], pp.263,264).

Una generalització d'aquesta fórmula per a pes semienter es troba en el treball de G. Shimura [Shi74].

Bibliografia

[Eic55a] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156–171.

[Eic57] M. Eichler, *Eine Verallgemeinerung der Abelschen Integrale*, Math. Z. **67** (1957), 267–298.

[Hec40] E. Hecke, *Analytische Arithmetik der positiven quadratischen Formen*, Danske Vid. Selsk. Math.-Fys. Medd. **17** (1940), num. 12, 1–134.

[Hij74] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(n)$, J. Math. Soc. Japan. **26** (1974), num. 1, 56–82.

[Ish73] H. Ishikawa, *On the trace formula for Hecke operators*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 217–238.

[Miy76] T. Miyake, *Modular forms*, Springer, Berlin, 1976.

[Sai72] H. Saito, *On Eichler's trace formula*, J. Math. Soc. Japan **24** (1972), 333–340.

[Sel56] A. Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc. **20** (1956), 47–87.

[Shi63a] H. Shimizu, *On discontinuous groups operating on the product of the upper half planes*, Ann. of Math. **77** (1963), 33–71.

[Shi63b] H. Shimizu, *On traces of Hecke operators*, J. Fac. Sci. Univ. Tokyo Sect. I **10** (1963), 1–19 (1963).

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[Shi74] G. Shimura, *On the trace formula for Hecke operators*, Acta-Math. **132** (1974), num. 3-4, 245–281.

[Sie45] C. Siegel, *Some remarks on discontinuous groups*, Ann. of Math. **46** (1945), 708–718.

[Wad71] H. Wada, *A table of Hecke operators. I*, United States-Japan Seminar on Modern Methods in Number Theory, Tokyo University, 1971, pp. 1–10.

[Wad73] H. Wada, *A table of Hecke operators. II*, Proc. Japan Acad. **49** (1973), 380–384.

[Wei67a] A. Weil, *Basic number theory*, vol. 144, Grundl. math. Wiss., 1967.

[Yam71] M. Yamauchi, *On traces of Hecke operators for certain modular gropus*, Nagoya Math. J. **43** (1971), 137–149.

Capítol 6

Congruències d'Eichler-Shimura

A. Travesa

6.1 Definicions i notacions

6.1.1 • Fixem una $\mathbb{Q}$-àlgebra de quaternions indefinida, B; un ordre maximal, $\mathcal{O} \subseteq B$; i una immersió de B en $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R})$, $\chi : B \longrightarrow \mathrm{M}(2,\mathbb{R})$.

• Sigui $D := \mathrm{disc}(B) = \mathrm{disc}(\mathcal{O})$ el discriminant de l'àlgebra de quaternions, que coincideix amb el dels ordres maximals, i considerem el subgrup d'unitats de norma 1 de $\mathcal{O}$, $\Gamma := \{\alpha \in \mathcal{O} : \mathrm{n}(\alpha) = 1\}$.

• Considerem, també, el semigrup dels elements de $\mathcal{O}$ de norma positiva, $\Delta := \{\alpha \in \mathcal{O} : \mathrm{n}(\alpha) > 0\}$.

• Denotarem per $\alpha \mapsto \alpha'$ la conjugació canònica de B; aquesta conjugació es pot veure com la restricció de la conjugació de $\mathrm{M}(2,\mathbb{R})$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

• Per a tot ideal bilateral $\mathfrak{a} = \alpha\mathcal{O} = \mathcal{O}\alpha \subseteq \mathcal{O}$, escriurem $\Gamma_\alpha := \Gamma_{\mathfrak{a}} := \{\gamma \in \Gamma : \gamma \equiv 1 \pmod{\mathfrak{a}}\}$.

• Notem que, per a tot nombre enter $m \neq 0$, $m\mathcal{O} = \mathcal{O}m$ és un ideal bilateral, ja que m és un element regular i central. En particular, podem considerar el grup Γ_m.

• Se satisfan les inclusions $\Gamma \subseteq \Delta \subseteq \tilde{\Gamma}$, on $\tilde{\Gamma} = B^*$ és el commensurador de Γ en B^*. Per tant, podem parlar de l'anell de Hecke $R(\Gamma, \Delta)$ (cf. Arenas, capítol 5).

• Si, per a $\alpha \in \Delta$, posem

$$\deg(\Gamma\alpha\Gamma) := \#\{\Gamma\alpha_i : \Gamma\alpha_i \subseteq \Gamma\alpha\Gamma,\ \alpha_i \in B^*\},$$

obtenim que $\deg(\Gamma\alpha\Gamma) = [\Gamma : \Gamma \cap \alpha^{-1}\Gamma\alpha] = [\alpha\Gamma\alpha^{-1} : \alpha\Gamma\alpha^{-1} \cap \Gamma] < +\infty$, perquè $\alpha \in \tilde{\Gamma}$.

6.1.1 Divisors elementals

6.1.2 Volem associar, a cada $\alpha \in \Delta$, una família de "divisors elementals", un per a cada nombre natural primer.

• Si $p \nmid D$, és $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{M}(2, \mathbb{Q}_p)$ i l'isomorfisme pot ésser triat de manera que $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ s'identifiqui amb $\mathrm{M}(2, \mathbb{Z}_p)$. Llavors, vist α en $\mathrm{M}(2, \mathbb{Z}_p)$, existeixen $\varepsilon_1, \varepsilon_2 \in \mathrm{GL}(2, \mathbb{Z}_p)$ tals que $\varepsilon_1\alpha\varepsilon_2 = \begin{bmatrix} p^{e_1} & 0 \\ 0 & p^{e_2} \end{bmatrix}$, on $e_1, e_2 \in \mathbb{Z}$ i $0 \leq e_1 \leq e_2$. El p-èsim divisor elemental associat a α és, per definició, la parella (e_1, e_2).

• Si $p|D$, B_p és un cos no commutatiu i $\mathcal{O}_p$ és l'únic ordre maximal de B_p. Sigui $\pi_p \in \mathcal{O}_p$ un element qualsevol de norma p (l'existència n'és garantida, ja que en B hi ha elements de norma qualsevol nombre racional donat). Ara, l'ideal $\mathcal{O}_p\alpha$ generat per α en $\mathcal{O}_p$ és una certa potència de $\mathcal{O}_p\pi_p$, posem $\mathcal{O}_p\alpha = (\mathcal{O}_p\pi_p)^{e_p}$, on $e_p \in \mathbb{Z}$, $e_p \geq 0$, és un nombre enter independent de l'element π_p elegit de norma p. El p-èsim divisor elemental associat a α és, per definició, e_p.

6.1.3 Proposició. *Siguin $\alpha, \beta \in \Delta$. Les propietats següents són equivalents.*

(a) $\Gamma\alpha\Gamma = \Gamma\beta\Gamma$.

(b) *Per a tot nombre natural primer p, el p-èsim divisor elemental de α coincideix amb el p-èsim divisor elemental de β.*

(c) *Els $\mathcal{O}$-mòduls $\mathcal{O}/\mathcal{O}\alpha$ $\mathcal{O}/\mathcal{O}\beta$ són isomorfs.*

(d) *Existeix $\gamma \in \Gamma$ tal que $\mathcal{O}\alpha\gamma = \mathcal{O}\beta$.* $\square$

Notem que les condicions (a), (c) i (d) són globals, mentre que la condició (b) és intrínsecament local.

6.2 Sèries de Dirichlet formals

Donat un anell R, que suposarem que és commutatiu, l'anell de les sèries de Dirichlet de coeficients en R és l'anell que té per elements les funcions aritmètiques $S : \mathbb{N} - \{0\} \longrightarrow R$; és a dir, les successions $S := (S(1), S(2), \dots, S(n), \dots)$ d'elements $S(n) \in R$. La suma es defineix com la suma de successions, i el producte és la convolució de Dirichlet, definida de la manera següent. Si $S = (S(1), S(2), \dots, S(n), \dots)$ i $T = (T(1), T(2), \dots, T(n), \dots)$, $S(n), T(n) \in R$, llavors,

$$S * T := (U(1), U(2), \dots, U(n), \dots),$$

on, per a tot nombre natural $n \geq 1$, és

$$U(n) := \sum_{d|n} S(d)T(n/d).$$

És un exercici immediat comprovar que aquestes operacions determinen una estructura d'anell, que anomenarem l'anell de les sèries de Dirichlet de coeficients en R.

És usual escriure les sèries de Dirichlet en la forma

$$D(S; s) = \sum_{n \geq 1} S(n) n^{-s},$$

i el producte de Dirichlet s'ha definit de manera que se satisfaci formalment la propietat que

$$\begin{aligned} D(S; s)D(T; s) &= \sum_{n \geq 1} S(n) n^{-s} \sum_{n \geq 1} T(n) n^{-s} \\ &= \sum_{n \geq 1} (S * T)(n) n^{-s} = D(S * T; s), \end{aligned}$$

on els símbols n^{-s} (de moment, només són símbols) satisfan les propietats $(n \cdot m)^{-s} = n^{-s}m^{-s}$, per a tot $m, n \in \mathbb{Z}$, $m, n \geq 1$, per definició.

6.2.1 Observació. Notem que si, per exemple, s és una variable complexa, es pot definir una funció $\mathbb{N} - \{0\} \times \mathbb{C} \longrightarrow \mathbb{C}$ per $(n, s) \mapsto n^{-s}$, de manera que se satisfan les propietats anteriors dels símbols n^{-s}.

6.2.1 Productes d'Euler formals

Sigui $D(S; s)$ una sèrie de Dirichlet formal de coeficients en un anell commutatiu R i suposem que la funció aritmètica $S : \mathbb{N} - \{0\} \longrightarrow R$ és multiplicativa; és a dir, que se satisfà que $S(mn) = S(m)S(n)$, per a $m, n \geq 1$ tals que $\text{mcd}(m, n) = 1$.

En aquest cas, se satisfà la propietat que

$$D(S; s) = \sum_{n \geq 1} S(n)n^{-s} = \prod_{p} \sum_{m \geq 0} S(p^m)p^{-ms} \text{ (producte d'Euler)},$$

el producte estès, com és habitual, al conjunt de tots els nombres naturals primers.

Això és dir que, d'una banda, considerem una infinitat de sèries de Dirichlet, una per a cada nombre primer p,

$$E_p(S; s) := \sum_{m \geq 0} S(p^m)p^{-ms},$$

els coeficients de la qual que corresponen als índexs n que no són potències de p són nuls; i, d'altra banda, que considerem el producte infinit d'aquestes sèries

$$\prod_{p} E_p(S; s).$$

Hem d'observar que cal definir aquest producte infinit; però això no comporta cap problema. En efecte; donat $n \in \mathbb{Z}$, $n \geq 1$, el conjunt de nombres primers p que divideixen n és finit; per tant, per a tot $n \geq 1$, i per al càlcul del coeficient de n^{-s} de la sèrie producte, només intervé una quantitat finita de sèries $E_p(S; s)$ en què el coeficient de

les quals que cal multiplicar és diferent de 1. Així, podem definir el producte infinit, perquè cadascun dels coeficients de la sèrie producte és definit com un producte (finit) d'elements de R.

6.2.2 Observació. Suposem que la funció aritmètica S és completament multiplicativa; és a dir, que la propietat que $S(mn) = S(m)S(n)$ se satisfà per a tota parella de nombres naturals $m, n \geq 1$, sense restricció. Aleshores, per als factors d'Euler se satisfà que

$$E_p(S;s) = \sum_{m\geq 0} S(p^m)p^{-ms} = (1 - S(p)p^{-s})^{-1}.$$

En efecte; observem que $1 - S(p)p^{-s}$ és una sèrie de Dirichlet que només conté els dos sumands que corresponen a $n = 1$ i $n = p$, de manera que el càlcul dels coeficients de la sèrie de Dirichlet producte de $1 - S(p)p^{-s}$ per

$$\sum_{m\geq 0} S(p^m)p^{-ms}$$

és immediat i proporciona la sèrie de Dirichlet 1; és a dir, $1 - S(p)p^{-s}$ és l'element invers, en l'anell de les sèries de Dirichlet, de

$$\sum_{m\geq 0} S(p^m)p^{-ms}.$$

Notem que, de fet, per a un factor d'Euler donat, $E_p(S;s)$, només cal demanar que se satisfaci la propietat que $S(p^m) = S(p)^m$, per a tot $m \geq 0$. Si és així, obtenim que aquest factor d'Euler és

$$E_p(S;s) = \sum_{m\geq 0} S(p^m)p^{-ms} = (1 - S(p)p^{-s})^{-1},$$

independentment de si els altres satisfan o no la propietat anàloga.

6.3 Sèries de Dirichlet a l'anell de Hecke

6.3.1 Definició i propietats

Volem definir una sèrie de Dirichlet de coeficients en l'anell de Hecke $R(\Gamma, \Delta)$; cal, doncs, donar els coeficients.

En el capítol anterior, i per a tot nombre enter $n \geq 1$, s'han definit els elements de Hecke o coeficients de Hecke (més endavant, definirem els *operadors* de Hecke)

$$T(n) := \sum\{(\Gamma\alpha\Gamma) : \alpha \in \Delta, \, \mathrm{n}(\alpha) = n\} \in R(\Gamma, \Delta).$$

6.3.1 Definició. Posarem,

$$D(T; s) := \sum_{n \geq 1} T(n) n^{-s},$$

la sèrie de Dirichlet definida pels coeficients de Hecke $T(n) \in R(\Gamma, \Delta)$.

6.3.2 En el nostre cas, les propietats dels elements Hecke anàlogues a les de **5.1.5** i **5.1.6** es poden escriure en la forma:

• La funció aritmètica $n \mapsto T(n)$ és multiplicativa.

• Si $p|D$, per a tot nombre enter $m \geq 0$, és

$$T(p^m) = T(p)^m.$$

A més a més, si $\alpha \in \Delta$ és un element de norma $\mathrm{n}(\alpha) = p$ i $m \geq 0$, és

$$T(p^m) = (\Gamma\alpha^m\Gamma).$$

• Suposem ara que $p \nmid D$; per a nombres enters $e_1, e_2 \in \mathbb{Z}$ tals que $0 \leq e_1 \leq e_2$, posem

$$T(p^{e_1}, p^{e_2}) := (\Gamma\alpha\Gamma),$$

on $(\Gamma\alpha\Gamma)$ és l'única classe doble amb $\alpha \in \Delta$ caracteritzada pel fet que el p-èsim divisor elemental de α és la parella (e_1, e_2). Llavors:

(a) $T(p^{e_1+1}, p^{e_2+1}) = T(p, p)T(p^{e_1}, p^{e_2})$.

(b) Per a tot $e \geq 1$, $T(p)T(p^e) = T(1, p^{e+1}) + (p+1)T(p, p)T(p^{e-1})$.

(c) Per a tot $e > 1$, $T(1, p)T(1, p^e) = T(1, p^{e+1}) + pT(p, p^e)$.

(d) Per a tot $e \geq 1$, $\deg(T(1, p^m)) = p^{m-1}(p+1)$.

(e) Notem que $T(1) = 1$ i que $T(1, p) = T(p)$; en particular, el cas $e = 1$ de (b) és $T(1, p)^2 = T(1, p^2) + (p+1)T(p, p)$.

(f) Per a $m \geq 2$, se satisfà que

$$T(p^m) = T(1, p^m) + T(p, p)T(p^{m-2}).$$

6.3.2 Producte d'Euler

Les propietats anteriors ens permeten establir fàcilment el resultat següent.

6.3.3 Teorema. *Per a la sèrie de Dirichlet $D(T;s)$ se satisfà que*

$$D(T;s)=\prod_{p|D}(1-T(p)p^{-s})^{-1}\prod_{p\nmid D}(1-T(p)p^{-s}+T(p,p)p^{1-2s})^{-1}.$$

Demostració: Com que la funció aritmètica $n\mapsto T(n)$ és multiplicativa, obtenim de seguida el desenvolupament de $D(T;s)$ com a producte d'Euler de la forma

$$D(T;s)=\sum_{n\geq 1}T(n)n^{-s}=\prod_{p}E_p(T;s),$$

on

$$E_p(T;s)=\sum_{m\geq 0}T(p^m)p^{-ms};$$

doncs, cal estudiar aquests factors.

Suposem, en primer lloc, que p és un divisor de D. El fet que, per a tot $m\geq 0$ sigui $T(p^m)=T(p)^m$ fa que el factor d'Euler $E_p(T;s)$ sigui la sèrie

$$E_p(T;s)=\sum_{m\geq 0}T(p)^mp^{-ms}=(1-T(p)p^{-s})^{-1},$$

com més amunt.

Suposem, finalment, que $p\nmid D$, i calculem els coeficients de la sèrie de Dirichlet producte de les dues sèries $1-T(p)p^{-s}+pT(p,p)p^{-2s}$ i

$$E_p(T;s)=\sum_{m\geq 0}T(p^m)p^{-ms}.$$

Clarament, per als valors de n que no siguin potències de p, els coeficients n-èsims del producte són nuls. A més a més, per a $n=1$, el coeficient del producte és $T(1)=1$; per a $n=p$, el coeficient del

producte és $T(p) - T(p)T(1) = 0$; i, per a $n = p^m$, amb $m \geq 2$, obtenim que el coeficient del producte és

$$\begin{aligned} &T(p^m) - T(p)T(p^{m-1}) + pT(p,p)T(p^{m-2}) \\ =&T(p^m) - (T(1,p^m) + (p+1)T(p,p)T(p^{m-2})) + pT(p,p)T(p^{m-2}) \\ =&T(p^m) - T(1,p^m) - T(p,p)T(p^{m-2}) = 0, \end{aligned}$$

ja que $T(p^m) = T(1,p^m) + T(p,p)T(p^{m-2})$. Això acaba la prova. □

6.3.4 Corol·lari. *Per a tot nombre enter $n \geq 1$, és té*

$$\deg(T(n)) = \sum_{\substack{d|n \\ \mathrm{mcd}(d,D)=1}} d. \quad \square$$

6.4 Operadors de Hecke

6.4.1 Caracterització de l'anell de Hecke

Interessa, a continuació, caracteritzar l'anell de Hecke a partir dels ideals bilaterals coprimers amb el discriminant D de l'àlgebra de quaternions. Per a això, comencem per observar que els subgrups $\Gamma_{\mathfrak{a}}$, per a $\mathfrak{a} = \mathcal{O}\alpha$ un ideal bilateral de $\mathcal{O}$, fan el paper dels subgrups $\Gamma(N) \subseteq \mathrm{SL}(2,\mathbb{Z})$ del cas clàssic. En efecte, se satisfan les propietats següents.

6.4.1 • Si $\mathfrak{a}$, $\mathfrak{b} \subseteq \mathcal{O}$ són ideals bilaterals primers entre si, llavors $\Gamma = \Gamma_{\mathfrak{a}}\Gamma_{\mathfrak{b}}$.

• Si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral de $\mathcal{O}$ i $\alpha, \beta \in \Delta$ són elements tals que $\mathrm{mcd}(\mathrm{n}(\alpha), \mathfrak{a}) = \mathrm{mcd}(\mathrm{n}(\beta), \mathfrak{a}) = 1$, llavors, condició necessària i suficient perquè sigui $\Gamma_{\mathfrak{a}}\alpha = \Gamma_{\mathfrak{a}}\beta$ és que sigui $\Gamma\alpha = \Gamma\beta$ i, alhora, $\alpha \equiv \beta \pmod{\mathfrak{a}}$.

• Si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral i $\alpha \in \Delta$ és un element tal que $\mathrm{mcd}(\mathrm{n}(\alpha), \mathfrak{a}) = 1$, llavors,

(a) $\Gamma\alpha\Gamma = \Gamma\alpha\Gamma_{\mathfrak{a}} = \Gamma_{\mathfrak{a}}\alpha\Gamma$.

(b) $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \{\beta \in \Gamma\alpha\Gamma : \beta \equiv \alpha \pmod{\mathfrak{a}}\}$.

(c) Si $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \biguplus_i \Gamma_{\mathfrak{a}}\alpha_i$, llavors, $\Gamma\alpha\Gamma = \biguplus_i \Gamma\alpha_i$.

6.4.2 Definició. Per a tot ideal bilateral $\mathfrak{a} \subseteq \mathcal{O}$, posarem $\Delta_{\mathfrak{a}} := \{\alpha \in \Delta : \mathrm{mcd}(\mathrm{n}(\alpha), \mathfrak{a}) = 1\}$.

6.4.3 Definició. Si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral tal que $\mathrm{mcd}(D, \mathfrak{a}) = 1$, llavors existeix un nombre enter $a \in \mathbb{Z}$, $a > 0$, tal que $\mathfrak{a} = a\mathcal{O}$ i $\mathcal{O}/\mathfrak{a} = \mathcal{O}/a\mathcal{O} \simeq \mathrm{M}(2, \mathbb{Z}/a\mathbb{Z})$. Posarem $\Delta^*_{\mathfrak{a}} := \{\alpha \in \Delta_{\mathfrak{a}} :$ existeix $c \in \mathbb{Z}/a\mathbb{Z}$ tal que $\alpha \equiv \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \pmod{a}\}$.

El conjunt $\Delta^*_{\mathfrak{a}}$ és un subsemigrup de B^* que conté $\Gamma_{\mathfrak{a}}$ i que, alhora, està inclòs en el commensurador de $\Gamma_{\mathfrak{a}}$. Per tant, podem parlar, també, de l'anell de Hecke $R(\Gamma_{\mathfrak{a}}, \Delta^*_{\mathfrak{a}})$. Se satisfà el resultat següent, que permet caracteritzar l'anell de Hecke $R(\Gamma, \Delta)$.

6.4.4 Proposició. *Si* $\mathfrak{a} \subseteq \mathcal{O}$ *és un ideal bilateral tal que* $\mathrm{mcd}(D, \mathfrak{a}) = 1$*, l'assignació*

$$\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} \mapsto \Gamma\alpha\Gamma$$

defineix un isomorfisme $R(\Gamma_{\mathfrak{a}}, \Delta^*_{\mathfrak{a}}) \longrightarrow R(\Gamma, \Delta)$ *entre els anells de Hecke.* □

Notem que, ara, el grup $\Gamma_{\mathfrak{a}}$ ja no és el grup de les unitats de norma 1 d'un ordre maximal de B, sinó que n'és un cert subgrup.

6.4.2 Formes modulars

Posarem $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, el semiplà superior de Poincaré, i considerarem l'acció usual de $\mathrm{GL}^+(2, \mathbb{R})$ en $\mathcal{H}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az + b}{cz + d};$$

denotarem per $j\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z\right)$ el nombre complex $cz + d$.

6.4.5 La representació (fidel) $\chi : B \longrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R})$ identifica Γ amb un subgrup discret de $\mathrm{GL}^+(2,\mathbb{R})$. En particular, per a tot ideal bilateral $\mathfrak{a} \subseteq \mathcal{O}$ i per a tot nombre enter $k \geq 0$ podem parlar de les formes parabòliques de pes k respecte de $\Gamma_{\mathfrak{a}}$; sigui $S_k(\Gamma_{\mathfrak{a}})$ l'espai vectorial complex d'aquestes formes parabòliques.

Recordem que f és una forma parabòlica de $S_k(\Gamma_{\mathfrak{a}})$ si:

(a) $f : \mathcal{H} \longrightarrow \mathbb{C}$ és una funció holomorfa;

(b) per a tot $\gamma \in \Gamma_{\mathfrak{a}}$ i tot $z \in \mathcal{H}$ és $f(\gamma(z))j(\gamma,z)^{-k} = f(z)$; i

(c) f s'anul·la en les puntes de $\Gamma_{\mathfrak{a}}$.

6.4.6 Definició. Sigui $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral. Donada una classe doble $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}$, $\alpha \in \Delta^*_{\mathfrak{a}}$, considerem una descomposició

$$\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \biguplus_i \Gamma_{\mathfrak{a}}\alpha_i$$

i, a cada $f \in S_k(\Gamma_{\mathfrak{a}})$, associem-li la funció $g(z)$ definida per

$$g(z) := \mathrm{n}(\alpha)^{k-1} \sum_i f(\alpha_i(z))j(\alpha_i,z)^{-k}.$$

6.4.7 Se satisfan les propietats següents:

• La funció g no depèn ni de α ni de la família de representants $\{\alpha_i\}_i$; només depèn de la classe doble $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}$ (i, naturalment, de la funció f).

• $g \in S_k(\Gamma_{\mathfrak{a}})$; és a dir, $g(z)$ és una forma parabòlica de pes k per a $\Gamma_{\mathfrak{a}}$.

• L'aplicació

$$(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k : S_k(\Gamma_{\mathfrak{a}}) \longrightarrow S_k(\Gamma_{\mathfrak{a}}),$$

definida per l'assignació

$$f \mapsto f|(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k := g,$$

és $\mathbb{C}$-lineal.

6.4.8 Proposició. *L'aplicació* $R(\Gamma_\mathfrak{a}, \Delta_\mathfrak{a}^*) \longrightarrow \mathrm{End}_\mathbb{C}(S_k(\Gamma_\mathfrak{a}))$, *definida per l'assignació* $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a}) \mapsto (\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_k$ *i estesa per linealitat, és una representació de l'anell de Hecke* $R(\Gamma, \Delta) \simeq R(\Gamma_\mathfrak{a}, \Delta_\mathfrak{a}^*)$ *en l'espai de les formes parabòliques* $S_k(\Gamma_\mathfrak{a})$. □

6.4.9 Si prenem una $\mathbb{C}$-base $\{f_1, \ldots, f_m\}$ de $S_k(\Gamma_\mathfrak{a})$, obtenim un isomorfisme d'anells $\mathrm{End}_\mathbb{C}(S_k(\Gamma_\mathfrak{a})) \simeq \mathbf{M}(m, \mathbb{C})$ i, per composició, una representació $R(\Gamma_\mathfrak{a}, \Delta_\mathfrak{a}^*) \longrightarrow \mathbf{M}(m, \mathbb{C})$, on designem per $\mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ la imatge de $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$. Així, $\mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a}) \in \mathbf{M}(m, \mathbb{C})$ és una matriu tal que, si posem $\mathbf{f} := \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix}$, és

$$\mathbf{f}|(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_k = \mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})\mathbf{f}.$$

Se satisfan les propietats següents.

• Si $\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a} = \biguplus_i \Gamma_\mathfrak{a}\alpha_i$, llavors $\Gamma_\mathfrak{a}\alpha'\Gamma_\mathfrak{a} = \biguplus_i \alpha_i'\Gamma_\mathfrak{a}$; i, per a tota funció $f \in S_k(\Gamma_\mathfrak{a})$, és

$$f|(\Gamma_\mathfrak{a}\alpha'\Gamma_\mathfrak{a})_k = \mathrm{n}(\alpha^{-1}) \sum_i f(\alpha_i'^{-1}(z)) j(\alpha_i'^{-1}, z)^{-k}.$$

• En particular, si $b \in \mathbb{Z}$, $b > 0$, obtenim que

$$f|(\Gamma_\mathfrak{a} b \Gamma_\mathfrak{a})_k = b^{k-2} f.$$

6.4.10 Proposició. *L'assignació* $\alpha \mapsto \mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ *proporciona una representació del grup* Γ *tal que* $\Gamma_\mathfrak{a}$ *està inclòs en el nucli de la representació; per tant, una representació de* $\Gamma/\Gamma_\mathfrak{a}$. □

6.4.3 Operadors de Hecke i sèries de Dirichlet

6.4.11 Definició. Sigui $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral tal que $\mathrm{mcd}(D, \mathfrak{a}) = 1$. Per a tot nombre enter $b \in \mathbb{Z}$ tal que $\mathrm{mcd}(b, \mathfrak{a}) = 1$, existeix un element $\gamma \in \Gamma$ tal que $\gamma \equiv \begin{bmatrix} b^{-1} & 0 \\ 0 & b \end{bmatrix} \pmod{\mathfrak{a}}$, i la matriu $\mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ és determinada unívocament per b; escriurem $R_k(b; \mathfrak{a}) := \mathcal{T}_k(\Gamma_\mathfrak{a}\gamma\Gamma_\mathfrak{a})$.

6.4.12 Definició. Anàlogament, per a tot nombre natural n i tot nombre primer p tal que $p \nmid D$, escriurem $T(n;\mathfrak{a})$, $T(p,p;\mathfrak{a})$ les imatges en $R(\Gamma_\mathfrak{a},\Delta_\mathfrak{a}^*)$ dels elements $T(n)$, $T(p,p)$, i $\mathcal{T}_k(n;\mathfrak{a})$, $\mathcal{T}_k(p,p;\mathfrak{a})$ les imatges en $\mathbf{M}(m,\mathbb{C})$, respectivament.

6.4.13 Si $\gamma \in \Gamma$ és un element tal que $\gamma \equiv \begin{bmatrix} p^{-1} & 0 \\ 0 & p \end{bmatrix} \pmod{\mathfrak{a}}$, llavors $p\gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & p^2 \end{bmatrix} \pmod{\mathfrak{a}}$, i $\mathcal{T}_k(p,p;\mathfrak{a}) = p^{k-2}R_k(p;\mathfrak{a})$.

Aquestes propietats formals dels operadors de Hecke —observem que, efectivament, ara són operadors lineals, mentre que abans eren elements d'un anell abstracte—, permeten escriure el resultat següent.

6.4.14 Teorema. *Sigui $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral tal que $\operatorname{mcd}(D,\mathfrak{a}) = 1$. Siguin $k \geq 0$ un nombre enter i m la dimensió de l'espai $S_k(\Gamma_\mathfrak{a})$, de les formes parabòliques, i fixem una $\mathbb{C}$-base, $\mathbf{f}$, d'aquest espai, respecte de la qual considerarem la representació matricial de l'anell de Hecke $R(\Gamma_\mathfrak{a},\Delta_\mathfrak{a}^*)$. Aleshores, com a sèries de Dirichlet de matrius de $\mathbf{M}(m,\mathbb{C})$, se satisfà la igualtat*

$$\sum_{\substack{(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a}) \\ \alpha \in \Delta_\mathfrak{a}^*}} \mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})\,\mathrm{n}(\alpha)^{-s} = \sum_{\operatorname{mcd}(n,\mathfrak{a})=1} \mathcal{T}_k(n;\mathfrak{a})n^{-s}.$$

D'altra banda, també es té la descomposició en producte de factors d'Euler

$$\sum_{\operatorname{mcd}(n,\mathfrak{a})=1} \mathcal{T}_k(n;\mathfrak{a})n^{-s} =$$

$$= \prod_{p|D}(1-\mathcal{T}_k(p;\mathfrak{a})p^{-s})^{-1} \prod_{p\nmid D\mathfrak{a}}(1-\mathcal{T}_k(p;\mathfrak{a})p^{-s}+R_k(p;\mathfrak{a})p^{k-1-2s})^{-1}.$$

A més a més, per a la topologia usual de $\mathbf{M}(m,\mathbb{C})$, la sèrie és convergent per a tot nombre complex $s \in \mathbb{C}$ tal que $\operatorname{Re}(s) > k+1$.

Demostració: Les igualtats formals es dedueixen immediatament del resultat anàleg formal; només cal preocupar-se de les qüestions de convergència.

Per a cada forma parabòlica $f \in S_k(\Gamma_\mathfrak{a})$, definim $f^* : \mathrm{SL}(2,\mathbb{R}) \longrightarrow \mathbb{C}$ per l'assignació $\beta \mapsto f^*(\beta) := f(\beta(i))j(\beta,i)^{-k}$, on $i^2 = -1$. Ara, si $\mathfrak{a} \subseteq \mathcal{O}$ és un ideal bilateral, $\alpha \in \Delta^*_\mathfrak{a}$, $\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a} = \biguplus_i \Gamma_\mathfrak{a}\alpha_i$, i $f \in S_K(\Gamma_\mathfrak{a})$ és una forma parabòlica qualsevol, podem considerar la funció g^* definida a partir de la forma parabòlica $g := f|(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_k$; obtenim immediatament que, per a tot $\beta \in \mathrm{SL}(2,\mathbb{R})$, se satisfà la igualtat

$$g^*(\beta) = \mathrm{n}(\alpha)^{k-1} \sum_i f^*(\alpha_i\beta).$$

Com que per a tot $\gamma \in \Gamma_\mathfrak{a}$ i tot $\beta \in \mathrm{SL}(2,\mathbb{R})$ és $f^*(\gamma\beta) = f^*(\beta)$, podem considerar la funció g^* com una funció definida en el conjunt quocient $\Gamma_\mathfrak{a}\backslash \mathrm{SL}(2,\mathbb{R})$, que és compacte (recordem que l'àlgebra de quaternions és indefinida), de manera que g^* assoleix el màxim en algun punt de $\mathrm{SL}(2,\mathbb{R})$. Com a conseqüència, s'obté que les arrels característiques de l'operador $\mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ són fitades, en valor absolut, per $\mathrm{n}(\alpha)^{k-1}\deg(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$.

Si ara tenim en compte que, per a una certa base de $S_k(\Gamma_\mathfrak{a})$, tots els operadors $\mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ són diagonals (cf. més avall), el corol·lari 3.5 ens serveix per a concloure que la sèrie de Dirichlet és absolutament convergent per a $\mathrm{Re}(s) > k+1$, com volíem demostrar. □

Resta provar que, per a una certa base de $S_k(\Gamma_\mathfrak{a})$, tots els operadors $\mathcal{T}_k(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ són diagonals. Per a això, comencem per observar que si $\varepsilon \in \mathcal{O}$ és un element de norma $\mathrm{n}(\varepsilon) = -1$, i si considerem l'operador $T(\varepsilon)_k \in \mathrm{End}_\mathbb{Z}(S_k(\Gamma_\mathfrak{a}))$ definit per

$$f|T(\varepsilon)_k(z) := f(\varepsilon(\overline{z}))j(\varepsilon,z)^{-k},$$

on la barra indica la conjugació complexa, llavors, per a tot nombre complex $a \in \mathbb{C}$, és $(af)|T(\varepsilon)_k = \overline{a}(f|T(\varepsilon)_k)$; és a dir, $T(\varepsilon)_k$ és un operador hermitià en $S_k(\Gamma_\mathfrak{a})$.

D'altra banda, en el cas en què $\mathfrak{a}$ sigui un ideal bilateral tal que $\mathrm{mcd}(D,\mathfrak{a}) = 1$, podem prendre $\varepsilon \equiv \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{\mathfrak{a}}$, i obtenim que $\varepsilon^2 \in \Gamma_\mathfrak{a}$ i que, per a tot $\alpha \in \Delta^*_\mathfrak{a}$, és $\varepsilon^{-1}\alpha\varepsilon \equiv \alpha \pmod{\mathfrak{a}}$. Això implica que és $T(\varepsilon)_k^2 = 1$ i que $T(\varepsilon)_k$ commuta amb tots els operadors $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_k$.

Com a conseqüència d'aquestes propietats, els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$ són tots hermitians respecte de la mètrica de Petersson i formen un anell commutatiu d'operadors normals; en conseqüència, obtenim el resultat següent.

6.4.15 Proposició. *Per a tot ideal bilateral $\mathfrak{a} \subseteq \mathcal{O}$ existeix una base de $S_k(\Gamma_{\mathfrak{a}})$ tal que tots els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$, $\alpha \in \Delta_{\mathfrak{a}}^*$, són representats per matrius diagonals.* □

6.4.16 Corol·lari. *Per a tot nombre natural parell k i tot element $\alpha \in \Delta$, les arrels característiques dels operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$ són nombres enters algebraics. A més a més, si $\mathfrak{a} = \mathcal{O}$, aquestes arrels característiques són nombres totalment reals.* □

Finalment, en el cas que $\mathfrak{a} = \mathcal{O}$, observem que podem elegir una base de $S_k(\Gamma_{\mathfrak{a}})$ formada per elements invariants per a l'operador $T(\varepsilon)_k$; per a aquesta base, els operadors $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_k$, $\alpha \in \Delta_{\mathfrak{a}}^*$, són representats per matrius de coeficients reals.

Suposem, ara, que B és un cos no commutatiu; és a dir, que l'àlgebra de quaternions B no és isomorfa a l'àlgebra de matrius $\mathrm{M}(2, \mathbb{Q})$.

Un procés d'adelització, que inclou considerar les adeles i les ideles de B, però no només aquestes, més l'elecció de mesures de Haar adequades i anàlisi harmònica en els grups de les adeles i de les ideles, més la fórmula de Selberg, més la fórmula de sumació de Poisson, més l'ús de transformades de Fourier, etcètera, permeten obtenir el teorema següent, en el qual només fem la descripció de l'equació funcional en el cas en què $\mathfrak{a} = \mathcal{O}$.

6.4.17 Teorema. *Siguin $\mathfrak{a} \subseteq \mathcal{O}$ un ideal bilateral tal que $\mathrm{mcd}(D, \mathfrak{a}) = 1$, i $k \geq 0$ un nombre enter. Posem*

$$H_k(s; \mathfrak{a}) := D^{s/2}(2\pi)^{-s}\Gamma(s) \sum_{\mathrm{mcd}(n,\mathfrak{a})=1} \mathcal{T}_k(n; \mathfrak{a})n^{-s}.$$

Llavors, $H_k(s; \mathfrak{a})$ és una funció holomorfa en tot $\mathbb{C}$, per a la qual se satisfà una certa equació funcional. Per al cas en què $\mathfrak{a} = \mathcal{O}$, una equació funcional es pot escriure en la forma

$$H_k(s; \mathcal{O}) = \Lambda H_k(k - s; \mathcal{O}),$$

on

$$\Lambda := (-1)^{k/2} \prod_{p|D} p^{k/2-1} \mathcal{T}_k(p; \mathcal{O})$$

és un nombre tal que $\Lambda^2 = 1$. □

Aquest teorema és el punt de partida per a l'obtenció del següent; l'altre ingredient bàsic és la fórmula de congruència de què parlarem en les dues subseccions següents.

6.4.18 Teorema. *Siguin B una $\mathbb{Q}$-àlgebra de quaternions indefinida i $\mathcal{O} \subseteq B$ un ordre maximal. Siguin $D := \operatorname{disc}(B) = \operatorname{disc}(\mathcal{O})$ el discriminant de l'àlgebra i de l'ordre, i $N \in \mathbb{Z}$, $N > 0$, un nombre enter tal que $\operatorname{mcd}(D, N) = 1$. Considerem el grup de congruència*

$$\Gamma_N := \{\gamma \in \mathcal{O}^* : \mathrm{n}(\gamma) > 0, \, \gamma \equiv 1 \pmod{N\mathcal{O}}\}.$$

Llavors, existeix una corba algebraica llisa $X(D, \Gamma_N)$, definida sobre $\mathbb{Q}$, anomenada corba de Shimura, tal que

(a) *el cos de les funcions de $X(D, \Gamma_N)$ és isomorf al cos de les funcions automorfes respecte de Γ_N.*

(b) *la funció zeta de $X(D, \Gamma_N)$ sobre $\mathbb{Q}$ s'escriu en la forma*

$$\zeta(s; X(D, \Gamma_N)) = f(s)\zeta(s)\zeta(s-1)D(s)^{-1},$$

on $f(s)$ és un producte de funcions racionals de p^{-s}, per a un conjunt finit de nombres primers p, $\zeta(s)$ és la funció zeta de Riemann, i

$$D(s) = \det\left(\sum_{\operatorname{mcd}(n,N)=1} \mathcal{T}_2(n; N\mathcal{O}) n^{-s} \right). \, \square$$

Per tant, la funció zeta $\zeta(s; X(D, \Gamma_N))$ admet prolongació meromorfa a tot $\mathbb{C}$ i satisfà una certa equació funcional, deduïda de l'equació funcional per a $D(s)$.

6.4.4 Correspondències modulars

Recordem que, si C és una corba llisa, una correspondència pròpia de C és un divisor de $C \times C$ sense components de cap de les formes $x \times C$ ni $C \times x$, per a $x \in C$; i que les correspondències pròpies de C formen un anell, en el qual la permutació dels dos factors del producte cartesià $C \times C$ indueix un antiautomorfisme, $x \mapsto {}^t x$, anomenat involució de Rosati.

En interessa especialment el cas en què $C = X(D, \Gamma_N)$ és la corba de Shimura definida més amunt; notem que el cas $N = 1$ correspon a la corba $X(D, \Gamma)$. Per a qualsevol element $\alpha \in \Delta$, posem $\Gamma(\alpha) := \Gamma \cap \alpha^{-1}\Gamma\alpha$ i sigui $f_1 : \Gamma(\alpha)\backslash\mathcal{H} \longrightarrow X(D, \Gamma)$ la projecció canònica. D'altra banda, per a tot $z \in \mathcal{H}$ i tot $\alpha \in \Delta$, és $\alpha\Gamma(\alpha)z \subseteq \Gamma\alpha z$; per tant, obtenim immediatament una altra aplicació $f_2 : \Gamma(\alpha)\backslash\mathcal{H} \longrightarrow X(D, \Gamma)$.

6.4.19 Proposició. *Per a tot element $\alpha \in \Delta$, la imatge de $\Gamma(\alpha)\backslash\mathcal{H}$ en $X(D, \Gamma) \times X(D, \Gamma)$ per l'aplicació (f_1, f_2) és una correspondència pròpia, que només depèn de la classe doble $\Gamma\alpha\Gamma$.* □

6.4.20 Definició. Aquesta correspondència s'anomena la correspondència modular, i l'escriurem en la forma $\mathrm{md}(\Gamma\alpha\Gamma)$.

6.4.21 • L'aplicació $\Gamma\alpha\Gamma \mapsto \mathrm{md}(\Gamma\alpha\Gamma)$ indueix un morfisme d'anells de l'anell de Hecke $R(\Gamma, \Delta)$ en l'anell de les correspondències modulars pròpies, definides sobre $\mathbb{Q}$, de la corba de Shimura.

• Per a tot nombre primer p, es té que la correspondència modular associada a l'element $T(p, p)$ és la identitat.

• Si $\Gamma\alpha\Gamma = \biguplus_i \Gamma\alpha_i$, i si pr indica la projecció canònica de $\mathcal{H}$ en $X(D, \Gamma_N)$, es té que

$$\mathrm{md}(\mathrm{pr}(z)) = \sum_i \mathrm{pr}(\alpha_i(z)).$$

6.4.5 Fórmula de congruència

6.4.22 Proposició. *Siguin red_p la reducció mòdul un nombre primer p que no divideixi el discriminant D de l'àlgebra de quaternions i que*

sigui un primer de bona reducció; $\mathrm{red}_p(T(p))$ *la reducció mòdul* p *de l'operador* $T(p)$ *vist com a correspondència sobre* $\mathrm{red}_p(X(D,\Gamma))$*; i* π_p *la correspondència de Frobenius de* $\mathrm{red}_p(X(D,\Gamma))$*; és a dir, el graf de l'aplicació que eleva a la potència* p *les coordenades homogènies dels punts. Se satisfà la fórmula de congruència:*

$$\mathrm{red}_p(T(p)) = \pi_p + {}^t\pi_p. \ \square$$

Per al cas més general de la corba $X(D,\Gamma_N)$, la fórmula de congruència no és tan senzilla; de fet, la demostració presenta algunes complicacions tècniques i cal introduir un automorfisme convenient Y_N de la corba $X(D,\Gamma_N)$ que deixa invariants les fibres de $X(D,\Gamma_N) \longrightarrow X(D,\Gamma)$.

En aquest cas, la fórmula de congruència s'escriu de la forma

$$\begin{aligned} \mathrm{red}_p(T(p)) &= \pi_p + {}^t\pi_p \circ \mathrm{red}_p(Y_p), \\ {}^t\pi_p \circ \mathrm{red}_p(Y_p) &= {}^t\mathrm{red}_p(Z) \circ {}^t\pi_p \circ \mathrm{red}_p(Z), \end{aligned}$$

on Z és un automorfisme convenient de $X(D,\Gamma_N)$ definit sobre $\mathbb{Q}$.

6.5 Reducció de les corbes de Shimura

Per als primers de bona reducció de les corbes de Shimura que apareixen a la fórmula de congruència, cal tenir en compte el teorema de Morita dels primers de bona reducció.

6.5.1 • Mantinguem la hipòtesi que la $\mathbb{Q}$-àlgebra de quaternions indefinida B sigui un cos no commutatiu; és a dir, que no sigui isomorfa a l'àlgebra de matrius $\mathrm{M}(2,\mathbb{Q})$. Siguin $\mathcal{O}$ un ordre maximal i D el seu discriminant.

• Siguin G el grup algebraic, definit sobre $\mathbb{Q}$, tal que $G_{\mathbb{Q}} = B^*$; i G_A, l'adelització de G.

• Notem que $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R})$, de manera que la projecció en ∞ de G_A és $\mathrm{M}(2,\mathbb{R})$; per tant, podem considerar $G_{A,+} := \{x \in G_A : \det x_\infty > 0\}$.

• Siguin $G_{\infty,+} := \mathrm{GL}^+(2,\mathbb{R})$ la part arquimediana, i G_0 la part finita de $G_{A,+}$; i $G_{\mathbb{Q},+} := G_{A,+} \cap G_{\mathbb{Q}} = G_{A,+} \cap B^*$.

• Sigui $\mathcal{S}$ la família dels subgrups $S \subseteq G_{A,+}$ tals que S és de la forma $S = G_{\infty,+} \cdot S_0$, on S_0 és qualsevol subgrup compacte i obert de G_0.

• Per a tot $S \in \mathcal{S}$, sigui $\Gamma_S := S \cap G_{\mathbb{Q},+} \subseteq \mathrm{GL}(2,\mathbb{R})$. Així, Γ_S actua en el semiplà $\mathcal{H}$ i l'espai quocient $\Gamma_S\backslash\mathcal{H}$ defineix una corba completa i no singular.

• Per teoria de cossos de classes, i si $\mathrm{n} : B^* \longrightarrow \mathbb{Q}^*$ és la norma reduïda, al subgrup $\mathrm{n}(S)\mathbb{Q}^* \subseteq \mathbb{Q}_A^*$ de les ideles de $\mathbb{Q}$ li correspon una extensió abeliana de $\mathbb{Q}$, que denotarem per $k_S|\mathbb{Q}$.

• En aquesta situació (i, més generalment, en una situació anàloga on $\mathbb{Q}$ es pot canviar per un cos de nombres totalment real, F, i B per una F-àlgebra de quaternions que sigui un cos i tal que $B \otimes_{\mathbb{Q}} \mathbb{R}$ sigui el producte d'una sola còpia de $\mathrm{M}(2,\mathbb{R})$ i, la resta, còpies dels quaternions de Hamilton), podem parlar de la corba de Shimura X_S; és una corba algebraica llisa, definida sobre k_S, i isomorfa, a nivell de punts complexos, a $\Gamma_S\backslash\mathcal{H}$.

6.5.2 Teorema. *Amb les notacions i les hipòtesis anteriors, i per a tot $S \in \mathcal{S}$, sigui P_S el conjunt dels ideals primers $\mathfrak{q}$ de k_S tals que $\mathfrak{q} \nmid D$ i existeix $x_p \in G_{\mathbb{Q},+}$ per al qual $S \subseteq x_p^{-1}\mathcal{O}_p^* x_p$, on $p\mathbb{Z} := \mathfrak{q} \cap \mathbb{Q}$, i $\mathcal{O}_p$ és la compleció p-àdica de $\mathcal{O}$. Llavors,*

(a) *P_S és un conjunt d'ideals primers de $\mathcal{O}_{k_S}$, tots llevat d'una quantitat finita.*

(b) *La corba de Shimura X_S admet un model enter sobre $\mathcal{O}_{k_S}$ que té bona reducció per a tot $\mathfrak{q} \in P_S$.* □

6.6 El teorema de comparació

Acabarem l'exposició amb l'enunciat d'un teorema de comparació aplicable a les funcions zeta associades a corbes de Shimura que corresponen a àlgebres de quaternions de discriminants diferents i a ordres de nivells diferents en aquestes àlgebres.

Fixem notacions.

• Siguin D, D', p nombres enters, p primer, tals que $DD'p$ sigui lliure

de quadrats.

• Siguin B una $\mathbb{Q}$-àlgebra de quaternions de discriminant D, i $\mathcal{O} \subseteq B$ un ordre d'Eichler de nivell D' cf. Rio, capítol 1.

• Siguin B' una $\mathbb{Q}$-àlgebra de quaternions de discriminant D, i $\mathcal{O}' \subseteq B'$ un ordre d'Eichler de nivell $D'p$.

• Siguin B'' una $\mathbb{Q}$-àlgebra de quaternions de discriminant Dp, i $\mathcal{O}'' \subseteq B''$ un ordre d'Eichler de nivell D'.

• Notem que B i B' són àlgebres del mateix discriminant i que el discriminant de B'' té exactament un divisor primer més. Per tant, si B, B' són indefinides, llavors B'' és definida; i, recíprocament, si B, B' són definides, llavors B'' és indefinida.

• Si considerem el grup de les ideles de B, $\mathcal{I}$, i el grup de les $\mathcal{O}$-unitats de $\mathcal{I}$, $\mathcal{U}$, per adelització de les nocions establertes en les seccions anteriors, podem parlar, per a tot nombre enter $k > 0$, d'un espai de funcions automorfes de pes k i d'una representació $\mathcal{T}_k$ de l'anell de Hecke $R(\mathcal{U}, \mathcal{I})$ en aquest espai.

• En conseqüència, podem parlar de la sèrie de Dirichlet

$$\mathcal{D}(s) := \sum_{n \geq 1} \mathcal{T}_k(T(n)) n^{-s};$$

aquesta sèrie és convergent per a $\Re(s) \gg 0$, i admet un producte d'Euler de la forma

$$\mathcal{D}(s) = \prod_{\ell} \mathcal{E}_\ell(s).$$

• Com que les sèries i els factors depenen de l'àlgebra i de l'ordre, escriurem $\mathcal{D}(B, \mathcal{O}; s)$ per a designar aquesta dependència.

• Escriurem $\mathcal{D}'(B, \mathcal{O}; s) := \prod_{\ell \neq p} \mathcal{E}_\ell(B, \mathcal{O}; s)$ el producte de tots els factors d'Euler, llevat el que correspon al primer p, fixat a l'inici.

• Un cop fixada una base de l'espai de representació, és a dir, de l'espai de funcions automorfes, la funció $\mathcal{D}(B, \mathcal{O}; s)$ pren valors en un espai de matrius. Per a $a, b \in \mathbb{Z}$, $a, b \geq 0$, i per a matrius X, Y, escriurem $aX \oplus bY$ per a designar la suma directa de a còpies de la matriu X i b còpies de la matriu Y.

6.6.1 Teorema. (Eichler, Shimizu) *Amb aquestes notacions i hipòtesis, se satisfà que*

(a) $\mathcal{D}'(B', \mathcal{O}'; s) = \mathcal{D}'(B'', \mathcal{O}''; s) \oplus 2\mathcal{D}'(B, \mathcal{O}; s)$.

(b) $\mathcal{D}(B, \mathcal{O}; s)$ *només depèn de* D *i de* D'*, però no de l'àlgebra de quaternions de discriminant* D *ni de l'ordre de nivell* D' *que considerem.* $\square$

Bibliografia

[Bor65] A. Borel, *Opérateurs de Hecke et fonctions zêta*, Séminaire Bourbaki, Vol. 9, exp.307, Soc. Math. France, 1965, pp. 441–463.

[Mor81] Y. Morita, *Reduction mod* $\mathfrak{p}$ *of Shimura curves*, Hokkaido Math. J. **10** (1981), num. 2, 209–238.

[Shi61] G. Shimura, *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), num. 3, 275–331.

[Shi65] H. Shimizu, *On zeta functions of quaternion algebras*, Ann. of Math. **81** (1965), 166–193.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

Capítol 7

Racionalitat de punts de corbes de Shimura

M. Alsina

En aquest capítol descriurem els principals resultats coneguts relatius als punts de les corbes de Shimura.

Considerem el model canònic $X(D,N)$ de la corba de Shimura associada a un ordre d'Eichler de nivell N en una àlgebra de quaternions H racional indefinida i de discriminant D. L'ordre el denotem $\mathcal{O}(D,N)$. Fixat un discriminant D i un nivell N, escriurem $X := X(D,N)$, $\mathcal{O} := \mathcal{O}(D,N)$.

En el cas $D = 1$, que anomenem cas no ramificat, s'obté la corba modular $X(1,N) = X_0(N)$. En aquest cas hi ha resultats ben coneguts i abundant experimentació numèrica, que no inclourem en aquesta descripció. En el cas $D > 1$, que anomenem cas ramificat, es coneixen molts menys resultats efectius. Concretament, pel que fa a la qüestió dels punts de les corbes de Shimura notem que la majoria de resultats coneguts són només existencials. Cal tenir en compte també que sovint s'apliquen només a $N = 1$, és a dir, que l'ordre de l'àlgebra de quaternions és maximal, o incorporen restricions sobre D. En particular, anomenarem cas poc ramificat el cas en què D és producte de tan sols dos nombres primers, $D = pq$. Per a més

detalls sobre les notacions, definicions i resultats bàsics de corbes de Shimura cf. [Als00a].

Al llarg d'aquesta exposició ens situarem sempre en el cas ramificat $D > 1$, que no inclou les corbes modulars.

En la primera secció esmentem el remarcable resultat de Shimura sobre la no-existència de punts reals ni, per tant, racionals; tractem també les corbes obtingudes fent quocient per involucions, que sí que poden tenir punts reals. La segona secció és dedicada als punts locals, sobre $\mathbb{Q}_p$ i sobre un cos local $K|\mathbb{Q}_p$. Posarem especial atenció també en l'existència de classes de divisors racionals sobre cossos locals, de manera que, com a aplicació, s'obtenen resultats sobre grups de Tate-Shafarevich. Dediquem la tercera secció a l'estudi dels punts de corbes de Shimura sobre cossos de nombres, on s'obtenen resultats de finitud, a partir de la interpretació modular i de la hiperel·lipticitat i biel·lipticitat de les corbes.

7.1 Punts reals de corbes de Shimura

G. Shimura va dur a terme l'estudi dels punts reals i donà el resultat remarcable següent.

7.1.1 Teorema. (cf. [Shi75]) *Sigui $X(D,N)$ la corba de Shimura associada a un ordre d'Eichler de nivell N en una àlgebra de quaternions de discriminant D. Aleshores, $X(D,N)(\mathbb{R}) = \emptyset$.*

Notem que, en particular, això implica la no-existència de punts racionals, la qual cosa comporta una situació molt diferent del cas de les corbes modulars. De fet, el resultat provat per Shimura és molt més general i inclou el cas modular. Donada una varietat de Shimura V associada a una àlgebra de quaternions H, demostrà que $V(\mathbb{R}) \neq \emptyset$ si, i només si, o bé la dimensió de la varietat V és parella o bé l'àlgebra de quaternions és l'àlgebra de matrius.

Això completà l'estudi dels punts reals de les corbes de Shimura i donà peu a traslladar la qüestió de l'existència de punts reals als quocients de les corbes per l'acció donada per les involucions d'Atkin.

L'estudi dels quocients fou dut a terme principalment per A. Ogg, cf. [Ogg83], i se'n dedueixen resultats com ara la determinació de les corbes de Shimura hiperel·líptiques. R. Roberts [Rob89] ho utilitzà també per a iniciar una classificació efectiva d'aquests quocients. Sigui $w := w(m)$ la involució d'Atkin associada a $m|DN$. Escriurem $X(D,N)^{(m)}$, o bé $X^{(m)}$, el quocient $X(D,N)/w(m)$. L'existència de punts reals es determina a partir del teorema següent.

7.1.2 Teorema. (cf. [Ogg83]) *Suposem $N = 1$. Aleshores tenim $X^{(m)}(\mathbb{R}) \neq \emptyset$ si, i només si, m no és un quadrat i existeix una immersió $\mathbb{Q}(\sqrt{m}) \hookrightarrow H$.*

En el treball d'Ogg es donen també fórmules explícites per a comptar el nombre de components dels punts reals del quocient $X^{(m)}(\mathbb{R})$, que escriurem $\sharp\,\mathrm{comp}(X^{(m)}(\mathbb{R}))$. Posem $\nu(\mathcal{O},\Lambda)$ el nombre de classes d'immersions optimals d'un ordre quadràtic Λ en un ordre quaterniònic $\mathcal{O}$. A continuació enunciem el resultat d'Eichler que mostra com aquest nombre de classes és calculable en funció del nombre de classes de l'ordre quadràtic, $h(\Lambda)$, i del nombre de classes d'immersions locals, $\nu_p(\mathcal{O}_p,\Lambda_p)$. Concretament,

$$\nu(\mathcal{O},\Lambda) = h(\Lambda)\prod_{p|DN}\nu_p(\mathcal{O}_p,\Lambda_p).$$

Per a fórmules explícites per al nombre de classes d'immersions locals consulteu per exemple [Ogg83]. En particular, notem que si $p \nmid DN$, es té $\nu_p(\mathcal{O}_p,\Lambda_p) = 1$.

Per a cada $m \mid DN$, posem

$$\nu(m) := \begin{cases} \nu(\mathbb{Z}[\sqrt{m}],\mathcal{O}), & \text{si } m \equiv 2,3 \mod 4, \\ \nu(\mathbb{Z}[\sqrt{m}],\mathcal{O}) + \nu(\mathbb{Z}[(1+\sqrt{m})/2],\mathcal{O}) & \\ \qquad\qquad \text{si } m \equiv 1 \mod 4. & \end{cases}$$

7.1.3 Teorema. (cf. [Ogg83]) *Suposem $D > 1$. Sigui m un enter no quadrat tal que $m||DN$. Diem que se satisfà la condició (*) si $\nu(m) > 0$, $i \in \mathcal{O}$, $DN = 2t$, amb t senar, $m = t$ o bé $m = 2t$, i $x^2 - my^2 = \pm 2$ té solució amb $x, y \in \mathbb{Z}$.*

(i) *Si no se satisfà (*), aleshores $\sharp\,\mathrm{comp}(X^{(m)}(\mathbb{R})) = \nu(m)/2$.*

(ii) *Si se satisfà* (*), *aleshores* $\sharp\,\mathrm{comp}(X^{(m)}(\mathbb{R})) = (\nu(m)+2^{r-2})/2$, *on* r *és el nombre de factors primers, diferents entre si, de* DN.

Es tenen també resultats sobre els punts racionals en el cas particular de $N = 1$ i $m = D$.

7.1.4 Proposició. (cf. [Mic84b]) *Suposem* $N = 1$. *Si existeix un cos* F *quadràtic imaginari de nombre de classes 1 que escindeix* H, *aleshores* $X^{(D)}(\mathbb{Q}) \neq \emptyset$.

7.1.5 Exemples. (1) Per als primers valors del discriminant, amb un ordre maximal, tenim
$X(6,1)^{(m)}(\mathbb{R}) \neq \emptyset$ per a $m = 2, 3, 6$;
$X(10,1)^{(m)}(\mathbb{R}) \neq \emptyset$ per a $m = 2, 5, 10$;
$X(14,1)^{(m)}(\mathbb{R}) = \emptyset$ per a $m = 2$ i $X(14,1)^{(m)}(\mathbb{R}) \neq \emptyset$ per a $m = 7, 14$;
$X(15,1)^{(m)}(\mathbb{R}) \neq \emptyset$ per a $m = 3, 5, 15$.
De fet, observem que sempre $X(D,1)^{(D)}(\mathbb{R}) \neq \emptyset$, ja que tots els primers $p|D$ ramifiquen a $\mathbb{Q}(\sqrt{D})$.

(2) Considerem $X = X(2p,1)$ i $m = p$ primer. Aleshores tenim $X^{(p)}(\mathbb{R}) \neq \emptyset$ si, i només si, $p \not\equiv 1 \mod 8$. En aquest cas, tenim que la condició (*) se satisfà per a $p \equiv 3 \mod 4$, i no se satisfà per a $p \equiv 5 \mod 8$.

7.2 Punts locals de corbes de Shimura

Després d'analitzar el cas dels punts reals, i tenint en compte la manca de punts racionals (sobre $\mathbb{Q}$), el pas natural següent consisteix a estudiar l'existència de punts en els cossos locals $\mathbb{Q}_p$. Els resultats obtinguts, que descrivim a continuació, podrien culpabilitzar els cossos locals $\mathbb{Q}_p$ de la no-existència de punts racionals.

Notem que la mateixa qüestió estesa als cossos de nombres és molt més complicada. Descriurem com els resultats anteriors es generalitzen als cossos locals $K \mid \mathbb{Q}_p$. L'estudi pel cas dels cossos de nombres el recollim en la secció 7.3. Notem que, en aquest cas, quedarà clar que la responsabilitat de la no-existència global de punts racionals no recau només en la no-existència local de punts.

Incloem també una recopilació de resultats sobre l'existència de classes de divisors locals, per tal d'il·lustrar una de les aportacions recents a l'estudi d'objectes importants com ara el grup de Tate-Shafarevich.

7.2.1 Punts de corbes de Shimura sobre $\mathbb{Q}_p$

Ens restringim als cossos p-àdics $\mathbb{Q}_p$. B. Jordan [Jor84] dóna resultats d'existència per a $N = 1$, en el cas de bona reducció i de mala reducció, que corresponen a $p \nmid D$ i $p|D$, respectivament. A continuació resumim les eines utilitzades i els resultats obtinguts.

Suposem que $p \nmid D$; és a dir, p és un primer de bona reducció. El lema de Hensel ens diu que $X(\mathbb{Q}_p) = \emptyset$ si, i només si, $\widetilde{X}(\mathbb{F}_p) = \emptyset$. Per altra banda, el nombre de punts sobre cossos finits es pot comptar: $\sharp\tilde{X}(\mathbb{F}_p) = 1 + p - a_p$, on a_p és la traça de l'operador de Hecke que es calcula com

$$a_p = 1 + p - \sum_s \sum_\Lambda \frac{h(\Lambda)}{[\Lambda^* : \mathbb{Z}^*]} \prod_{q|D} \left(1 - \left(\frac{\Lambda}{q}\right)\right),$$

on Λ varia entre els ordres quadràtics imaginaris que contenen arrels de $x^2 + sx + p$. Aquest resultat és conseqüència de la fórmula de les traces i les congruències d'Eichler-Shimura (cf. Arenas, capítol 5; A. Travesa, capítol 6).

Recordem que el fet que un cos quadràtic F escindeixi l'àlgebra de quaternions H (cf. Rio, capítol 1), és caracteritzat per la condició que hi hagi una immersió de F en H. Això equival a què hi hagi immersions locals de F_p en H_p, per a tot p, i és equivalent a què, per a tot $p \mid D_H$, p no descompongui completament en el cos quadràtic F; és a dir, $\left(\dfrac{F}{p}\right) \neq 1$.

Així es demostra el teorema següent.

7.2.1 Teorema. (cf. [Jor84]) *Suposem $p \nmid DN$. Aleshores $X(\mathbb{Q}_p) = \emptyset$ si, i només si, cap dels cossos quadràtics imaginaris que contenen enters de norma p escindeix l'àlgebra de quaternions.*

Suposem ara $p|D$; és a dir, p és un primer de mala reducció. En aquest cas es necessita una versió més fina del lema de Hensel.

7.2.2 Lema. *Sigui X una corba pròpia i llisa sobre $\mathbb{Q}_p$. Aleshores tenim que $X(\mathbb{Q}_p) = \emptyset$ si, i només si, un model regular de X sobre $\mathbb{Z}_p$ no té punts racionals llisos a $\mathbb{F}_p$.*

Jordan realitza un estudi sistemàtic de la fibra especial del model minimal (els seus components, l'acció del Frobenius, etc.), a partir del model construït per Drinfeld i introdueix combinatòria en el graf dual. Això el condueix a provar el teorema següent.

7.2.3 Teorema. (cf. [Jor84]) *Suposem $p|D$. Aleshores, $X(\mathbb{Q}_p) \neq \emptyset$ si, i només si, es satisfà una de les dues condicions següents*

(1) $D = 2p$, $p \equiv 1 \mod 4$,

(2) $p = 2$ *i* $D = 2q_1 \cdots q_{2r-1}$, $q_i \equiv 3 \mod 4$, $1 \leq i \leq 2r-1$.

7.2.4 Exemples.
$X = X(6,1)$: $X(\mathbb{Q}_3) = \emptyset$ i $X(\mathbb{Q}_p) \neq \emptyset$, per a $p \neq 3$.
$X = X(10,1)$: $X(\mathbb{Q}_2) = \emptyset$ i $X(\mathbb{Q}_p) \neq \emptyset$, per a $p \neq 2$.
$X = X(14,1)$: $X(\mathbb{Q}_7) = \emptyset$ i $X(\mathbb{Q}_p) \neq \emptyset$, per a $p \neq 7$.
$X = X(15,1)$: $X(\mathbb{Q}_3) = X(\mathbb{Q}_5) = \emptyset$ i $X(\mathbb{Q}_p) \neq \emptyset$, per a $p \neq 3, 5$.
$X = X(87,1)$: $X(\mathbb{Q}_3) = X(\mathbb{Q}_{29}) = \emptyset$ i $X(\mathbb{Q}_2) = \emptyset$ (notem que $2 \not| 87$).
$X = X(194,1)$: $X(\mathbb{Q}_2) = \emptyset$, $X(\mathbb{Q}_{97}) \neq \emptyset$ i $X(\mathbb{Q}_3) = \emptyset$ (notem que $3 \not| 194$).

Considerem ara el cas de mala reducció, $p|D$ per a $N > 1$, tractat per Ogg a [Ogg85]. Les eines són aproximadament les mateixes que en el cas de nivell 1: lema de Hensel adequat, graf dual, ... També s'hi utilitzen de manera essencial els resultats sobre la uniformització p-àdica. En l'enunciat del resultat intervenen condicions sobre el graf dual (cf. Xarles, capítol 3). Donat un vèrtex x del graf dual, $\widehat{\mathcal{O}}_x$ denota l'ordre per la dreta de l'ideal corresponent al vèrtex.

7.2.5 Teorema. (cf. [Ogg85]) *Fixem $p \mid D$. Sigui $m > 1$ tal que $m \mid\mid ND/p$.*

(i) $X(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow$ *o bé* $i \in \mathcal{O}$ *i* $p = 2$
o bé $p \equiv 1 \mod 4$, $N = 1$, $D = 2p$.

(ii) *Suposem* $X(\mathbb{Q}_p) = \emptyset$. *Aleshores,* $X^{(m)}(\mathbb{Q}_p) \neq \emptyset$ *si, i només si,*

- *o bé* $p = 2$, $m = DN/p$ *i* $\sqrt{-2} \in \mathcal{O}$,
- *o bé* $p > 2$, $\sqrt{-p} \in \mathcal{O}$, $\left(\frac{-m}{p}\right) = 1$, DN/p *igual a* m *o* $2m$, *i* $(p+1)(m+1) \equiv 0 \mod 8$ *si* $DN/p = 2m$ *i* $2 \mid N$,
- *o bé* $p \equiv 1 \mod 4$, $\sqrt{-1} \in \widehat{\mathcal{O}}_x$ *per a cert* x, DN/p *igual a* m *o* $2m$, *i* $\sqrt{-pm} \in \mathcal{O}$.

(iii) $X^{(p)}(\mathbb{Q}_p) \neq \emptyset$ *si, i només si, en el graf dual existeix un vèrtex* x *tal que* $\widehat{\mathcal{O}}_x$ *conté* $\sqrt{-p}$ *o una unitat* $\neq \pm 1$.

(iv) *Suposem* $X(\mathbb{Q}_p) = \emptyset$. *Aleshores,* $X^{(pm)}(\mathbb{Q}_p) \neq \emptyset$ *si, i només si, en el graf dual hi ha un vèrtex* x *tal que* $w_m(x) = x$ (*i.e.* $\sqrt{-m} \in \widehat{\mathcal{O}}_x$, *o bé* $\sqrt{-1} \in \widehat{\mathcal{O}}_x$ *en el cas* $m = 2$).

En particular se'n dedueix el corol·lari següent.

7.2.6 Corol·lari. (cf. [Ogg85]) *Si* $p|D$, *aleshores* $X^{(DN)}(\mathbb{Q}_p) \neq \emptyset$.

7.2.2 Punts de corbes de Shimura sobre cossos locals

El cas de cossos locals en general és considerat per Jordan i Livné en [JL85]. Sigui K una extensió finita de $\mathbb{Q}_p$, i posem R l'anell d'enters de K.

Els resultats obtinguts pel cas de bona i mala reducció, respectivament, són els següents. Les eines inclouen, altre cop, una versió més sofisticada del lema de Hensel i la construcció de Drinfeld d'un model de la corba sobre $\operatorname{Spec} \mathbb{Z}_p$, que cal traslladar a $\operatorname{Spec} R$. Cal desenvolupar també combinatòria sobre el graf dual, per a la qual cosa utilitzen part del treball que féu Kurihara [Kur79] per tal de determinar algunes equacions de corbes de Shimura, (cf. Rotger, capítol 8).

Posem $f = f(K|\mathbb{Q}_p)$ i $e = e(K|\mathbb{Q}_p)$.

7.2.7 Teorema. (cf. [JL85]) *Suposem $p \nmid D$.*

(i) *Si f és parell, aleshores $X(K) \neq \emptyset$.*

(ii) *Si f és senar, aleshores $X(K) = \emptyset$ si, i només si, per a cada α solució de $x^2 + sx + p^f = 0$ amb $s \in \mathbb{Z}$, $|s| < 2p^{f/2}$, o bé $\mathbb{Q}(\alpha)$ no escindeix H o bé $p \mid \alpha$ i p descompon a $\mathbb{Q}(\alpha)$.*

7.2.8 Teorema. (cf. [JL85]) *Suposem $p|D$.*

(i) *Si f és parell, aleshores $X(K) \neq \emptyset$.*

(ii) *Si f és senar i e és parell, aleshores $X(K) \neq \emptyset$ si, i només si, o bé $\mathbb{Q}(\sqrt{-p})$ escindeix H o bé $p = 2$ i $\mathbb{Q}(\sqrt{-1})$ escindeix H.*

(iii) *Si f i e són senars, aleshores $X(K) \neq \emptyset$ si, i només si, o bé $D = 2p$ amb $p \equiv 1 \mod 4$ o bé $p = 2$ i $D = 2q_1 \cdots q_{2r-1}$, $q_i \equiv 3 \mod 4$, $1 \leq i \leq 2r-1$.*

7.2.3 Classes de divisors racionals sobre cossos locals

Donats un cos K i una corba de Shimura X, considerem $\mathrm{Pic}^d X(K)$, el conjunt de classes de divisors de la corba X de grau d racionals sobre K (i.e. $[D]$ tal que $[D]^\sigma = [D]$, $D^\sigma \sim D$, per a tot $\sigma \in \mathrm{Gal}(\overline{K}|K)$). Considerem també $\mathrm{Pic}^d X(K)^+$, el conjunt de classes de divisors de X de grau d que contenen un divisor racional sobre K (i.e. $[D]$ tal que $D^\sigma = D$, per a tot $\sigma \in \mathrm{Gal}(\overline{K}|K)$).

L'existència de divisors racionals sobre el cos dels nombres reals es coneix en general per a qualsevol corba projectiva, llisa i geomètricament irreductible, cf. [GH81]. Utilitzant la fórmula pel gènere de les corbes de Shimura i el fet que no tenen punts reals, se'n dedueix el resultat següent.

7.2.9 Proposició. *Sigui $X = X(D, 1)$.*

(i) $\mathrm{Pic}^d X(\mathbb{R})^+ = \emptyset$ *si, i només si, d és senar.*

(ii) $\mathrm{Pic}^d X(\mathbb{R}) = \emptyset$ *si, i només si, d és senar i $D \neq 2p$ amb $p \equiv 3, 5 \mod 8$.*

El resultat obtingut per Jordan i Livné per als cossos locals no arquimedians és anàleg a aquest resultat general per al cas real. Notem que es tracta d'una caracterització explícita, ja que l'existència de punts de la corba sobre els cossos locals és també explícita, com hem vist a la secció anterior.

7.2.10 Teorema. (cf. [JL87]) *Sigui $K|\mathbb{Q}_p$ finita. Considerem la corba $X := X(D,1)$. Aleshores,*

(i) $\mathrm{Pic}^d X(K)^+ = \emptyset$ *si, i només si, d és senar, $p \mid D$ o bé $p = \infty$, i $X(K) = \emptyset$.*

(ii) $\mathrm{Pic}^d X(K) = \emptyset$ *si, i només si,* $\mathrm{Pic}^d X(K)^+ = \emptyset$ *i $g(X)$ és senar.*

En el cas de corbes de Shimura associades a àlgebres de quaternions poc ramificades, Jordan i Livné plantegen també el problema de l'existència de classes de divisors racionals en els quocients de la corba per la involució d'Atkin. El resultat que obtenen és el següent.

7.2.11 Proposició. (cf. [JL99]) *Considerem $X = X(pq,1)$, per a p,q primers senars. Aleshores,*

(i) $\mathrm{Pic}^1 X^{(p)}(\mathbb{R})^+ \neq \emptyset$ *si, i només si, $\mathbb{Q}(\sqrt{p})$ escindeix H.*

(ii) $\mathrm{Pic}^1 X^{(p)}(\mathbb{Q}_p)^+ \neq \emptyset$.

(iii) $\mathrm{Pic}^1 X^{(q)}(\mathbb{Q}_p)^+ \neq \emptyset$ *si, i només si, el discriminant d'una de les àlgebres de quaternions* $\left(\dfrac{-1,-pq}{\mathbb{Q}}\right)$ *i* $\left(\dfrac{-p,-q}{\mathbb{Q}}\right)$ *és igual a q. De fet, aquesta condició és equivalent a què $X^{(q)}(\mathbb{Q}_p) \neq \emptyset$.*

Utilitzant aquest estudi sobre l'existència de divisors i resultats del treball de B. Poonen i M. Stoll [PS99], Jordan i Livné donen exemples de grups de Tate-Shafarevich d'ordre no quadrat. Això contrasta amb els exemples de grups de Tate-Shafarevich finits i no trivials coneguts anteriorment. Aquests exemples, començant pels determinats per Rubin (1987), provenien de corbes el·líptiques sobre $\mathbb{Q}$. Això implicava, pels resultats de Cassels [Cas62] (generalitzats per Tate [Tat63] a corbes el·líptiques sobre un cos de nombres K), que l'ordre era sempre un quadrat.

7.2.12 Definició. (cf. [PS99]) Sigui A una varietat abeliana principalment polaritzada sobre un cos global. Suposem que el quocient del seu grup de Tate-Shafarevich pel subgrup divisible maximal té ordre finit. Diem que A és parella si aquest ordre és igual a un quadrat i diem que és senar si aquest ordre no és un quadrat. En aquest darrer cas, l'ordre és el doble d'un quadrat.

7.2.13 Criteri. (cf. [PS99]) Sigui C una corba de gènere g sobre un cos global K. Aleshores, la jacobiana de C és senar si, i només si, el nombre de places v de K en les quals C no té divisors K_v-racionals de grau $g-1$ és senar.

7.2.14 Teorema. (cf. [JL99]) *Siguin p, q dos primers diferents, tals que $p \equiv 5 \mod 24$, $q \equiv 5 \mod 12$ i $\left(\frac{p}{q}\right) = -1$. Posem $X := X(pq,1)$ la corba de Shimura sobre $\mathbb{Q}$ i considerem el seu quocient $X^{(p)}$. Aleshores, la jacobiana de $X^{(p)}$ és senar.*

En la demostració d'aquest resultat, les hipòtesis sobre p i q s'utilitzen per a provar que el gènere de la corba quocient és parell. A partir dels resultats anteriors sobre l'existència de divisors racionals, es té que l'única plaça en què no hi ha divisors racionals de grau $g-1$ (senar) és q. El teorema s'obté aleshores aplicant el criteri de Poonen-Stoll.

7.2.15 Exemple. Considerem $p = 5$ i $q = 17$. Aleshores la corba $X := X(85,1)$ té gènere 5 i el quocient $X^{(5)}$ té gènere 2. Pels resultats sobre divisors tenim que $\mathrm{Pic}^1 X^{(5)}(\mathbb{Q}_l)^+ \neq \emptyset$ per a tot $l \neq 17$. Per tant, la jacobiana de $X^{(5)}$ és una varietat abeliana senar i ens dóna un exemple de grup de Tate-Shafarevich no trivial d'ordre no quadrat.

7.3 Punts de corbes de Shimura sobre cossos de nombres

Els primers resultats sobre l'existència de punts racionals sobre cossos de nombres es dedueixen dels resultats de Shimura, en dues direccions. En primer lloc la que fa referència a la no-existència de

punts reals [Shi75]. En segon lloc, la caracterització dels punts de multiplicació complexa donada en el model canònic [Shi67].

7.3.1 Remarca. Sigui K un cos de nombres. Si $X(K) \neq \emptyset$, aleshores $X(K_v) \neq \emptyset$ per a tota plaça v de K. Això ens permet, en alguns casos, demostrar la no-existència de punts racionals sobre K a partir de l'estudi dels punts als cossos locals K_v corresponents, que realitzem mitjançant els resultats enunciats a la secció anterior. És clar que el recíproc no és pas cert. Per exemple, es prova que per la corba de Shimura $X := X(39,1)$ i pel cos quadràtic $K = \mathbb{Q}(\sqrt{-13})$, es té $X(K) = \emptyset$ malgrat $X(K_v) \neq \emptyset$ per a tota plaça v de K.

En particular, si utilitzem la informació local sobre el cos dels nombres reals, cf. 7.1.1, com que tota extensió de grau senar té almenys una plaça infinita real obtenim el resultat següent.

7.3.2 Proposició. *Sigui K un cos de nombres de grau senar. Aleshores, per a qualsevol corba de Shimura X, es té $X(K) = \emptyset$.*

D'ara en endavant suposarem doncs que K és un cos de nombres de grau parell.

Per altra banda, els primers exemples de punts racionals de corbes de Shimura sobre cossos de nombres són donats ja per les propietats del model canònic provades per Shimura. Els punts de multiplicació complexa (CM) per un cos quadràtic imaginari K són sempre algebraics, ja que tenen coordenades en una extensió finita de K. Més precisament, si una corba de Shimura X té punts de multiplicació complexa per un ordre quadràtic $\Lambda \subseteq K$, aleshores $X(K_{\mathrm{ab}}) \neq \emptyset$, on K_{ab} denota l'extensió abeliana maximal de K. De fet, existeix un cos L (que es pot explicitar en funció de la teoria de cossos de classes, en relació amb els ordres quadràtics), $K \subseteq L \subseteq K_{\mathrm{ab}}$, de manera que $X(L) \neq \emptyset$. Així, quan el nombre de classes de K és 1, podem assegurar que els punts CM per un ordre quadràtic $\Lambda \subseteq K$ són racionals sobre K. Això només és aplicable a un nombre finit de cossos quadràtics. En particular, podem enunciar-ho de la manera següent.

7.3.3 Proposició. *Sigui K un cos quadràtic imaginari de nombre de classes 1. Si K escindeix H, aleshores $X(K) \neq \emptyset$.*

Per a nombre de classes més gran que 1, el fet d'escindir ja no serà una condició suficient per a tenir punts racionals, cf. 7.3.8 i 7.3.11.

Independentment, pel teorema de Mordell-Faltings, per a les corbes de Shimura de gènere més gran que 1 i per a qualsevol cos de nombres K, obtenim només un nombre finit, que pot ser 0, de punts K-racionals. Aquests resultats apunten a conjecturar una certa finitud en el conjunt de punts racionals. Els principals resultats coneguts sobre punts racionals, que descriurem en aquesta secció, van en aquesta direcció i es limiten bàsicament a cossos quadràtics o quàrtics. Per una banda, Jordan dóna resultats sobre un nombre finit de corbes de Shimura possibles amb punts K-racionals per un cos K fixat, a partir de la interpretació modular. Per altra banda, Kamienny i Rotger donen resultats sobre finitud del conjunt de punts racionals d'una corba de Shimura variant el cos de racionalitat.

7.3.1 Interpretació modular dels punts K-racionals

Una manera d'estudiar els punts racionals de les corbes de Shimura sobre cossos de nombres és via la interpretació modular, com fa Jordan a [Jor86] per a $X := X(D,1)$. Descrivim a continuació els resultats obtinguts.

Recordem que cada punt x d'una corba de Shimura X es correspon amb una tripleta $P_x = (A, i, \mathcal{C})$ on A és una superfície abeliana amb multiplicació quaterniònica, (cf. Rotger, capítol 2). El cos de moduli d'una tripleta P_x és $\mathrm{M}(P_x) := \overline{K}^G$ on $G = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid P_x^\sigma \simeq P_x\}$.

Sigui K un cos de característica 0. Aleshores un punt K-racional $x \in X(K)$ es correspon amb P_x superfície abeliana amb multiplicació quaterniònica (QM) amb cos de moduli $\mathrm{M}(P_x) \subseteq K$. Ara bé, un punt x K-racional no es correspon necessàriament amb què P_x tingui un model racional sobre K. Recordem les definicions habituals.

7.3.4 Definició. Es diu que $P = (A, i, \mathcal{C})$ és racional sobre un cos K si A és definida sobre K, $i : \mathcal{O} \hookrightarrow \mathrm{End}_K(A)$ i la polarització conté un divisor racional sobre K. Es diu que P té un model racional sobre un cos K si existeix P' racional sobre K tal que $P' \otimes_K \mathbb{C} \simeq P$.

De fet, és ben conegut que, si E és una corba el·líptica sobre K, aleshores E té un model racional sobre el cos de moduli, que és $K(j_E)$. Però en el cas de les superfícies abelianes, corresponents als punts de les corbes de Shimura, només tenim que si P_x és racional sobre un cos K, aleshores $\mathrm{M}(P_x) \subseteq K$. En aquesta direcció, el teorema següent dóna una caracterització de la racionalitat de P en funció de la relació entre el cos i l'àlgebra de quaternions. Com a corol·lari se'n dedueix un criteri per a l'existència de punts racionals en corbes de Shimura.

7.3.5 Teorema. (cf. [Jor86]) *Sigui $P = (A, i, \mathcal{C})$ i sigui K un cos de característica 0 que conté el cos de moduli de P, $K \supseteq \mathrm{M}(P)$. Aleshores, P té un model racional sobre el cos K si, i només si, K escindeix l'àlgebra de quaternions H.*

7.3.6 Exemple. Considerem la corba de Shimura $X = X(6, 1)$. Per una banda, es comprova que X té punts racionals sobre $\mathbb{Q}(\sqrt{-7})$ a partir de l'equació de la corba donada a [Kur79]. Sigui P_x una superfície abeliana amb QM corresponent a $x \in X(\mathbb{Q}(\sqrt{-7}))$. Aleshores el seu cos de moduli satisfà $\mathrm{M}(P_x) \subseteq \mathbb{Q}(\sqrt{-7})$. Per altra banda, notem que $p = 2$ descompon a $\mathbb{Q}(\sqrt{-7})$, per tant $\mathbb{Q}(\sqrt{-7})$ no escindeix cap àlgebra de quaternions de discriminant parell. En deduïm que P_x no té cap model racional sobre $\mathbb{Q}(\sqrt{-7})$.

7.3.7 Remarca. Si K no escindeix H, aquest resultat aporta poca efectivitat, ja que l'existència de punts racionals $x \in X(K)$ es correspondria amb l'existència de superfícies abelianes amb multiplicació quaterniònica P_x tals que $K \supseteq \mathrm{M}(P_x)$ però P_x no tindria model racional sobre K. Ara bé, de manera independent, si en aquest cas utilitzem 7.3.1 i la informació local donada per 7.2.8 cobrim bona part de les possibilitats. Concretament, si K no escindeix H aleshores existeix $p|D$ amb $\mathfrak{p}|p$ tal que $[K_\mathfrak{p} : \mathbb{Q}_p] = e(K_\mathfrak{p} : \mathbb{Q}_p) f(K_\mathfrak{p} : \mathbb{Q}_p)$ és senar. Aleshores $X(K_\mathfrak{p}) = \emptyset$, i per tant $X(K) = \emptyset$, excepte potser si $D = 2p$ amb $p \equiv 1 \mod 4$ o bé $p = 2$ i $D = 2q_1 \cdots q_{2r-1}$, $q_i \equiv 3 \mod 4$, $1 \leq i \leq 2r - 1$. Per a aquests casos, que Jordan anomena excepcionals, no es coneixen resultats generals.

En cas contrari, si K escindeix H mitjançant el teorema anterior, l'estudi de la racionalitat de la superfície abeliana ens dóna una via per a estudiar l'existència de punts racionals.

7.3.8 Corol·lari. *Suposem que K escindeix H. Aleshores, $X(K) \neq \emptyset$ si, i només si, existeix $P = (A, i, \mathcal{C})$ racional sobre K.*

A partir d'aquí, l'estratègia emprada per Jordan és buscar criteris i condicions necessàries per a l'existència de superfícies abelianes amb QM que siguin racionals sobre un cos K. En els casos en els quals aquestes condicions no es puguin satisfer, obtindrem la no-existència de punts racionals. En aquesta direcció realitza un bon estudi de les superfícies amb QM, la reducció, els subgrups de torsió, les L-sèries, etc. A continuació enunciem els resultats obtinguts. Cal remarcar que se'n podrien deduir resultats per a cossos més generals, no necessàriament quadràtics imaginaris. En particular, s'obté també una redemostració de resultats sobre l'existència de punts als cossos locals.

7.3.9 Notació. Fixat un primer q, considerem el conjunt d'àlgebres de quaternions $\mathcal{B}(q)$ donat de la forma següent. Si $q \neq 2$, $H \in \mathcal{B}(q)$ si, i només si, $\mathbb{Q}(\sqrt{-q})$ no escindeix H; si $q = 2$, $H \in \mathcal{B}(q)$ si, i només si, $\mathbb{Q}(\sqrt{-2})$ i $\mathbb{Q}(\sqrt{-1})$ no escindeixen H. Donada una àlgebra de quaternions H, D_H denota el seu discriminant.

7.3.10 Teorema. (cf. [Jor86]) *Sigui K un cos quadràtic imaginari tal que q ramifica en K. Aleshores existeix un subconjunt finit d'àlgebres de quaternions $\mathcal{S}(q) \subseteq \mathcal{B}(q)$ tal que, si $H \in \mathcal{B}(q) - \mathcal{S}(q)$ i K escindeix H, tenim $X(K) = \emptyset$ per a la corba de Shimura $X := X(D_H, 1)$.*

7.3.11 Teorema. (cf. [Jor86]) *Sigui K un cos quadràtic imaginari de nombre de classes diferent de 1. Aleshores, hi ha un nombre finit d'àlgebres de quaternions H tals que K escindeix H i $X(K) \neq \emptyset$, on X denota la corba de Shimura associada, $X := X(D_H, 1)$.*

7.3.2 Altres resultats de finitud

Es coneixen també altres resultats sobre la finitud dels punts racionals, obtinguts amb eines diferents de les anteriors, de la mà de Kamienny i Rotger. El denominador comú podríem trobar-lo en l'ús de qüestions com ara la hiperel·lipticitat i la biel·lipticitat, respectivament.

7.3.12 Teorema. (cf. [Kam90]) *Considerem la corba de Shimura poc ramificada $X(pq,1)$. Suposem que existeix n tal que divideix el numerador de $(p+1)(q-1)/24$ però no divideix $q(q-1)$.*

(i) *Si $(p-1)(q-1) > 240$, aleshores variant K entre els cossos quadràtics, el conjunt de punts "quadràtics" $\bigcup_K X(pq,1)(K)$ és finit.*

(ii) *Sigui K un cos quadràtic tal que p descompon a K, q no descompon a K i $\mathrm{mcd}(h(K),n) = 1$. Aleshores, variant F entre els cossos quadràtics sobre K, el conjunt de punts "quàrtics" sobre $\mathbb{Q}$, $\bigcup_F X(pq,1)(F)$, és finit.*

El primer pas de la demostració consisteix a provar que de les hipòtesis sobre p i q es dedueix que $X(pq,1)$ no és una corba hiperel·líptica. Aleshores, si la corba no és hiperel·líptica, el nombre de punts amb coordenades en un cos quadràtic sobre $\mathbb{Q}$ és finit si $J_0^{\mathrm{new}}(pq)(\mathbb{Q})$ és finit (Mazur). La finitud d'aquest conjunt es determina per mitjà de la isogènia de Ribet entre les jacobianes $J_0(pq)^{\mathrm{new}} = J(1,pq)^{\mathrm{new}}$ i $J(pq,1)$ (cf. Arenas, Vila, capítol 9) i l'estudi de propietats del grup de Mordell-Weil (modular).

La part de punts quadràtics d'aquest resultat és generalitzada per Rotger, com mostra el teorema següent.

7.3.13 Teorema. (cf. [Rot02]) *Hi ha un nombre finit de discriminants D tals que, variant K entre els cossos quadràtics, el conjunt de punts "quadràtics"de la corba de Shimura $X(D,1)$ de gènere $g \geq 2$, $\bigcup_K X(D,1)(K)$, és infinit.*

Per a obtenir aquest resultat, Rotger utilitza el fet que per tal que el conjunt de punts considerat sigui infinit la corba ha de ser necessàriament hiperel·líptica o biel·líptica, provat per Abramovich i Harris a [AH91]. Aleshores, a partir de la determinació de quines són les corbes de Shimura biel·líptiques, feta pel mateix autor, es dóna la llista explícita de discriminants. Notem que pràcticament tots corresponen al cas poc ramificat, amb l'excepció de 5 casos, en què D és producte de quatre factors primers.

Bibliografia

[AH91] D. Abramovich, J. Harris, *Abelian varieties and curves in* $W_d(C)$, Compositio Math. **78** (1991), num. 2, 227–238.

[Als00a] M. Alsina, *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura*, Tesi doctoral, Publ. Universitat de Barcelona, 2000.

[Cas62] J. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[Dri76] V. G. Drinfeld, *Coverings of p-adic symmetric regions*, Funct. Anal. Appl. **10** (1976), 107–115.

[GH81] B. Gross, J. Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), num. 2, 157–182.

[JL85] B. Jordan, R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985), num. 2, 235–248.

[JL87] B. Jordan, R. Livné, *Divisor classes on Shimura curves rational over local fields*, J. Reine Angew. Math. **378** (1987), 46–52.

[JL99] B. Jordan, R. Livné, *On Atkin-Lehner quotients of Shimura curves*, Bull. London Math. Soc. **31** (1999), 681–685.

[Jor84] B. Jordan, *p-adic points on Shimura curves*, Séminaire de théorie des nombres de Paris 1982-83 (M.J. Bertin, C. Goldstein, eds.), Progress in Math., vol. 51, Birkhäuser, 1984, pp. 135–142.

[Jor86] B. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[Kam90] S. Kamienny, *Points on Shimura curves over fields of even degree*, Math. Ann. **286** (1990), num. 3, 731–734.

[Kur79] A. Kurihara, *On some exemples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Tokyo **25** (1979), num. 3, 277–300.

[Mic84b] J-F. Michon, *Courbes de Shimura*, Séminaire de Théorie des Nombres de Paris 1982-83 (M.J. Bertin, C. Goldstein, eds.), Progr. Math., num. 51, Birkhäuser, 1984, pp. 185–197.

[Ogg83] A. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, 1983, pp. 277–307.

[Ogg85] A. Ogg, *Mauvaise réduction des courbes de Shimura*, Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser, 1985, pp. 199–217.

[PS99] B. Poonen, M. Stoll, *On the Cassels-Tate pairing for abelian varieties*, Ann. of Math. **150** (1999), 1109–1149.

[Rob89] D. Roberts, *Shimura curves analogous to $X_0(N)$*, Tesi doctoral, Harvard University, 1989.

[Rot02] V. Rotger, *On the group of automorphisms of Shimura curves and applications*, Compositio Math. **132** (2002), num. 2, 229–241.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

[Shi75] G. Shimura, *On the real points of arithmetic quotient of a bounded symetric domain*, Math. Ann. **215** (1975), 135–164.

[Tat63] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

Capítol 8

Models explícits de corbes de Shimura deguts a Kurihara

V. Rotger

8.1 Introducció

En els darrers anys, ha aparegut abundant literatura al voltant del coneixement efectiu de les corbes modulars $X(\Gamma)$ associades a subgrups $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$ d'índex finit. En gran part, l'aproximació computacional a aquestes corbes ha estat facilitada pel fet que les funcions i formes automorfes admeten expansions en sèries de Fourier al voltant de les *puntes* o *punts cuspidals*.

Això contrasta amb la gran dificultat que han trobat els matemàtics a desenvolupar aproximacions explícites en el cas de les corbes de Shimura associades a àlgebres de quaternions B de discriminant $\mathrm{disc}(B) \neq 1$ no trivial. En aquest cas, l'absència de punts cuspidals en aquestes corbes o, el que és equivalent, l'absència d'elements parabòlics en els grups Fuchsians que les uniformitzen analíticament, fa que el tractament aritmètic de les formes automorfes sigui molt

més inaccessible.

De tota manera, en els darrers temps s'han conegut aportacions en aquesta direcció. Podríem citar-ne algunes:[Als00a], [Bay02], [Elk98], [Jor81], [Kur79], [Mor95], [Rob89] i [Rot02].

En [Bay02] s'ofereix el primer tractament efectiu i computacional del desenvolupament en sèries de potències de funcions automorfes en corbes de Shimura al voltant de punts CM. El punt de partida són els dominis fonamentals de la uniformització hiperbòlica d'aquestes corbes que es donen en [Als00a].

En aquesta breu nota, ens centrarem en la determinació de models explícits de corbes de Shimura i, en particular, en els construïts per Kurihara en [Kur79].

8.2 Models de corbes de Shimura coneguts

Fixem i recordem algunes nocions introduïdes en A. Rio, capítol 1. Sigui $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, $ij = -ji$, $i^2 = a$, $j^2 = b \in \mathbb{Q}^*$, a ó $b > 0$, una àlgebra de quaternions indefinida sobre $\mathbb{Q}$.

Sigui $D = \mathrm{disc}(B) = p_1 \cdot ... \cdot p_{2r} \neq 1$ el discriminant de B. En la pràctica, pot calcular-se com segueix:

- Sigui p un primer senar. Aleshores $p \mid D$ si, i només si, el símbol de Hilbert $(a, b)_p = -1$ (veure [Vig80] per al càlcul en termes de residus quadràtics).
- Tenim que $2 \mid D$ si, i només si, hi ha un nombre senar de primers senars p que divideixen D.

Sigui $X_D/\mathbb{Q} = X(D, 1)/\mathbb{Q}$ el model canònic sobre $\mathbb{Q}$ de la corba de Shimura associada a (qualsevol ordre maximal en) B i estructura de nivell trivial. És una corba algebraica llisa i definida sobre $\mathbb{Q}$ (cf. Rotger, capítol 2).

És interessant remarcar aquí de nou que, tot i estar definida sobre $\mathbb{Q}$, un teorema de Shimura (cf. Alsina, capítol 7, [Shi75]) afirma que

$$X_D(\mathbb{Q}) = \emptyset.$$

El gènere geomètric de X_D pot calcular-se com

$$g(X_D) = 1 + \frac{1}{12}\prod_{p|D}(p-1) + \frac{1}{4}\prod_{p|D}(1-(\frac{\mathbb{Q}(i)}{p})) + \frac{1}{3}\prod_{p|D}(1-(\frac{\mathbb{Q}(\sqrt{-3})}{p})).$$

D'aquesta manera es pot veure fàcilment que les úniques corbes de Shimura X_D de gènere 0 són les corbes X_6, X_{10} i X_{22}. Potser cal insistir en el fet que $X_6 \ncong \mathbb{P}^1_{\mathbb{Q}}$, $X_{10} \ncong \mathbb{P}^1_{\mathbb{Q}}$ i $X_{22} \ncong \mathbb{P}^1_{\mathbb{Q}}$ degut a què no hi ha punts racionals en aquestes corbes.

És per aquest motiu que fins i tot per a aquests tres casos més senzills, $D = 6$, 10 i 22, conèixer-ne un model explícit és una questió interessant.

Similarment, les úniques corbes de Shimura X_D de gènere 1 són X_{14}, X_{15}, X_{21}, X_{33}, X_{34} i X_{46}. De la mateixa manera, aquestes corbes *no* són corbes el·líptiques sobre $\mathbb{Q}$ perquè no admeten cap punt racional.

8.2.1 Teorema. (Ihara, Kurihara, Jordan) *D'acord amb la taula següent, les corbes de Shimura $X_D/\mathbb{Q}$ associades a les àlgebres de quaternions de discriminants respectius $D = 6, 10, 14, 15, 22, 33, 46$ admeten els següents models*

Equacions de corbes de Shimura		
D	g	*Model sobre* $\mathbb{Q}$
6	0	$x^2 + y^2 + 3 = 0$
10	0	$x^2 + y^2 + 2 = 0$
14	1	$(x^2 - 13)^2 + 7^3 + 2y^2 = 0$
15	1	$(x^2 + 243)(x^2 + 3) + 3y^2 = 0$
22	0	$x^2 + y^2 + 11 = 0$
33	1	$x^4 + 30x^2 + 3^8 + 3y^2 = 0$
46	1	$(x^2 - 45)^2 + 23 + 2y^2 = 0$

És remarcable que, segons els coneixements de que disposo, no es coneixen equacions per a les corbes de Shimura de gènere 1 de discriminant $D = 21$ i 34.

Pel que fa a equacions de quocients $X_D/\langle\omega\rangle$ de corbes de Shimura per involucions d'Atkin-Lehner, Roberts ([Rob89]) dóna alguns exemples d'equacions de Weierstrass de corbes el.lípiques obtingudes així. En [Rot02] es dóna una llista exhaustiva de totes elles.

8.3 Punts CM i la teoria de cossos de classes

La idea d'Ihara i Kurihara per a determinar un model sobre $\mathbb{Q}$ de les corbes de Shimura X_D es basa en el fet que les coordenades de certs punts privilegiats, anomenats punts CM o punts de Heegner, generen cossos de classes sobre cossos quadràtics imaginaris (cf. Alsina, capítol 7, [Shi67], [Jor81], [Als00a]).

En efecte, més precisament, tenim

8.3.1 Teorema. *Sigui $P \in X_D(\bar{\mathbb{Q}})$.*

Sigui (A, ι, L) una superfície abeliana principalment polaritzada amb multiplicació quaterniònica que representa la classe d'isomorfisme associada al punt P en la interpretació modular de X_D.

Suposem que $R = \mathrm{End}_{\iota(\mathcal{O})}(A)$ és un ordre en un cos quadràtic imaginari K (cf. Rotger, capítol 2 per a la notació i més detalls). És a dir, P és un punt de Heegner en X_D amb CM per R.

Sigui H_R el cos de classes d'anell R sobre K.

Aleshores $H_R = K \cdot \mathbb{Q}(P)$, on $\mathbb{Q}(P)$ denota l'extensió de $\mathbb{Q}$ que s'obté en adjuntar a $\mathbb{Q}$ les coordenades del punt $P \in X_D(\bar{\mathbb{Q}})$.

Juntament amb el fet que $X_D(\mathbb{Q}) = \emptyset$, aquest teorema permet determinar exactament l'extensió $\mathbb{Q}(P)/\mathbb{Q}$ en molts casos (cf. Alsina, capítol 7).

De tota manera, molt sovint aquestes dues informacions no són suficients per a descriure $\mathbb{Q}(P)$. Degut a què la determinació explícita de $\mathbb{Q}(P)$ és fonamental per a obtenir equacions de corbes de Shimura segons el procediment desenvolupat en [Kur79], és convenient citar que Jordan, en la seva tesi [Jor81], descriu $\mathbb{Q}(P)$ completament en termes de l'aritmètica de B. A més, il.lustra la necessitat i aplicabi-

litat del seu resultat tot donant l'equació de la corba X_{15}.

És important remarcar aquí també que el model sobre $\mathbb{Q}$ de Shimura de les corbes X_D està unívocament determinat pel fet que els punts CM generen els cossos de classes tal com descriu el teorema anterior. Aquesta observació garanteix la consistència del mètode d'Ihara i Kurihara que expliquem a continuació.

8.4 El mètode d'Ihara i de Kurihara

En aquesta secció traçarem les idees bàsiques del mètode que utilitza Kurihara per a obtenir equacions d'algunes corbes de Shimura de gèneres 0 i 1. Tot i que en principi el mètode és vàlid per a qualsevol corba, la quantitat de càlculs necessaris és de seguida excessivament voluminosa quan el gènere creix.

Sigui X_D la corba de Shimura associada a l'àlgebra de quaternions de discriminant $D = p_1 \cdot ... \cdot p_{2r}$ i sigui W el grup d'Atkin-Lehner actuant en X_D.

Aleshores els elements de

$$W = \{\omega_m, m \mid D\} \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$$

actuen en X_D com involucions definides sobre $\mathbb{Q}$. En molts casos, W coincideix amb tot el grup d'automorfismes de la corba X_D (veure [Rot02]).

Suposem ara que $D = pq$, p, q primers. En aquest cas $W = \{\mathrm{id}, \omega_p, \omega_q, \omega_D\}$. La idea d'Ihara i Kurihara per a obtenir una equació de X_D parteix del següent requisit sobre la corba:

- Cal conèixer un model explícit dels quocients $X_D/\langle\omega\rangle$, $\omega \in W$.

Això fa el mètode practicable especialment per a aquelles corbes de Shimura tals que $X_D/\langle\omega\rangle \cong \mathbb{P}^1_{\mathbb{Q}}$ per a tot $\omega \in W$. Això és només possible si $g(X_D) = 0$ ó 1.

En aquesta situació es pot procedir de la següent manera. Per a

exemplificar-ho, considerarem el cas de la corba X_D, $D = 2 \cdot 7 = 14$ amb detall, tal com fa Kurihara en [Kur79].

1. *Determinació del tipus de model de la corba*

   En primer lloc podem usar els morfismes (o projeccions) naturals

   $$y_\omega : X_D \to X_D/\langle\omega\rangle$$

   i les equacions conegudes dels quocients $X_D/\langle\omega\rangle$ per a determinar el tipus de model $f(x, y) = 0, f \in \mathbb{Q}[x, y]$ que volem trobar per a la corba X_D.

   La situació més habitual es produeix quan, per a cert automorfisme involutiu $\omega \in W$ de X_D, $X_D/\langle\omega\rangle \cong \mathbb{P}^1_{\mathbb{Q}}$. En aquest cas podem assegurar que

   $$X_D : y^2 = p(x)$$

   on $p(x)$ és un polinomi de grau $2g+2$, no necessàriament mònic, amb coeficients a $\mathbb{Q}$. A més, la funció coordenada $y : X_D \to \mathbb{P}^1_{\mathbb{Q}}$ factoritza a través de l'isomorfisme $X_D/\langle\omega\rangle \cong \mathbb{P}^1_{\mathbb{Q}}$.

   En el cas particular de la corba X_{14}, de gènere 1, la involució d'Atkin-Lehner ω_{14} indueix un morfisme

   $$X_{14} \to X_{14}/\langle\omega_{14}\rangle$$

   que té 4 punts fixos. A més, tot i que $X_{14}(\mathbb{Q}) = \emptyset$, pot mostrar-se que la corba quocient $X_{14}/\langle\omega_{14}\rangle$ admet punts racionals i per tant $X_{14}/\langle\omega_{14}\rangle \cong \mathbb{P}^1_{\mathbb{Q}}$. Podem assegurar aleshores que

   $$X_{14} : y^2 = p(x) = ax^4 + bx^3 + cx^2 + dx + e,$$

   per a certs a, b, c, d, $e \in \mathbb{Q}$, de tal manera que el morfisme natural de projecció $X_{14} \to X_{14}/\langle\omega_{14}\rangle \cong \mathbb{P}^1_{\mathbb{Q}}$ és donat per la coordenada y.

   Els punts fixos d'aquesta projecció són els punts $R_i = \{(\beta_i, 0)\}$, on $\beta_i \in \bar{\mathbb{Q}}$, $i = 1, 2, 3, 4$, són les quatre arrels de $p(x)$.

   A continuació cal determinar els coeficients a, b, c, d, $e \in \mathbb{Q}$.

2. *Reducció a un nombre finit de possibles models*

   En el cas que coneguem el tipus de model $f(x, y) = 0$ per a X_D i coneguem explícitament els morfismes $X_D \to X_D/\langle\omega\rangle$ per a tot $\omega \in W$, aleshores probablement també podem conèixer quins són els punts fixos de $\omega \in W$ en termes dels coeficients (incògnites) de $f(x, y)$.

   D'altra banda, si $\omega \in W$, els punts fixos $P \in X_D(\bar{\mathbb{Q}})$ de ω són punts de Heegner. El teorema 8.3.1 (veure també [Jor81]) ens permet calcular l'extensió $\mathbb{Q}(P)/\mathbb{Q}$ explícitament i això imposa restriccions importants en els coeficients de f(x, y).

   Aquestes condicions aritmètiques en els coeficients de $f(x, y)$ poden ser suficientment restrictives perquè donin lloc a un nombre finit de possibilitats per a f. En els casos més afortunats, poden fins i tot determinar f unívocament.

   Il.lustrem-ho en l'exemple de Kurihara.

   En la corba $X_{14} : y^2 = p(x) = ax^4 + bx^3 + cx^2 + dx + e$, la involució ω_7 no té punts fixos mentre que la involució ω_2 té quatre punts fixos $P_1 = (0, \sqrt{e})$, $P_2 = (0, -\sqrt{e})$, $Q_1 = \infty_1$, $Q_2 = \infty_2 \in X_{14}(\bar{\mathbb{Q}})$ tals que, segons mostra Kurihara usant els arguments que hem citat anteriorment,

$$\mathbb{Q}(P_i) = \mathbb{Q}(i),$$

$$\mathbb{Q}(Q_i) = \mathbb{Q}(\sqrt{-2}).$$

   Anàlogament, la involució ω_{14} té quatre punts fixos $R_i = (\beta_i, 0)$. Aquests punts fixos són punts de Heegner per l'ordre d'enters $\mathbb{Z}[\sqrt{-14}]$ del cos quadràtic imaginari $K = \mathbb{Q}(\sqrt{-14})$.

   Aquest cos té nombre de classes $h(K) = 4$ i el cos de classes de Hilbert és una extensió H/K de grau 4. Tal com mostra Kurihara, les extensions $\mathbb{Q}(R_i)/\mathbb{Q}$ són $\mathbb{Q}\left(\pm\sqrt{\frac{1\pm\sqrt{-7}}{2}}\right)$.

   Tot plegat porta Kurihara a la conclusió que

$$X_{14} : y^2 = p_{\alpha(x)} = -\frac{1}{2}(x^2 - \alpha)(x^2 - \bar{\alpha}),$$

on $\alpha \in \mathbb{Q}(\sqrt{-7})$ i $\bar{\alpha}$ denota l'element conjugat d'α en $\mathbb{Q}(\sqrt{-7})$.

Canvis de variable adequats i un estudi ad hoc (no trivial, vegeu [Kur79], p. 282, 283), donen tan sols **vint** possibles valors per a α. Tan sols resta doncs determinar exactament el valor correcte d'α d'entre els vint possibles.

3. *Estudi de les fibres especials, de bona i mala reducció, per a determinar completament el model*

   Si podem assegurar que la corba de Shimura X_D ha de ser isomorfa sobre $\mathbb{Q}$ a un model d'entre un nombre finit $\{f_i(x,y)=0\}$ de possibles models, podem intentar destriar el model correcte d'entre els incorrectes estudiant la reducció de les corbes X_D i $f_i(x,y)=0$ en diferents primers p.

   En el cas de Kurihara $D = 2 \cdot 7$, la corba X_{14} té bona reducció en tot primer $p \neq 2, 7$. Això es deu a un teorema de Morita (cf. Re, capítol 4, A. Travesa, capítol 6). La funció zeta de la corba X_D mod p, $p \neq 2, 7$, es pot calcular explícitament en termes de traces d'operadors de Hecke degut a les relacions d'Eichler-Shimura i la fórmula de traces d'Eichler-Selberg (cf. Arenas, capítol 5, Travesa, capítol 6, Alsina, capítol 7, [JL85], [Kur79]).

   En comparar la funció zeta de X_D mod p amb les funcions zeta de les corbes $f_i(x,y) = 0 \bmod p$, $p \neq 2, 7$, (que es poden calcular explícitament comptant el nombre de punts sobre cossos finits), arribem a la conclusió que la corba X_D ha de ser isomorfa a una de les tres corbes següents:

$$y^2 = p_{\alpha_k}(x), k = 1, 2, 3,$$

   per a

$$\begin{aligned} \alpha_1 &= 2\pi^5, \\ \alpha_2 &= 2\pi^7, \\ \alpha_3 &= 2\pi^{13}, \end{aligned}$$

   on $\pi = \sqrt{\dfrac{1+\sqrt{-7}}{2}}$.

   Finalment, es conclou que

$$X_{14} : (x^2 - 13)^2 + 7^3 + 2y^2 = 0$$

tot estudiant les reduccions de X_{14} i les tres corbes $y^2 = p_{\alpha_k}(x)$ en els primers de mala reducció $p = 2$ i 7.

Això es pot dur efectivament a terme perquè la teoria de Čerednik-Drinfeld descriu de manera explícita la reducció de les corbes de Shimura en els primers que divideixen el discriminant (cf. Xarles, capítol 3, [JL85], [Kur79]).

Bibliografia

[Als00a] M. Alsina, *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de shimura*, Tesi doctoral, Publ. Universitat de Barcelona, 2000.

[Bay02] P. Bayer, *Uniformization of certain Shimura curves*, Differential Galois Theory, Banach Center Publications, Polish Academy of Sciences **58** (2002), 13–26.

[Elk98] N. Elkies, *Shimura curve computations*, Algorithmic number theory ANTS-3 (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, 1998, pp. 1–47.

[JL85] B. Jordan, R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985), num. 2, 235–248.

[Jor81] B. Jordan, *On the diophantine arithmetic of Shimura curves*, Tesi doctoral, Harvard University, 1981.

[Kur79] A. Kurihara, *On some exemples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Tokyo **25** (1979), num. 3, 277–300.

[Mor95] A. Mori, *Power series expansions of modular forms at CM points*, Rend. Sem. Mat. Univ. Pol. Torino **53** (1995), 361–374.

[Ogg83] A. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, 1983, pp. 277–307.

[Ogg85] A. Ogg, *Mauvaise réduction des courbes de Shimura*, Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser, 1985, pp. 199–217.

[Rob89] D. Roberts, *Shimura curves analogous to* $X_0(N)$, Tesi doctoral, Harvard University, 1989.

[Rot02] V. Rotger, *On the group of automorphisms of Shimura curves and applications*, Compositio Math. **132** (2002), num. 2, 229–241.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

[Shi75] G. Shimura, *On the real points of arithmetic quotient of a bounded symetric domain*, Math. Ann. **215** (1975), 135–164.

[ST61] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[Vig80] M-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., num. 800, Springer, 1980.

Capítol 9

Aplicacions de les corbes de Shimura. Teoremes de Ribet

A. Arenas, N. Vila

L'objectiu d'aquest capítol és presentar una prova alternativa del teorema de Ribet de la $\mathbb{Q}$-isogènia entre jacobianes de corbes de Shimura i certes subvarietats abelianes de les jacobianes de corbes modulars ([Rib80], [Rib90b]), i el paper de les corbes de Shimura en la demostració de Ribet ([Rib90b]) de la conjectura ϵ de Serre.

9.1 Teorema de Ribet de la isogènia

En primer lloc recordarem el teorema de Faltings [Fal83] relatiu a $\mathbb{Q}-$isogènies entre varietats abelianes sobre $\mathbb{Q}$, així com també els resultats relatius a la reducció de les corbes de Shimura $X(D,1)$ respecte dels primers p de bona reducció ([Mor70], [Shi67]).

En el que segueix, G denotarà el grup de Galois absolut $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Si $l \in \mathbb{Z}$ és un nombre primer i $T_l(A)$ és el $\mathbb{Z}_l$-mòdul de Tate corresponent a una varietat abeliana A definida sobre $\mathbb{Q}$, escriurem

$T_l(A) \bigotimes \mathbb{Q}_l =: V_l(A)$ per a la seva extensió sobre $\mathbb{Q}_l$. A més, $L_p(A,s)$ designarà, com és habitual, el p-èsim, p primer, factor d'Euler de la seva sèrie L.

9.1.1 Teorema. (Faltings) *Donades dues varietats abelianes A_1, A_2 definides sobre $\mathbb{Q}$, les següents condicions són equivalents:*

1. *A_1 i A_2 són $\mathbb{Q}$-isògenes.*
2. *$V_l(A_1)$ i $V_l(A_2)$ són $\mathbb{Q}_l[G]$-isomorfs.*
3. *$L_p(A_1,s) = L_p(A_2,s)$, per a quasi tot primer p.*
4. *$L_p(A_1,s) = L_p(A_2,s)$, per a tot primer p.*

9.1.2 Teorema. (Eichler, Shimura, Ihara, Morita) *Sigui B una $\mathbb{Q}$-àlgebra de quaternions indefinida de discriminant $D > 1$. Considerem la corba de Shimura $X(D,1)$. Aleshores si $p \nmid D$, p primer, es té:*

1. *La funció zeta de la corba reduïda $\overline{X}$ sobre $\mathbb{F}_p$ és donada per*

$$Z(\overline{X}/\mathbb{F}_p, t) = \frac{\det(1 - T(p)t + p\,t^2)}{(1-t)(1-p\,t)},$$

on $T(p)$ es considera com a operador en $\Omega^1(X) \cong \mathcal{S}_2(\Gamma(D,1))$.

2. *Posem $N_r = \#\overline{X}(\mathbb{F}_{p^r}), r \geq 1$. Aleshores*

$$\frac{d}{dt} \log Z(\overline{X}/\mathbb{F}_p, t) = \sum_{r=1}^{\infty} N_r t^{r-1},$$

i

$$N_r = 1 + p^r - \mathrm{tr}(T(p^r) - pT(p^{r-2}))$$

convenint que $T(p^{-1}) = 0$.

En particular,

$$\#\overline{X}(\mathbb{F}_p) = 1 + p - \mathrm{tr}(T(p) | \mathcal{S}_2(\Gamma(D,1))).$$

Sigui N un enter lliure de quadrats producte d'un nombre parell de primers. Considerem els grups fuchsians de primera espècie $\Gamma(1,N) =$

$\Gamma_0(N)$ i el grup $\Gamma(N,1)$ d'unitats de norma 1 d'un ordre maximal d'una $\mathbb{Q}$-àlgebra de quaternions indefinida de discriminant N. Com és habitual, denotarem per $S_2(\Gamma_0(N))^{new}$ l'espai de formes parabòliques *noves* de pes 2 i nivell N (vegeu [AL70], [Miy71]), i per $\mathcal{S}_2(\Gamma(N,1))$ l'espai de formes parabòliques de pes 2 respecte del grup $\Gamma(N,1)$.

9.1.3 Teorema. *Si $N > 1$ és un enter lliure de quadrats producte d'un nombre parell de primers i si p és un primer que no divideix N, aleshores:*

$$\mathrm{tr}(T(p)|\mathcal{S}_2(\Gamma(N,1))) = \mathrm{tr}(T(p)|\mathcal{S}_2(\Gamma(1,N))^{new}).$$

La demostració d'aquest teorema (cf. [Are03]) es basa en la descomposició de l'espai $S_2(\Gamma_0(N))$ en suma directa dels subespais de formes noves i velles:

$$\mathcal{S}_2(\Gamma_0(N)) = \bigoplus_{M|N} \bigoplus_{d|\frac{N}{M}} \delta_d(\mathcal{S}_2(\Gamma_0(M)^{new})),$$

on δ_d és l'aplicació

$$\mathcal{S}_2(\Gamma_0(M)) \hookrightarrow \mathcal{S}_2(\Gamma_0(N))$$

$$\textstyle\sum_{n\geq 1} a_n q^n \mapsto \sum_{n\geq 1} a_n q^{nd},$$

juntament amb la fórmula de les traces que ens permet escriure la traça de l'operador de Hecke $T(p)$ operant sobre l'espai $\mathcal{S}_2(\Gamma(1,N))$ de la següent manera :

$$1 + p - 2^{\nu(N)} - \sum_t \left(\sum_{r|m} \frac{h(\Delta r^{-2})}{w(\Delta r^{-2})} \prod_{q|N} \left(1 + \left\{ \frac{\Delta r^{-2}}{q} \right\} \right) \right),$$

on $\nu(N)$ designa el nombre de divisors primers de N, i entenent que el sumatori respecte de t indica que només hem de sumar respecte dels t tals que $t^2 - 4p =: \Delta$ sigui discriminant negatiu, que sempre serà considerat sota la forma $\Delta = \Delta_0 m^2$ amb Δ_0 fonamental i la segona suma és respecte dels divisors positius de m. A més a més, $q \in \mathbb{N}$ denota un primer, $h(d)$ el nombre de classes de formes quadràtiques binàries de discriminant d, $w(d)$ l'ordre del grup d'isotropia de les formes quadràtiques binàries de discriminant d, i

$$\left\{\frac{\Delta r^{-2}}{q}\right\} = \begin{cases} 1, & \text{si } q|r, \\ \left(\frac{\Delta r^{-2}}{q}\right), & \text{si } q \nmid r \end{cases}$$

Denotarem per $J(D,N)$ la jacobiana de la corba de Shimura $X(D,N)$. D'aquests tres teoremes resulta sense gaires dificultats el teorema de la isogènia de Ribet (cf. [Rib80]):

9.1.4 Teorema. *Sigui N producte d'un nombre parell de primers diferents. Aleshores, les varietats abelianes $J(N,1)$ i $J(1,N)^{new}$ són $\mathbb{Q}$- isògenes. En particular, si N és un enter lliure de quadrats i D un divisor de N producte d'un nombre parell de primers, $J(D,1)$ és $\mathbb{Q}$- isògena a una subvarietat abeliana de $J_0(N) = J(1,N)$.*

Considerem un enter N lliure de quadrats de la forma $N = pqM$, amb p i q primers. L'espai $S_2(\Gamma_0(N))$ conté dos subespais isomorfs respectivament a

$$S_2(\Gamma_0(qM)) \bigoplus S_2(\Gamma_0(qM)) \ , \ S_2(\Gamma_0(pM)) \bigoplus S_2(\Gamma_0(pM)).$$

Sigui $S_2(\Gamma_0(pqM))^{pq-old}$ la suma d'aquests dos subespais de l'espai $S_2(\Gamma_0(N))$ (en general no directa), i sigui $S_2(\Gamma_0(pqM))^{pq-new}$ el complement ortogonal de $S_2(\Gamma_0(pqM))^{pq-old}$ en $S_2(\Gamma_0(pqM))$ respecte del producte escalar de Petersson. Denotem per $J_0(pqM)^{pq-new}$ el quocient $J_0(pqM)/A$ on $A \subset J_0(pqM)$ és una subvarietat abeliana $\mathbb{Q}$-isògena a $J_0(qM)^2 \times J_0(pM)^2$, i per $J(pq,M)$ la jacobiana de la corba de Shimura $X(pq,M)$ corresponent a l'àlgebra de quaternions de discriminant pq i nivell M. Aleshores, procedint de manera anàloga al cas precedent es té (cf. [Rib90b])

9.1.5 Teorema. (Ribet) *$J(pq,M)$ és $\mathbb{Q}$-isògena a $J_0(pqM)^{pq-new}$.*

De fet, molts dels treballs sobre les jacobianes de corbes de Shimura $J(pq,M)$ han estat motivats pel desig de trobar una isogènia *natural* entre les dues jacobianes anteriors.

9.2 Corbes de Shimura i la conjectura ε de Serre

La demostració de Ribet [Rib90b] de la conjectura ε de Serre, qualificat de "théorème difficile"per Serre ([Ser00], Nota 125.4), ha jugat un paper fonamental. D'una banda amb aquest teorema es té que Shimura-Taniyama-Weil implica Fermat. D'altra, és un primer resultat en el marc de l'equivalència de les conjectures dèbil ($3.2.3_?$) i forta ($3.2.4_?$) de Serre ([Ser00], 143, 168).

9.2.1 La conjectura ε

Sigui

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

una representació contínua i irreductible, on $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ i $l \geq 3$ és un primer.

- Suposem que ρ és modular de nivell N, és a dir, ρ prové d'una forma modular nova de pes 2, nivell dividint N i caràcter trivial. Aleshores tenim que:

  - ρ és una representació imparell: $\rho(c)$ té valors propis ± 1.

  - ρ té un model sobre tot cos finit $\mathbb{F}_{l^r}$ contenint les traces de ρ.

- Suposem que ρ és finita en p, on p és un primer que divideix exactament N ($p||N$). Això vol dir que existeix un esquema en grups H sobre $\mathbb{Z}_p$ finit i pla tal que l'acció de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sobre el $\mathbb{F}_{l^r}$-espai vectorial $H(\overline{\mathbb{Q}}_p)$ coincideix amb la restricció de ρ al grup de descomposició en p.

Remarques.

1. Notem que si $l \neq p$, ρ és finita en p si i només si ρ és no ramificada en p.

2. Si ρ és modular de nivell N/p aleshores és finita en p.

Serre conjectura el recíproc, de fet aquesta és la conjectura anomenada ε (cf. [Ser87]). Immediatament Mazur, en una carta a Mestre (16 d'agost 1985), demostra la conjectura en el cas $p \not\equiv 1 \pmod{l}$. Ribet a [Rib90b] la demostra en el cas $l \nmid N$, combinant les tècniques de Mazur i una relació geomètrica entre les corbes modulars clàssiques i corbes de Shimura.

9.2.1 Teorema. (Ribet) *Sigui*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

una representació contínua i irreductible, $l \geq 3$ primer. Suposem que la representació ρ és modular de nivell N, finita en p, $p||N$, i una de les dues condicions es satisfà:

- $p \not\equiv 1 \pmod{l}$,
- *N és primer amb l,*

aleshores ρ és modular de nivell N/p.

9.2.2 Representacions modulars

Sigui N un enter positiu. Sigui $\mathbb{T} = \mathbb{T}_N$ l'anell generat pels operadors de Hecke T_n ($n \geq 1$) sobre l'espai de formes modulars parabòliques $S_2(\Gamma_0(N))$. Sigui m un ideal maximal de $\mathbb{T}$. Per Deligne sabem que

9.2.2 Teorema. *Existeix una única representació semisimple*

$$\rho_{\mathrm{m}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}/\mathrm{m}),$$

no ramificada fora de mN *i satisfent*

$$\mathrm{tr}(\rho_{\mathrm{m}}(\mathrm{Frob}_r)) = T_r \pmod{\mathrm{m}}, \qquad \det(\rho_{\mathrm{m}}(\mathrm{Frob}_r)) = r \pmod{\mathrm{m}},$$

per a tots els primers r no dividint mN.

Definició. Una representació contínua

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

diem que és *modular de nivell* N si el determinant de ρ és el caràcter ciclotòmic mod l i existeix un morfisme

$$\omega : \mathbb{T} \to \overline{\mathbb{F}}_l$$

tal que

$$\mathrm{tr}(\rho(\mathrm{Frob}_r)) = \omega(T_r)$$

per a quasi tot primer r. Aleshores, si $\mathrm{m} = \ker(\omega)$, la semisimplificació ρ^{ss} de ρ és equivalent a ρ_{m}.

Remarques.

1. Les representacions modulars també les podem pensar com les associades a la q-expansió d'una forma modular $f \in S_2(\Gamma_0(N))$ vector propi de tots els operadors de Hecke.

2. Si ρ_{m} és irreductible, l'espai vectorial V subjacent a ρ_{m} es pot incloure a $J_0(N)[\mathrm{m}]$: $V \subseteq J_0(N)[\mathrm{m}]$, on $J_0(N)[\mathrm{m}]$ és el nucli de la multiplicació per m en la jacobiana $J_0(N)$ de la corba modular $X_0(N)$.
   Si l és primer amb $2N$, es té l'isomorfisme de $\mathbb{T}/\mathrm{m}[G_{\mathbb{Q}}]$-mòduls

   $$V \approx J_0(N)[\mathrm{m}].$$

   En general, la semisimplificació $J_0(N)[\mathrm{m}]^{ss}$, és un producte d'espais V com a $\mathbb{T}/\mathrm{m}[G_{\mathbb{Q}}]$-mòduls (cf. [Maz77]).

9.2.3 L'abaixament del nivell

Fixem un enter positiu M i un primer p que no divideixi a M. Sigui $N = pM$.

El primer resultat sobre l'abaixament de nivell el dóna el següent teorema de Mazur en el cas $p \not\equiv 1 \pmod{l}$.

9.2.3 Teorema. (Mazur) *Sigui*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

una representació contínua, irreductible, modular de nivell N, $l \geq 3$, *finita en* p *i* $p \not\equiv 1 \pmod{l}$. *Aleshores* ρ *és modular de nivell* M.

La prova d'aquest resultat es pot seguir a [Rib90b]. Té com a eines fonamentals els resultats de [DR73] i de [Maz77] i no hi intervenen les corbes de Shimura. Es demostra per reducció a l'absurd i requereix analitzar l'acció de Galois i de l'àlgebra de Hecke sobre la fibra especial en p de $J_0(N)$.

Així, per demostrar el teorema de Ribet, podem suposar que:

- $\rho \approx \rho_\lambda$, on λ és un ideal maximal de $\mathbb{T}_{Mp}$, doncs ρ és irreductible i modular de nivell Mp.
- $p \equiv 1 \pmod{l}$, en particular els primers p i l són diferents, pel teorema de Mazur.
- λ prové del quocient p-nou de $\mathbb{T}_{Mp}$, si fos p-vell ja estaríem.

L'estratègia de Ribet consisteix a introduir un nou primer q, que fa de pivot: q és primer amb pM i tal que $\rho_\lambda(\mathrm{Frob}_q)$ té traça 0 i determinant -1. Pel teorema Čebotarev hi ha infinits primers que actuen com la conjugació complexa. Com que el determinant de $\rho_\lambda(\mathrm{Frob}_q)$ és q mòdul λ, tenim que $q \equiv -1 \pmod{l}$.

Sigui m un ideal maximal p-nou de $\mathbb{T}_{Mpq}$ compatible amb λ.

Ribet prova els dos resultats clau següents, on intervenen de manera fonamental les corbes de Shimura.

- m és pq-nou de $\mathbb{T}_{Mpq}$.
- ρ és modular de nivell qM.

Ara $q \not\equiv 1 \pmod{l}$ doncs $l \neq 2$, i pel teorema de Mazur, obtenim que ρ és modular de nivell M. $\square$

9.2.4 Resultats clau

Siguin p, q primers diferents, M un enter positiu primer amb pq. Sigui $l \geq 3$ primer, primer amb pqM.

9.2.4 Teorema. (A) *Sigui* m *un ideal maximal p-nou de* $\mathbb{T}_{pqM}$*, amb característica residual* l*. Suposem que* ρ_{m} *és irreductible. Suposem que* $\rho_{\mathrm{m}}(\mathrm{Frob}_q)$ *té traça 0 i determinant -1. Aleshores* m *és pq-nou de* $\mathbb{T}_{Mpq}$*.*

9.2.5 Teorema. (B) *Sigui* m *un ideal maximal pq-nou de* $\mathbb{T}_{pqM}$*, amb característica residual* l*. Suposem que* $q \not\equiv 1 \pmod{l}$*. Suposem que* ρ_{m} *és irreductible i finita en p. Aleshores* ρ_{m} *és modular de nivell* qM*.*

Notem que el primer teorema fa pujar el nivell a pqM i el segon permet fer l'abaixament a qM.

La prova d'aquests dos teoremes requereix la introducció d'una corba de Shimura associada a l'ordre d'Eichler de nivell M d'una àlgebra de quaternions de discriminant pq. En aquesta corba els primers p i q juguen un paper similar, això permetrà intercanviar els primers p i q.

9.2.5 La corba de Shimura

Siguin p, q primers diferents, M un enter positiu primer amb pq. Sigui $l \geq 3$ primer, relativament primer amb pqM. Sigui $C/\mathbb{Q}$ la corba de Shimura associada al grup d'unitats de norma 1 d'un ordre d'Eichler de nivell M en l'àlgebra de quaternions sobre $\mathbb{Q}$ de discriminant pq.

Sigui $J = \mathrm{Pic}^0(C)$ la jacobiana de C.

Sigui $\overline{\mathbb{T}}$ el quocient pq-nou de $\mathbb{T}_{pqM}$. Sigui m un ideal maximal de $\overline{\mathbb{T}}$ de característica residual $l \geq 3$. Suposem que ρ_{m} és irreductible.

Considerem el $\mathbb{T}/\mathrm{m}[G_{\mathbb{Q}}]$-mòdul

$$W = J(\overline{\mathbb{Q}})[\mathrm{m}],$$

$W \neq 0$ doncs m és ideal de $\overline{\mathbb{T}}$.

Sigui

$$V = J_0(pqM)(\overline{\mathbb{Q}})[\mathrm{m}]$$

el $\mathbb{T}/\mathrm{m}[G_{\mathbb{Q}}]$-mòdul corresponent a ρ_{m}.

Tenim els fets següents:

- De les relacions de Eichler-Shimura per a J (cf. Travesa, capítol 6) tenim una immersió $V \hookrightarrow W$ de $\mathbb{T}/\mathrm{m}[G_{\mathbb{Q}}]$-mòduls i podem identificar $V \hookrightarrow J(\overline{\mathbb{F}}_p)$, doncs $p \neq l$ i V és no ramificat en p. A més, les accions naturals de $\mathbb{T}$ i de $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ a V i a $J(\overline{\mathbb{F}}_p)$ respecten aquesta inclusió.
- Pels treballs de Cerednik i de Drinfeld (cf. Xarles, capítol 3) sabem que J té reducció a p purament tòrica.
- Pel Teorema 9.1.5 (Ribet) tenim que J és $\mathbb{Q}$-isògena al quocient pq-nou de $J_0(pqM)$.

Cal tenir en compte que $S_2(\Gamma_0(pM)) \oplus S_2(\Gamma_0(pM))$ es pot veure com el subespai q-vell de $S_2(\Gamma_0(pqM))$. L'anell $\mathbb{T}_{pqM}$ actua fidelment a $S_2(\Gamma_0(pqM))$ i preserva la descomposició $S_2(\Gamma_0(pM)) \oplus S_2(\Gamma_0(pM))$. La imatge de $\mathbb{T}_{pqM}$ en l'anell $\mathrm{End}(S_2(\Gamma_0(pM))^2)$ és el quocient q-vell de $\mathbb{T}_{pqM}$.

Siguin $\mathcal{X}(qM)_q$, $\mathcal{X}(pqM)_q$ els grups de caràcters de la part tòrica de la reducció de $J_0(qM)$ a q i de $J_0(pqM)$ a q.

Sigui Y el nucli de l'epimorfisme $\mathcal{X}(pqM)_q \to \mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q$.

Es té la successió exacta:

$$0 \to Y \to \mathcal{X}(pqM)_q \to \mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q \to 0.$$

Siguin $\Phi_{qM,q}$, $\Phi_{pqM,q}$ els grups de components de la reducció de $J_0(qM)$ a q i de $J_0(pqM)$ a q. Es té la successió exacta:

$$0 \to A \to \Phi_{qM,q} \oplus \Phi_{qM,q} \to \Phi_{pqM,q} \to B \to 0,$$

on A i B són el nucli i el conucli del morfisme natural

$$\Phi_{qM,q} \oplus \Phi_{qM,q} \to \Phi_{pqM,q}.$$

Sigui Z el grup de caràcters i Ψ el grup de components del torus associat a la reducció de J a p.

Ribet demostra els dos resultats següents que relacionen la reducció en p en la corba de Shimura i la reducció en q en la modular, respectant l'acció de l'àlgebra de Hecke.

- Z i Y són $\mathbb{T}$-isomorfs (Th. 4.1, [Rib90b]).
- La successió de $\mathbb{T}$-mòduls és exacta (Th. 4.3, [Rib90b]):

$0 \to A \to \mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q/(T_p^2-1)(\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q) \to \Psi \to B \to 0$.

9.2.6 Prova dels teoremes clau

En lloc del teorema A provarem el teorema A' que diu exactament el mateix però intercanviant la q i la p, a fi d'estar en la situació de poder utilitzar les notacions de l'apartat anterior.

9.2.6 Teorema. (A') *Sigui* m *un ideal maximal q-nou de $\mathbb{T}_{pqM}$, amb característica residual l. Suposem que ρ_{m} és irreductible. Suposem que $\rho_{\mathrm{m}}(\mathrm{Frob}_p)$ té traça 0 i determinant -1. Aleshores* m *és pq-nou de $\mathbb{T}_{Mpq}$.*

Es prova primer que el polinomi característic de T_p,

$$(T_p)^2 - 1 \in \mathrm{m}.$$

Ara m és q-nou/p-vell, per tant

$$\mathrm{m} \in \mathrm{Sup}(\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q).$$

Aleshores,

$$\mathrm{m} \in \mathrm{Sup}(\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q)/(T_p^2-1)(\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q).$$

De la successió exacta s'obté que

$$\mathrm{m} \in \mathrm{Sup}(\Psi).$$

Però $\mathbb{T}_{Mpq}$ actua a Ψ a través de $\overline{\mathbb{T}}$, el quocient pq-nou de $\mathbb{T}_{pqM}$.□

Per provar el teorema B distingim dos casos.

Primer cas: La imatge de V a Ψ és no nul.la. Aleshores $\mathrm{m} \in \mathrm{Sup}(\Psi)$. De la successió exacta tenim que

$$\mathrm{m} \in \mathrm{Sup}(\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q).$$

D'altra banda, l'àlgebra de Hecke $\mathbb{T}$ actua a $\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q$ a través del seu quocient q-nou/p-vell, fidelment (cf. [Rib90b], Th. 3.21). És a dir, m prové d'un quocient de $\mathbb{T}$, q-nou/p-vell. En conseqüència, ρ_{m} és isomorf a un ρ_λ, per λ ideal maximal de $\mathbb{T}_{qM}$, per tant ρ_{m} és modular de nivell qM.

Segon cas: La imatge de V a Ψ és nul.la. Aleshores tenim la inclusió $V \subset \mathrm{Hom}(Z/\mathrm{m}Z, \mu_l)$. Per tant,

$$\dim_{\mathbb{T}/\mathrm{m}}(Z/\mathrm{m}Z) \geq 2.$$

Ara com que Z i Y són $\mathbb{T}$-isomorfs,

$$\dim_{\mathbb{T}/\mathrm{m}}(Y/\mathrm{m}Y) \geq 2.$$

Podem suposar que $\mathrm{m} \nsubseteq \mathrm{Sup}(\mathcal{X}(qM)_q \oplus \mathcal{X}(qM)_q)$, doncs en cas contrari, estem en el primer cas i ja sabem deduir que ρ_{m} és modular de nivell qM. Aleshores, tenim l'isomorfisme

$$Y/\mathrm{m}Y \approx \mathcal{X}(pqM)_q/\mathrm{m}\mathcal{X}(pqM)_q,$$

que ens permet afirmar que

$$\dim_{\mathbb{T}/\mathrm{m}}(\mathcal{X}(pqM)_q/\mathrm{m}\mathcal{X}(pqM)_q) \geq 2.$$

Però això és una contradicció amb el fet que $q \not\equiv 1 \pmod{l}$ i el teorema de Mazur, canviant p per q i M per pM. $\square$

Bibliografia

[AL70] A. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[Are03] A. Arenas, *On the traces of Hecke operators*, J. Number Theory **100** (2003), num. 2, 307–312.

[DR73] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Antwerp, 1972), Lecture Notes in Math., vol. 349, Springer, 1973, pp. 143–316.

[Eic55a] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156–171.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), num. 3, 349–366.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), num. 47, 33–186 (1978).

[Miy71] T. Miyake, *On automorphic forms on* GL_2 *and Hecke operators*, Ann. of Math. **94** (1971), 174–189.

[Mor70] Y. Morita, *Ihara's conjectures and moduli space of abelian varieties*, Thesis, Univ. Tokyo, 1970.

[Rib80] K. Ribet, *Sur les variétés abéliennes à multiplications réelles*, C. R. Acad. Sci. Paris Sér. A-B **291** (1980), num. 2, 121–123.

[Rib90b] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), num. 2, 431–476.

[Ser87] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), num. 1, 179–230, *Oeuvres*, vol. IV, Springer, 2000.

[Ser00] J-P. Serre, *Œuvres. Collected papers. IV*, Springer, Berlin, 2000, 1985–1998.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

Capítol 10

Corbes de Shimura i codis de Goppa

P. Bayer

Donada una corba $X/\mathbb{F}_q$ projectiva, no singular i de gènere g, sabem pel teorema de Weil que el nombre dels seus punts racionals $n = \#X(\mathbb{F}_q)$ no pot excedir $1 + q + 2g\sqrt{q}$. Certes corbes de Shimura, associades a àlgebres de quaternions definides sobre cossos quadràtics reals, proporcionen corbes $X/\mathbb{F}_{p^4}$, per a $p \geq 3$ primer, que posseeixen molts punts racionals en relació amb el seu gènere. S'aconsegueixen així successions de corbes (X_i) per a les quals (g_i) i (n_i) tendeixen a ∞ i $g_i/n_i \approx (p^2-1)^{-1}$. El bon comportament asimptòtic d'aquestes famílies és rellevant en el context de la teoria de codis correctors d'errors.

Introducció

Un esquema de codificació lineal $\mathcal{C} = [n, k, d]$ sobre un cos finit $\mathbb{F}_q$ és donat per un subespai vectorial $C \subseteq \mathbb{F}_q^n$, de dimensió k, en el qual tot vector $x \in C$, $x \neq 0$, té un mínim de d coordenades no nul·les. El subespai C s'anomena el *codi*; el quocient $R := k/n$, la *taxa de transmissió*; i el quocient $\delta := d/n$, la *distància mínima relativa*.

Els paràmetres d'un codi estan sotmesos a certes restriccions. D'entrada, per una fita deguda a Singleton, es té que

$$R + \delta \leq 1 + 1/n.$$

Un dels problemes que es plantegen en la teoria de codis correctors d'errors és la construcció de successions $(\mathcal{C}_i)$ que posseeixin bones propietats asimptòtiques. És a dir, tals que si $\mathcal{C}_i = [n_i, k_i, d_i]$, se satisfaci que $\lim n_i = \infty$, i $R\delta > 0$, per a $R = \lim R_i$, $\delta = \lim \delta_i$.

L'any 1973, V. D. Goppa s'adonà de la possible construcció de codis lineals a partir de corbes algebraiques definides sobre cossos finits. L'obtenció de bons codis es tradueix aleshores en la construcció efectiva de corbes amb molts punts racionals en relació amb el seu gènere.

Si (X_i) és una successió de corbes sobre $\mathbb{F}_q$ per a la qual la successió (g_i) tendeix a ∞ i

$$\lim_{i\to\infty} g_i/\#X_i(\mathbb{F}_q) = \gamma < \infty,$$

aleshores, en la successió associada de codis de Goppa, es té que

$$R + \delta \geq 1 - \gamma.$$

L'any 1982, Y. Ihara [Iha81] i, independentment, M. A. Tsfasman-S. G. Vlăduț- Th. Zink [TVZ82] posaren de manifest l'existència de successions de corbes sobre $\mathbb{F}_{p^2}$, $p \geq 7$ primer, per a les quals

$$\gamma \approx (p-1)^{-1}.$$

Per a tal fi, utilitzaren les corbes modulars $X_0(N)$, les seves fibres de bona reducció en primers racionals, $p \nmid N$, i els punts supersingulars d'aquestes.

En el mateix treball, Tsfasman-Vlăduț-Zink [TVZ82] obtingueren successions de corbes definides sobre $\mathbb{F}_{p^4}$, $p \geq 3$ primer, per a les quals

$$\gamma \approx (p^2-1)^{-1}.$$

Per a tal fi, utilitzaren corbes de Shimura, torçaments de les seves fibres de bona reducció en primers $\mathfrak{P}$ d'un cos quàrtic totalment real, i punts especials d'aquestes.

Aquesta exposició versa sobre el teorema de Tsfasman-Vlăduț-Zink. Ens limitarem a tractar el cas associat a les corbes de Shimura, que és el més elaborat. El teorema de Tsfasman-Vlăduț-Zink es basa en un teorema previ de Zink [Zin82], en el qual s'analitzen fibres de reducció dolenta de certes *superfícies* de Shimura.

10.1 Superfícies de Shimura

En aquesta secció presentem una introducció breu a certes superfícies de Shimura i a la seva interpretació com a solució d'un problema de moduli definit sobre el cos complex $\mathbb{C}$.

Denotem per $\mathbb{A}$ l'anell de les adeles racionals; per $\mathbb{A}_f = \mathbb{Q} \otimes \widehat{\mathbb{Z}}$, el subanell de $\mathbb{A}$ de les adeles finites; i per $\mathbb{A}_f^p = \mathbb{Q} \otimes \widehat{\mathbb{Z}}^p$, el subanell de $\mathbb{A}_f$ de les adeles finites allunyades de p.

En tot el treball, K designarà un cos quadràtic totalment real i $\mathcal{O}_K$, el seu anell d'enters. Siguin p un primer racional, inert en K, i $\mathfrak{p} = p\mathcal{O}_K$.

Donats elements $\alpha, \beta \in K^*$, sigui $\mathrm{H} = \left(\dfrac{\alpha, \beta}{K}\right)$ la K-àlgebra de quaternions de base $\{1, i, j, k\}$ definida per les relacions

$$i^2 = \alpha, \quad j^2 = \beta, \quad ij = -ji = k.$$

Suposarem que H és ramificada en $\mathfrak{p}$ i que és no ramificada en les dues places de l'infinit de K. Aquesta darrera condició es tradueix en l'existència d'un isomorfisme

$$\mathrm{H} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2, \mathbb{R}) \times \mathrm{M}(2, \mathbb{R}),$$

on $\mathrm{M}(2, \mathbb{R})$ designa l'àlgebra de les matrius reals 2×2.

Donat un quaternió

$$q = a + bi + cj + dk, \quad a, b, c, d \in K,$$

definim

$$q^* = a - bi - cj - dk.$$

L'aplicació $q \to q^*$ és la involució principal de H.

Denotarem per $\mathrm{Tr}^0, \mathrm{Nr}^0$ la traça i la norma reduïdes en H:

$$\mathrm{Tr}^0(q) = q + q^*, \quad \mathrm{Nr}^0(q) = qq^*.$$

Interpretem el grup multiplicatiu H^* com un grup algèbric, definit sobre $\mathbb{Q}$, i fixem la immersió

$$\begin{array}{rccc} h_0: & \mathbb{Q}(i) & \hookrightarrow & \mathrm{H} \otimes_{\mathbb{Q}} \mathbb{R} \\ & i & \mapsto & \begin{bmatrix} & -1 \\ 1 & \end{bmatrix} \times \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}. \end{array}$$

D'aquesta manera, podem considerarem el grup

$$\Gamma_\infty := h_0(\mathbb{Q}(i)^*)$$

com un subgrup de $(\mathrm{H} \otimes_{\mathbb{Q}} \mathbb{R})^* = \mathbf{GL}(2,\mathbb{R}) \times \mathbf{GL}(2,\mathbb{R})$.

Donat un subgrup $\Gamma \subseteq \mathrm{H}^*(\mathbb{A}_f)$ compacte, obert i suficientment petit, els treballs de Shimura, exposats per Deligne [Del71], posen de manifest l'existència d'una superfície complexa $X(\mathrm{H},\Gamma)$ llisa i quasi-projectiva tal que

$$X(\mathrm{H},\Gamma)(\mathbb{C}) = (\Gamma_\infty \times \Gamma)\backslash \mathrm{H}^*(\mathbb{A})/\mathrm{H}^*(\mathbb{Q}).$$

En molts casos, la *superfície de Shimura* $X(\mathrm{H},\Gamma)$ posseeix un model canònic, definit sobre un cos de nombres $E = E(\mathrm{H}, h_0)$.

El grup d'adeles quaterniòniques $\mathrm{H}^*(\mathbb{A}_f)$ opera per l'esquerra en el sistema projectiu

$$X(\mathrm{H}) = \lim_\Gamma X(\mathrm{H},\Gamma),$$

obtingut en prendre el límit sobre tots els subgrups Γ possibles.

A fi d'obtenir una interpretació modular de les superfícies $X(\mathrm{H},\Gamma)$, ens caldrà fixar certs ordres de H.

Començarem per triar una extensió quadràtica totalment real E/K tal que l'extensió quàrtica $E/\mathbb{Q}$ sigui de Galois i no ramificada en p. Sigui $\mathrm{Gal}(E|K) = \langle\tau\rangle$. Suposarem que el cos E descompon l'àlgebra de quaternions H; és a dir,

$$\mathrm{H} \otimes_K E \simeq \mathrm{M}(2,E).$$

Pel teorema de Skolem-Noether, existeix un quaternió $a \in \mathrm{H}$ tal que $e^\tau = aea^{-1}$, per a tot $e \in E$. Se satisfà que $a^2 = -\delta \in K$. Sense restricció, podem suposar que δ és un element totalment positiu de $\mathcal{O}_K$ i que $v_\mathfrak{p}(\delta) = 1$. La fórmula

$$q \mapsto \hat{q} = aq^* a^{-1}$$

defineix una involució positiva de H.

Si $\mathcal{O}_E$ designa l'anell d'enters de E, l'extensió d'anells

$$\mathcal{O}_\mathrm{H} := \mathcal{O}_E[a]$$

defineix un ordre de H que és maximal en $\mathfrak{p}$. Considerarem el conjunt $V = \mathcal{O}_\mathrm{H}$ com un $\mathcal{O}_\mathrm{H}$-mòdul per l'esquerra i, en particular, com un $\mathcal{O}_K$-mòdul lliure. Notem que $\dim_{\mathcal{O}_K} V = 4$.

La proposició que segueix s'obté sense dificultat a partir de les definicions donades.

10.1.1 Proposició. *Sigui $B : V \times V \longrightarrow \mathcal{O}_K$ l'aplicació definida per*

$$B(v, w) = \mathrm{Tr}^0(a^{-1}\hat{v}w) = \mathrm{Tr}^0(a^{-1}wv^*), \quad v, w \in V.$$

Se satisfà que

i) B és una $\mathcal{O}_K$-forma bilineal, alternada i no degenerada.

ii) Per a tot $q \in \mathcal{O}_\mathrm{H}$ i per a tot $v, w \in V$,

$$B(qv, w) = B(v, \hat{q}w).$$

iii) Existeix un element $k \in K$ tal que $kB(v, w\, h_0(i))$ és una forma bilineal sobre $V \otimes \mathbb{R}$, simètrica i definida positiva.

El teorema següent interpreta la superfície $X(\mathrm{H}, \Gamma)$ com a esquema de moduli d'esquemes abelians amb *multiplicació quaterniònica* (MQ).

10.1.2 Teorema. *Existeix un esquema groller de moduli $X(\mathrm{H}, \Gamma)$, projectiu sobre $\mathbb{C}$, associat al functor que a tot esquema T sobre* Spec($\mathbb{C}$) *li fa correspondre els objectes $(A, \iota, \overline{\lambda}, \overline{\eta})$ següents:*

1. *Una classe d'isomorfia d'esquemes abelians A/T, de dimensió relativa* 4.

2. *Un monomorfisme $\iota : \mathcal{O}_{\mathrm{H}} \hookrightarrow \mathrm{End}_T(A)$ tal que*

$$\mathrm{Tr}(\iota(q) \mid \mathrm{Lie}(A)) = \mathrm{Tr}_{K|\mathbb{Q}}\mathrm{Tr}^0(q), \quad q \in \mathcal{O}_{\mathrm{H}}.$$

3. *Una classe de polaritzacions $\overline{\lambda} \in \mathrm{Hom}^0_K(A, A^*)/K^*$ tal que $\iota(\hat{q})$ és la involució de Rosati de $\iota(q)$.*

4. *Una Γ-classe d'equivalència d'isomorfismes de $\mathcal{O}_{\mathrm{H}} \otimes \widehat{\mathbb{Z}}$-mòduls*

$$\overline{\eta} : \widehat{T}(A) \longrightarrow \mathcal{O}_{\mathrm{H}} \otimes \widehat{\mathbb{Z}} \ (\mathrm{mod}\, \Gamma)$$

que respecten, llevat de constants, les formes $\mathcal{O}_K \otimes \widehat{\mathbb{Z}}$-bilineals d'ambdós termes.

En el teorema, $\widehat{T}(A) := \prod_{\ell \in \mathrm{Spec}(\mathbb{Z})} T_\ell(A)$ designa el mòdul de Tate de A.

10.2 Interpretació modular local

Abans de procedir a la interpretació modular de les fibres de les superfícies de Shimura, ens caldrà escollir certes estructures de nivell.

Donat un enter N, primer amb p, definim

$$\Gamma(N) = \{q \in \mathrm{Aut}_{\mathcal{O}_{\mathrm{H}}}(V \otimes \widehat{\mathbb{Z}}) \mid q \equiv 1 \,\mathrm{a}\, (V \otimes \mathbb{Z}/N\mathbb{Z})\}.$$

Siguin

$$\Gamma^p \subseteq \mathrm{H}^*(\mathbb{A}_f^p), \quad \Gamma_p = \mathrm{GL}_{\mathcal{O}_{\mathrm{H}}}(V \otimes \mathbb{Z}_p).$$

Considerarem únicament subgrups $\Gamma := \Gamma^p\Gamma_p$ tals que $\Gamma \subseteq \Gamma(N)$, per a un cert $N \geq 3$.

10.2.1 Definició. *Sigui A un T-esquema abelià amb multiplicació quaterniònica*

$$\iota : \mathcal{O}_{\mathrm{H}} \hookrightarrow \mathrm{End}_T(A).$$

El parell (A, ι) s'anomena un $\mathcal{O}_{\mathrm{H}}$-esquema abelià especial si

$$\mathrm{Tr}(\iota(q) \mid \mathrm{Lie}(A)) = \mathrm{Tr}_{K|\mathbb{Q}}\mathrm{Tr}^0(q), \quad q \in \mathcal{O}_{\mathrm{H}}.$$

Cal tenir present el resultat següent.

10.2.2 Proposició. *Tota varietat abeliana A de dimensió parella amb multiplicació quaterniònica per $\mathcal{O}_{\mathrm{H}}$ i definida sobre un cos valorat, respecte d'una valoració discreta, té bona reducció potencial.*

Descrivim tot seguit la interpretació modular local de les superfícies de Shimura.

10.2.3 Teorema. *Existeix un esquema groller de moduli $\mathcal{X}(\mathrm{H},\Gamma)$, projectiu sobre $\mathbb{Z}_p$, associat al functor que a tot esquema T sobre* $\mathrm{Spec}(\mathbb{Z}_p)$ *li fa correspondre els objectes següents:*

1. *Un $\mathcal{O}_{\mathrm{H}}$-esquema abelià especial (A,ι) definit sobre T.*
2. *Una classe de polaritzacions $\overline{\lambda}\in \mathrm{Hom}^0_{K_{\mathfrak{p}}}(A,A^*)/K^*_{\mathfrak{p}}$ tal que $\iota(\hat{q})$ és la involució de Rosati de $\iota(q)$.*
3. *Una Γ^p-classe d'equivalència d'isomorfismes de $\mathcal{O}_{\mathrm{H}}\otimes\widehat{\mathbb{Z}}^p$-mòduls*

$$\overline{\eta}:\widehat{T}^p(A)\longrightarrow \mathcal{O}_{\mathrm{H}}\otimes\widehat{\mathbb{Z}}^p \pmod{\Gamma^p}.$$

La demostració del teorema anterior s'obté a partir de la consideració d'un problema fi de moduli, recobriment galoisià del problema anterior, que descriurem tot seguit.

Sigui

$$K^*(\mathbb{A}_f^p(-1))=\{k\in K\otimes\widehat{\mathbb{Z}}^p(-1)\mid k'\cdot k=1,\ \text{per a un } k'\in K\otimes\widehat{\mathbb{Z}}^p(1)\}.$$

Considerem el conjunt, finit,

$$\mathrm{Nr}^0(\Gamma^p)\backslash K^*(\mathbb{A}_f^p(-1))/U_p(K_+)=\{\kappa_1,\dots,\kappa_h\}.$$

Suposarem donada una extensió quadràtica no ramificada $E_{\mathfrak{P}}/K_{\mathfrak{p}}$ tal que $E_{\mathfrak{P}}\subseteq \mathrm{H}_{\mathfrak{p}}$; equivalentment,

$$\mathrm{H}_{\mathfrak{p}}\otimes_{K_{\mathfrak{p}}} E_{\mathfrak{P}}=\mathrm{M}(2,E_{\mathfrak{P}}).$$

Siguin $\sigma=\mathrm{Frob}(E|\mathbb{Q}_p)$, $\mathrm{Gal}(E|K)=\langle\tau\rangle$, $\tau=\sigma^2$.

Sigui $\widetilde{\mathcal{X}}(\mathrm{H},\Gamma)$ la forma de $\mathcal{X}(\mathrm{H},\Gamma)$ definida sobre $\mathcal{O}_{E_{\mathfrak{P}}}$ en què l'element de Frobenius sobre $\mathbb{F}_p$ actua com $\tau\circ(1,\dots,p^{-2},\dots,1)$, on τ designa l'acció de l'element de Frobenius sobre $\mathcal{X}(\mathrm{H},\Gamma)$. En particular,

$$\widetilde{\mathcal{X}}(\mathrm{H},\Gamma)\otimes\mathcal{O}_{E_{\mathfrak{P}}^{\mathrm{nr}}}=\mathcal{X}(\mathrm{H},\Gamma)\otimes\mathcal{O}_{E_{\mathfrak{P}}^{\mathrm{nr}}}.$$

10.2.4 Teorema. *Existeixen una extensió $R/\mathbb{Z}_p$, finita i no ramificada, i un esquema R-esquema quasiprojectiu $\widetilde{\mathcal{X}}(\mathrm{H},\Gamma)$ tal que, per a tot R-esquema T, els punts $\widetilde{\mathcal{X}}(\mathrm{H},\Gamma)(T)$ descriuen els objectes següents:*

1. *Un $\mathcal{O}_{\mathrm{H}}$-esquema abelià especial (A,ι) definit sobre T.*
2. *Una polarització λ de A, principal en p, tal que $\iota(\hat{q})$ és la involució de Rosati de $\iota(q)$.*
3. *Una Γ^p-classe d'equivalència d'isomorfismes de $\mathcal{O}_{\mathrm{H}}\otimes\widehat{\mathbb{Z}}^p$-mòduls*

$$\overline{\eta}:\widehat{T}^p(A)\longrightarrow\mathcal{O}_{\mathrm{H}}\otimes\widehat{\mathbb{Z}}^p\ (\mathrm{mod}\,\Gamma^p)$$

tal que $\kappa(A,\iota,\lambda,\overline{\eta})=\kappa_i$, per a un i, $1\le i\le h$.

10.3 Mòduls formals

El proper objectiu és la descripció de la fibra especial $\mathcal{X}(\Gamma,H)\otimes_{\mathbb{Z}_p}\mathcal{O}_{E_{\mathfrak{P}}}/\mathfrak{P}\mathcal{O}_{E_{\mathfrak{P}}}$. Per a aquest fi, necessitem estudiar amb més detall els esquemes abelians especials sobre cossos algebraicament tancats de característica positiva. Introduirem prèviament el concepte de tipus en els mòduls formals amb multiplicació quaterniònica.

Sigui $K_{\mathfrak{p}}/\mathbb{Q}_p$ una extensió quadràtica i no ramificada, i sigui $\mathrm{H}_{\mathfrak{p}}=\left(\dfrac{\alpha,\beta}{K_{\mathfrak{p}}}\right)$ una àlgebra de quaternions d'invariant $1/2$. Designem per $\mathcal{O}_{\mathrm{H}_{\mathfrak{p}}}$ el seu ordre maximal. Prenem l'extensió $E_{\mathfrak{P}}/K_{\mathfrak{p}}$ com en la secció anterior.

10.3.1 Definició. *Un tipus t és una aplicació*

$$t:\mathbb{Z}/4\mathbb{Z}\to\{-1,0,1\}$$

tal que

$$t(i)+t(i+2)=0,\quad |t(i+1)+t(i+2)|\le 1,\quad \text{per a tot } i\in\mathbb{Z}/4\mathbb{Z}.$$

10.3.2 Definició. *Sigui T un esquema sobre $\mathrm{Spec}(\mathcal{O}_{E_\mathfrak{P}})$. Donats un T-esquema formal X i una immersió d'anells*

$$\iota : \mathcal{O}_{\mathrm{H}_\mathfrak{p}} \hookrightarrow \mathrm{End}_T(X),$$

el parell (X, ι) s'anomena un $\mathcal{O}_{\mathrm{H}_\mathfrak{p}}$-mòdul formal de tipus t si

$$\mathrm{Tr}_{\mathcal{O}_T}(\iota(e)|\mathrm{Lie}(X)) = \mathrm{Tr}_{E_\mathfrak{P}|\mathbb{Q}_p}\mathrm{Tr}^0(e) + \sum_i t(i)\sigma^{-i}(e),$$

per a tot $e \in \mathcal{O}_{E_\mathfrak{P}}$.

Si $t \equiv 0$, l'esquema formal X s'anomena un $\mathcal{O}_{\mathrm{H}_\mathfrak{p}}$-mòdul formal especial. Si $t \not\equiv 0$ i $T = \mathrm{Spec}(R)$, aleshores $pR = 0$.

Tota $\mathbb{Z}_p$-àlgebra R té associats un anell de Witt, $W(R)$, i un anell de Cartier, $\mathrm{Cart}(R)$. Recordem que

$$\mathrm{Cart}(R) = \left\{ \sum_{r,s\geq 0} V^r[x_{r,s}]F^s \mid x_{r,s} \in R, x_{r,s} = 0 \quad \text{q.p.t. } s, \text{ fixat } r \right\}.$$

L'estructura de $\mathrm{Cart}(R)$ com a $\mathbb{Z}_p$-àlgebra és donada per les relacions següents:

$$1 = [1], \quad FV = p, \quad F[x] = [x^p]F, \quad [x]V = V[x^p],$$

$$[x][y] = [y][x], \quad \text{per a tot } x, y \in R,$$

$$[x] + [y] = [x + y] + \sum_{r\geq 1} V^r[z_r]F^r, \quad \text{per a certs } z_r \in R.$$

10.3.3 Definició. *Un mòdul M sobre $\mathrm{Cart}(R)$ s'anomena reduït quan satisfà les condicions que segueixen.*

i) L'element $V \in \mathrm{Cart}(R)$ opera de manera injectiva en M.

ii) El quocient M/VM és un R-mòdul projectiu i finitament generat.

iii) $\limproj M/V^iM = M$.

Donada una $\mathcal{O}_{E_{\mathfrak{P}}}$-àlgebra R, existeix un homomorfisme canònic de $\mathcal{O}_{E_{\mathfrak{P}}}$ en $\mathrm{Cart}(R)$ que permet obtenir la graduació $M = \oplus_{i=1}^{4} M_i$:

$$M_i = \{m \in M \mid \iota(e)m = e^{\sigma^{-i}}m, \quad e \in \mathcal{O}_{E_{\mathfrak{P}}}\}.$$

10.3.4 Proposició. *Donada una $\mathcal{O}_{E_{\mathfrak{P}}}$-àlgebra R, la categoria dels $\mathcal{O}_{\mathrm{H}_{\mathfrak{p}}}$-mòduls formals amb multiplicació quaterniònica de tipus t sobre R és equivalent a la categoria dels mòduls de Cartier reduïts i $\mathbb{Z}/4\mathbb{Z}$-graduats, $M = \oplus_{i\in\mathbb{Z}/4\mathbb{Z}} M_i$, que satisfan les propietats següents:*

i) *V, F, i els elements $x \in R$ operen en M com a aplicacions homogènies de graus $1, -1, 0$, respectivament.*

ii) *Existeix un endomorfisme homogeni Π de grau 2 de M tal que $\Pi^2 = p$.*

iii) $\mathrm{rang} M_i/VM_{i-1} = 1 + t(i)$, *per a $i \in \mathbb{Z}/4\mathbb{Z}$.*

10.3.5 Teorema. *Siguin L un cos perfecte de característica p i X un grup formal d'altura h sobre L. Aleshores,*

i) *El mòdul de Cartier $M(X)$ és un $W(L)$-mòdul lliure, de rang h.*

ii) *Si X és un $\mathcal{O}_{\mathrm{H}_{\mathfrak{p}}}$-mòdul, aleshores h és igual a 0 o bé a 8.*

iii) *Si $\mathcal{K}$ designa el cos de fraccions de $W(L)$, el submòdul*

$$(M_0 \otimes_{W(L)} \mathcal{K}, V^2\Pi^{-1})$$

determina la classe d'isogènia de X.

10.3.6 Definició. *Suposem que R és un anell de característica p. Siguin $X/\mathrm{Spec}(R)$ un $\mathcal{O}_{\mathrm{H}_{\mathfrak{p}}}$-mòdul formal i $M = \oplus_{i=1}^{4} M_i$, el seu mòdul de Cartier. El conjunt crític de X es defineix com*

$$S(X) = \{i \mid \Pi : M_i/VM_{i-1} \to M_{i+2}/VM_{i+1}, \Pi \equiv 0\}.$$

10.3.7 Definició. *Un subconjunt $S \subseteq \mathbb{Z}/4\mathbb{Z}$ s'anomena admissible si per a tot i se satisfà que $i \in S$ o bé $i + 2 \in S$.*

10.3.8 Definició. *Un conjunt $S = S_t$ s'anomena saturat si*

$$S_t = \{i \in \mathbb{Z}/4\mathbb{Z} \mid |t(i)| = 1, o\ bé\ t(i-1) + t(i) = 1\}.$$

10.4 Esquemes abelians especials

Els conceptes de la secció anterior permeten obtenir informació del problema de moduli sobre $\overline{\mathbb{F}}_p$.

10.4.1 Proposició. *Sigui A un $\mathcal{O}_{\mathrm{H}_\mathfrak{p}}$-esquema abelià especial definit sobre un cos algebraicament tancat L de característica p. Aleshores,*

i) $\mathrm{rang}_p(A) = 0$.

ii) L'esquema A és isogen a un producte de corbes el·líptiques supersingulars si, i només si, el $\mathcal{O}_{\mathrm{H}_\mathfrak{p}}$-mòdul formal especial $X = X(A)$ és supersingular; és a dir, $S(X) = \mathbb{Z}/4\mathbb{Z}$.

iii) Si $X(A)$ és supersingular, A és producte de corbes el·líptiques supersingulars.

10.4.2 Proposició. *Donat un conjunt saturat $S \subseteq \mathbb{Z}/4\mathbb{Z}$, existeix un $\mathcal{O}_{\mathrm{H}_\mathfrak{p}}$-mòdul formal especial Y, únic a menys d'isomorfismes, tal que el seu conjunt crític $S(Y) = S$.*

i) Si $S = \mathbb{Z}/4\mathbb{Z}$, Y és supersingular.

ii) Si $S \neq \mathbb{Z}/4\mathbb{Z}$, aleshores el tipus d'isogènia de Y és determinat per la matriu

$$J = \begin{bmatrix} p^{s_1} & 0 \\ 0 & p^{s_2} \end{bmatrix},$$

on $s_1 = \frac{1}{2}(\frac{1}{2}\#\overline{S} - 1)$, $s_2 = 2 - \frac{1}{2}(\frac{1}{2}\#\overline{S} + 1)$, $\overline{S} := S \cap (S+2)$.

Volem ara calcular els endomorfismes dels $\mathcal{O}_{\mathrm{H}}$-esquemes abelians especials en $\mathfrak{p}$.

10.4.3 Proposició. *Sigui A un $\mathcal{O}_{\mathrm{H}}$-esquema abelià especial definit sobre el cos algebraicament tancat $\overline{\mathbb{F}}_p$.*

i) Si A no és supersingular, aleshores $\mathrm{End}^0_{\mathrm{H}}(A)$ és un cos totalment imaginari, extensió quadràtica del cos K, en el qual $\mathfrak{p}$ descompon completament.

ii) Si A és supersingular, aleshores $\mathrm{End}^0_{\mathrm{H}}(A) = \mathrm{H}_-$ *on* H_- *és la K-àlgebra de quaternions definida pels invariants següents:*

$$\mathrm{inv}_\nu \mathrm{H}_- = \begin{cases} \frac{1}{2}, & \text{si } \nu = \mathfrak{p}, \\ \mathrm{inv}_\nu \mathrm{H}, & \text{si } \nu \text{ és no arquimedià i } \nu \neq \mathfrak{p}, \\ \frac{1}{2}, & \text{si } \nu \text{ és arquimedià.} \end{cases}$$

10.4.4 Corol·lari. *En prendre com a esquema base $\mathcal{O}_{E_\mathfrak{P}}$, es té que*

i) $\mathrm{Aut}(A, \iota, \overline{\lambda}, \overline{\eta}) = K^* \cap \Gamma$.

ii) $\mathcal{X}(\mathrm{H}, \Gamma) \otimes_{\mathbb{Z}_p} \mathcal{O}_{E_\mathfrak{P}}$ és un esquema fi de moduli.

10.5 El teorema de Zink

Donat un conjunt admissible $S \subseteq \mathbb{Z}/4\mathbb{Z}$, sigui $\mathcal{X}(\mathrm{H}, \Gamma, S)$ el subesquema tancat de

$$\mathcal{X}(\mathrm{H}, \Gamma) \otimes_{\mathbb{Z}_p} \mathcal{O}_{E_\mathfrak{P}} / \mathfrak{P}\mathcal{O}_{E_\mathfrak{P}} = \mathcal{X}(\mathrm{H}, \Gamma) \otimes_{\mathbb{Z}_p} \mathbb{F}_{p^4}$$

tal que

$$\mathcal{X}(\mathrm{H}, \Gamma, S)(T) = \{(A, \iota, \overline{\eta})\} \mid S(A) \supseteq S\}.$$

Es demostra que $\mathcal{X}(\mathrm{H}, \Gamma, S)$ és un esquema llis de dimensió $4 - \#S$.

L'estructura de la fibra especial de $\mathcal{X}(\mathrm{H}, \Gamma)$ s'obté a partir dels resultats de Zink [Zin82].

10.5.1 Teorema. *La fibra en $\mathfrak{P}$ de $\mathcal{X}(\mathrm{H}, \Gamma)$ admet la descripció següent:*

i) $\mathcal{X}(\mathrm{H}, \Gamma) \otimes_{\mathbb{Z}_p} \mathcal{O}_{E_\mathfrak{P}} / \mathfrak{P}\mathcal{O}_{E_\mathfrak{P}} = \bigcup_S \mathcal{X}(\mathrm{H}, \Gamma, S)$.

ii) Els esquemes $\mathcal{X}(\mathrm{H}, \Gamma, S)$, $\mathcal{X}(\mathrm{H}, \Gamma, S')$ es tallen transversalment. A més,

$$\mathcal{X}(\mathrm{H}, \Gamma, S) \cap \mathcal{X}(\mathrm{H}, \Gamma, S') = \mathcal{X}(\mathrm{H}, \Gamma, S \cup S').$$

iii) $\mathcal{X}(\mathrm{H},\Gamma,S)$ *és una* $\mathbb{P}^1$*-fibració.*

Sigui $[i+1,j]\subseteq\overline{S}$ *un interval tal que* $i\in S\backslash\overline{S}$*,* $j+1\notin\overline{S}$ *i* $j+1\in S$ *si, i només si,* $j-i$ *és senar. Sigui* $m=\#[i+1,j]$*.*

iv) Si la diferència $j-i$ *és senar, la base de la fibració és*

$$\mathcal{X}(\mathrm{H},\Gamma,S\cup\{i+2\}),\quad \mathcal{X}(\mathrm{H},\Gamma,S\cup\{j+3\}).$$

Les fibres tallen l'esquema $\mathcal{X}(\mathrm{H},\Gamma,S\cup\{i+2\})$ *amb multiplicitat* p^{m+1} *i l'esquema* $\mathcal{X}(\mathrm{H},\Gamma,S\cup\{j+3\})$ *amb multiplicitat* 1*.*

v) Si la diferència $j-i$ *és parella, la base de la fibració és*

$$\mathcal{X}(\mathrm{H},\Gamma,S\cup\{i+2\}),\quad \mathcal{X}(\mathrm{H},\Gamma,S\cup\{j+1\}).$$

Les fibres tallen l'esquema $\mathcal{X}(\mathrm{H},\Gamma,S\cup\{i+2\})$ *amb multiplicitat* p^{m+1} *i l'esquema* $\mathcal{X}(\mathrm{H},\Gamma,S\cup\{j+1\})$ *amb multiplicitat* 1*.*

10.6 El teorema de Tsfasman-Vlăduț-Zink

Sigui $B=\left(\dfrac{a,b}{K}\right)$ una àlgebra de quaternions ramificada únicament en una plaça de l'infinit del cos K. Aleshores

$$B\otimes_{\mathbb{Q}}\mathbb{R}=\mathrm{M}(2,\mathbb{R})\times\mathbb{H},$$

on $\mathbb{H}=\left(\dfrac{-1,-1}{K}\right)$ designa el cos dels quaternions de Hamilton. Suposem que B és no ramificada en p; o sigui que $\mathrm{inv}_p(B)=1$.

Sigui $\Gamma\subseteq B^*(\mathbb{A}_f)$ un subgrup compacte i obert, que suposarem de la forma

$$\Gamma=\Gamma^p\Gamma_p,\quad \Gamma^p\subseteq B^*(\mathbb{A}_f^p),\quad \Gamma_p\subseteq B^*(\mathbb{Q}_p)=\mathbf{GL}(2,\mathbb{Q}_p),$$

per a Γ_p un subgrup compacte maximal.

Suposarem, també, que $\Gamma\subseteq\Gamma(N)$, on $\Gamma(N)$ és el grup de congruència de nivell $N\geq 3$, primer amb p, definit per

$$\Gamma(N)=\{q\in B^*(\mathbb{A}_f)\mid (q-1)(\mathcal{O}_B)\otimes\widehat{\mathbb{Z}}\subseteq N(\mathcal{O}_B\otimes\widehat{\mathbb{Z}})\},$$

i on $\mathcal{O}_B$ és un cert ordre de B.

En aquest cas, la teoria dels models canònics proporciona una *corba* llisa $X(B,\Gamma)$, definida sobre K, tal que

$$X(B,\Gamma)(\mathbb{C}) = (\Gamma \times \Gamma_\infty)\backslash B^*(\mathbb{A})/B^*(\mathbb{Q}).$$

La corba en qüestió té bona reducció en p. Per tant, existeix un esquema projectiu i llis $\mathcal{X}(B,\Gamma)/\mathrm{Spec}(\mathcal{O}_{K_\mathfrak{p}})$ de fibra genèrica $X(B,\Gamma)$.

Denotarem per $\widetilde{X}(B,\Gamma)$ la forma de $X(B,\Gamma)$ definida sobre $\mathcal{O}_{E_\mathfrak{P}}$ en què l'element de Frobenius sobre $\mathbb{F}_p$ actua com $\tau\circ(1,\dots,p^{-1},\dots,1)$, on τ designa l'acció de l'element de Frobenius sobre $X(B,\Gamma)$. L'esquema $\pi_0(\widetilde{\mathcal{X}}(B,\Gamma) = \mathrm{Nr}(\Gamma)\backslash K^*(\mathbb{A}_f)/K_+^*$ és ara un esquema constant. A partir de la norma reduïda, s'obté un morfisme

$$\widetilde{\mathcal{X}}(B,\Gamma) \to \pi_0(X(B,\Gamma)).$$

Procedirem tot seguit a l'anomenat *intercanvi d'invariants*. Definim àlgebres de quaternions $\mathrm{H} = \mathrm{H}_+, \mathrm{H}_-$ ramificades en p i tals que

$$\mathrm{H} \otimes_\mathbb{Q} \mathbb{R} = \mathrm{M}(2,\mathbb{R}) \times \mathrm{M}(2,\mathbb{R}), \quad \mathrm{H}_- \otimes_\mathbb{Q} \mathbb{R} = \mathbb{H} \times \mathbb{H}.$$

Prenem la resta de la ramificació en H i en H_- com en B.

Siguin $\Gamma_\pm \subseteq \mathrm{H}_\pm^*(\mathbb{A}_f)$ subgrups compactes i oberts. Suposem que són de la forma següent:

$$\Gamma_\pm = \Gamma^p\Gamma_{\pm,p}, \quad \Gamma^p \subseteq \mathrm{H}_\pm^*(\mathbb{A}_f^p) = \mathrm{B}^*(\mathbb{A}_f^p),$$

el mateix subgrup de més amunt, i $\Gamma_{\pm,p} \subseteq \mathrm{H}_\pm^*(\mathbb{Q}_p)$ un subgrup compacte maximal.

Considerem la projecció

$$\widetilde{\mathcal{X}}(\mathrm{H},\Gamma_+) \to \pi_0(\widetilde{\mathcal{X}}(\mathrm{H},\Gamma_+)) = \pi_0(\widetilde{\mathcal{X}}(B,\Gamma)).$$

Sigui C un component connex de $\widetilde{\mathcal{X}}(B,\Gamma)$ i sigui X el component connex corresponent de $\widetilde{\mathcal{X}}(\mathrm{H},\Gamma_+)$. Sigui $s = \mathrm{Spec}(\mathbb{F}_{q^4})$. La fibra especial X_s de X és unió de quatre superfícies reglades

$$X_s = \bigcup_{i\in\mathbb{Z}/4\mathbb{Z}} Y_i.$$

Les interseccions $C_i = Y_i \cap Y_{i+1}$ proporcionen corbes irreductibles totes isomorfes a una mateixa corba, C, definida sobre $\mathbb{F}_{q^4}$.

A partir de la norma reduïda, s'obté la factorització de Stein:

$$\Gamma_-\backslash \mathrm{H}^*_-(\mathbb{A}_f)/\mathrm{H}^*_- \to \mathrm{Nr}^0(\Gamma_+)\backslash K^*(\mathbb{A}_f)/K^*_+ = \pi_0(\mathcal{X}(B,\Gamma)).$$

En definir

$$k(C) := \#(\mathrm{Nr}^0)^{-1}(C),$$

s'obté que $Y_i \cap Y_{i+2} = (\mathrm{Nr}^0)^{-1}(C)$ és un esquema constant que posseeix k punts sobre $\mathbb{F}_{q^4}$.

La classe canònica de Y_i és $K_i = -2C_i + yL_i$, on L_i és una de les corbes racionals que defineixen la fibració de Y_i. Es té que

$$(L_i \cdot C_i) = 1, \quad (L_i \cdot C_{i-1}) = p,$$

amb la qual cosa, la fórmula d'adjunció permet calcular el gènere de la corba C:

$$g(C_i) = 1 + \frac{(C_i(C_i + K_i))}{2} = 1 + \frac{k}{p^2 - 1}.$$

El principal resultat de Tsfasman-Vlăduț-Zink és l'obtenció d'aquesta fórmula per al gènere.

10.6.1 Teorema. *Sigui C un component connex de la fibra especial torçada $\widetilde{\mathcal{X}}(B,\Gamma)_s$ de la corba de Shimura $X(B,\Gamma)$, on $s = \mathrm{Spec}(\mathbb{F}_{p^4})$. Aleshores,*

i) $g(C) = 1 + \dfrac{k(C)}{p^2 - 1}$.

ii) $\dfrac{g(C)}{\#C(\mathbb{F}_{p^4})} \leq \dfrac{1}{k(C)} + \dfrac{1}{p^2 - 1}$.

Per veure els avantatges del resultat anterior, considerem la recta de Goppa, d'equació

$$R = 1 - \gamma - \delta, \quad \gamma = g/n,$$

i l'anomenada corba de Gilbert-Varshamov, d'equació

$$R = 1 - \mathrm{H}(\delta),$$

on

$$\mathrm{H}(x) := x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$$

és la funció d'entropia.

Per Gilbert-Varshamov, se sap que existeixen codis lineals per als quals $1 - R \approx H(\delta)$.

10.6.2 Corol·lari. *Els codis de Goppa definits per corbes de Shimura milloren la fita de Gilbert-Varshamov.*

Atès que, en el nostre cas, $\gamma \approx (\sqrt{q}-1)^{-1}$, on $q = p^4$, $p \geq 3$, els codis lineals sobre $\mathbb{F}_{p^4}$ obtinguts per torçament de les fibres en $\mathfrak{P}$ de les corbes de Shimura milloren la fita de Varshamov-Gilbert en l'interval (δ_1, δ_2), on $\delta_1 < \delta_2$ designen les dues arrels de

$$\mathrm{H}(\delta) - \delta = (\sqrt{q}-1)^{-1}.$$

Bibliografia

[Del71] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23 année 1970-71, exp. 389, 139–172, Lecture Notes in Math., vol. 244, Springer, 1971, pp. 123–165.

[Elk98] N. Elkies, *Shimura curve computations*, Algorithmic number theory ANTS-3 (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, 1998, pp. 1–47.

[Iha81] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), num. 3, 721–724.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

[vdG01] G. van der Geer, *Curves over finite fields and codes*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, 2001, pp. 225–238.

[Zin82] Th. Zink, *Über die schlechte Reduktion einiger Shimuramannigfaltigkeiten*, Compositio Math. **45** (1982), num. 1, 15–107.

Bibliografia

[AAB01] M. Alsina, A. Arenas, P. Bayer (eds.), *Corbes de Shimura*, Notes del Seminari de teoria de nombres (UB-UAB-UPC), vol. 8, STNB, Barcelona, 2001.

[AB00a] A. Arenas, P. Bayer, *Complex multiplication points on modular curves*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 333–338.

[AB00b] A. Arenas, P. Bayer, *Heegner points on modular curves*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 323–332.

[AB04] M. Alsina, P. Bayer, *Quaternion orders, quadratic forms and Shimura curves*, CRM Monograph Series, vol. 22, American Mathematical Society, Providence, RI, 2004.

[AH91] D. Abramovich, J. Harris, *Abelian varieties and curves in* $W_d(C)$, Compositio Math. **78** (1991), num. 2, 227–238.

[AL70] A. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[Als97] M. Alsina, *Fundamental domains of the upper half plane by the action of matrix groups*, Meeting on matrix analysis and applications, Dept. Mat. Apl. I, Fac. Informática y Estadística, Univ. de Sevilla, 1997, pp. 10–17.

[Als99] M. Alsina, *Dominios fundamentales geométricos de* $\Gamma_0(p)$, VIII Encuentros de geometría computacional, Treballs d'informàtica i tecnologia, vol. 1, Univ. Jaume I, 1999, pp. 321–330.

[Als00a] M. Alsina, *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura*, Tesi doctoral, Publ. Universitat de Barcelona, 2000.

[Als00b] M. Alsina, *Dominios fundamentales modulares*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 309–322.

[Als05] M. Alsina, *Binary quadratic forms and eichler orders*, per aparèixer a J. Théor. Nombres Bordeaux **17** (2005), num. 1, 1–10, 23rd Journées Arithmetiques (Graz, 2003).

[Are03] A. Arenas, *On the traces of Hecke operators*, J. Number Theory **100** (2003), num. 2, 307–312.

[Bab01] S. Baba, *Shimura curve quotients with odd Jacobian*, J. Number Theory **87** (2001), 96–108.

[Bay02] P. Bayer, *Uniformization of certain Shimura curves*, Differential Galois Theory, Banach Center Publications, Polish Academy of Sciences **58** (2002), 13–26.

[BB66] W. Baily, A. Borel, *Compactification of arithmetic quotients of bounded symmetric domains*, Ann. of Math. **84** (1966), 442–528.

[BC91] J-F. Boutot, H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld*, Astérisque **196–197** (1991), 45–158, Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[BD96] M. Bertolini, H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), 413–456.

[BD97] M. Bertolini, H. Darmon, *A rigid analytic Gross-Zagier formula and arithmetic applications*, Ann. of Math. **146** (1997), num. 1, 111–147, With an appendix by Bas Edixhoven.

[BD98] M. Bertolini, H. Darmon, *Heegner points, p-adic L-functions and the Čerednik-Drinfeld uniformization*, Invent. Math. **131** (1998), num. 3, 453–491.

[BD99] M. Bertolini, H. Darmon, *p-adic periods, p-adic L-functions and the p-adic uniformization of Shimura curves*, Duke Math. J. **98** (1999), num. 2, 305–334.

[Bes93] A. Besser, *Universal families over Shimura curves*, Tesi doctoral, Tel-Aviv University, 1993.

[Bes95] A. Besser, *CM cycles over Shimura curves*, J. Algebraic Geom. **4** (1995), num. 4, 659–691.

[Bes98] A. Besser, *Elliptic fibrations of K3 surfaces and QM Kummer surfaces*, Math. Z. **228** (1998), num. 2, 283–308.

[BG97] P. Bayer, J. González, *On the Hasse-Witt invariants of modular curves*, Experimental Math. **6** (1997), num. 1, 57–76.

[BGR84] S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 261, Springer, Berlin, 1984, A systematic approach to rigid analytic geometry.

[BL] A. Besser, R. Livné, *Universal families of Kummer surfaces over Shimura curves*, in preparation.

[BL79] L. Breen, J-P. Labesse (eds.), *Variétés de Shimura et fonctions L*, Publications Mathématiques, vol. 6, Université Paris VII, 1979.

[BL84a] S. Bosch, W. Lütkebohmert, *Stable reduction and uniformization of abelian varieties. II*, Invent. Math. **78** (1984), num. 2, 257–297.

[BL84b] J. L. Brylinski, J-P Labesse, *Cohomologie d'intersection et fonctions L de certaines variétés de Shimura*, Ann. Scient. Ec. Norm. Sup. **17** (1984), 361–412.

[BL85] S. Bosch, W. Lütkebohmert, *Stable reduction and uniformization of abelian varieties. I*, Math. Ann. **270** (1985), num. 3, 349–379.

[BL91] S. Bosch, W. Lütkebohmert, *Degenerating abelian varieties*, Topology **30** (1991), num. 4, 653–698.

[BL92] C. Birkenhake, H. Lange, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer, 1992.

[Bor65] A. Borel, *Opérateurs de Hecke et fonctions zêta*, Séminaire Bourbaki, Vol. 9, exp.307, Soc. Math. France, 1965, pp. 441–463.

[Bou79] J-F. Boutot, *Le problème de modules en inégale caractéristique*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 43–62.

[Bra24] H. Brandt, *Der Kompositionsbegriff bei den quaternären quadratischen Formen*, Math. Ann. **91** (1924), 300–315.

[Bra28] H. Brandt, *Idealtheorie in Quaternionenalgebren*, Math. Ann. **99** (1928), 1–29.

[Bra43] H. Brandt, *Zur Zahlentheorie der Quaternionen*, Jahresbericht Deutsche Math. Verein **53** (1943), 23–57.

[Bre79] L. Breen, *Calcul des classes d'isogénie*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 63–72.

[Brz80] J. Brzezinski, *Arithmetical quadratic surfaces of genus* 0. I, Math. Scand. **46** (1980), 183–208.

[Brz82] J. Brzezinski, *A characterization of Gorenstein orders in quaternion algebras*, Math. Scand. **50** (1982), 19–24.

[Brz83] J. Brzezinski, *On orders in quaternion algebras*, Comm. in Algebra **11** (1983), 501–522.

[Brz84] J. Brzezinski, *Arithmetical quadratic surfaces of genus* 0. II, Math. Scand. **54** (1984), num. 2, 295–309.

[Brz90] J. Brzezinski, *On automorphisms of quaternion orders*, J. Reine Angew. Math. **403** (1990), 166–186.

[Brz95] J. Brzezinski, *Definite quaternion orders of class number one*, J. Théor. Nombres Bordeaux **7** (1995), 93–96.

[Brz97] J. Brzezinski, *A generalization of Eichler's trace formula*, Collect. Mathematica **48** (1997), num. 1-2, 53–61.

[BT65] A. Borel, J. Tits, *Groupes réductifs*, IHES Publ. Math. **27** (1965), 55–150.

[BT72] F. Bruhat, J. Tits, *Groupes réductifs sur un corps local*, IHES Publ. Math. **41** (1972), 5–251.

[BT92] P. Bayer, A. Travesa (eds.), *Corbes Modulars: Taules*, Notes del Seminari de teoria de nombres (UB-UAB-UPC), vol. 1, STNB, Barcelona, 1992.

[BT97] P. Bayer, A. Travesa (eds.), *Representacions automorfes de* GL(2), Notes del Seminari de teoria de nombres (UB-UAB-UPC), vol. 2, STNB, Barcelona, 1997.

[BT00a] P. Bayer, A. Travesa, *Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 347–356.

[BT00b] P. Bayer, A. Travesa, *Inmersiones de órdenes cuadráticos en el orden generado por* $\Gamma_0(N)$, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 357–376.

[BT00c] P. Bayer, A. Travesa, *órdenes matriciales generados por grupos de congruencia*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 339–346.

[Bui03] A. Buium, *Differential modular forms on Shimura curves. I*, Compositio Math. **139** (2003), num. 2, 197–237.

[Bui04] A. Buium, *Differential modular forms on Shimura curves. II. Serre operators*, Compos. Math. **140** (2004), num. 5, 1113–1134.

[Buz97] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), num. 3, 591–612.

[Car83] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, C. R. Acad. Sc. Paris **296** (1983), num. 13, 557–560.

[Car86a] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. **59** (1986), num. 2, 151–230.

[Car86b] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), num. 3, 409–468.

[Cas62] J. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[CDT99] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), num. 2, 521–567.

[Čer76] I. Čerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(k_w)$ *with compact quotients*, Math. USSR Sb. **29** (1976), num. 1, 55–78.

[CF86] T. Chinburg, E. Friedman, *The smallest arithmetic hyperbolic 3-orbifold*, Invent. Math. **86** (1986), 507–527.

[CF90] C. Chai, G. Faltings, *Degenerations of abelian varieties*, vol. 22, Ergeb. Math. Grenzgeb., num. 3, Springer, 1990.

[CF99] T. Chinburg, E. Friedman, *An embedding theorem for quaternion algebras*, J. London Math. Soc. **60** (1999), 33–44.

[CF00a] T. Chinburg, E. Friedman, *The finite subgroups of maximal arithmetic Kleinian groups*, Annals Inst. Fourier Grenoble **50** (2000), 1765–1798.

[CF00b] T. Chinburg, E. Friedman, *Hilbert symbols, class groups and quaternion algebras*, J. Théor. Nombres Bordeaux **12** (2000), 367–377.

[Cha74] J. Chalk, *Generators of fuchsian groups*, Tôhoku Math. Journ. **26** (1974), 203–218.

[Chu73] Y. Chuman, *Generators and relations of* $\Gamma_0(N)$, J. Math. Kyoto Univ. **13** (1973), num. 2, 381–390.

[CK74] J. Chalk, B. Kelly, *Generating sets for fuchsian groups*, Proc. Roy. Soc. Edinburgh Sect. A **72** (1974), 317–325.

[Cla03] P. Clark, *Local ang global points on moduly spaces of abelian surfaces with potential quaternionic multiplication*, Tesi doctoral, Harvard, 2003.

[Clo93] L. Clozel, *Nombre de points des variétés de Shimura sur un corps fini (d'après R. Kottwitz)*, Astérisque (1993), num. 216, 121–149, Séminaire Bourbaki 1992/93, vol. 4, Exp. 766.

[CM90] L. Clozel, J. Milne (eds.), *Automorphic forms, Shimura varieties, and L-functions. Vol. I-II*, Perspect. Math., vol. 10-11, Academic Press, 1990.

[Coh78] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Universitext, Springer, 1978.

[Coh95] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1995.

[Coh00] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer, 2000.

[Col87] R. Coleman, *Computing stable reductions*, Séminaire de Théorie des Nombres, Paris 1985–86, Progr. Math., vol. 71, Birkhäuser, Boston, MA, 1987, pp. 1–18.

[Con92] I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra **145** (1992), 463–467.

[Cor02] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495–523.

[Cre92] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992.

[CSS97] G. Cornell, J. H. Silverman, G. Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer, 1997, Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, 1995.

[CvdG92] C. Ciliberto, G. van der Geer, *Non-isomorphic curves of genus four with isomorphic (non-polarized) jacobians*, Contemp. Math. **162** (1992), 129–133.

[DDT94] H. Darmon, F. Diamond, R. Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.

[DDT97] H. Darmon, F. Diamond, R. Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Internat. Press, 1997, pp. 2–140.

[Del71] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23 année 1970-71, exp. 389, 139–172, Lecture Notes in Math., vol. 244, Springer, 1971, pp. 123–165.

[Del79] P. Deligne, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, Automorphic forms, representations and L-functions, part 2, (Proc. Sympos. Pure Math., XXXIII, 1977), AMS, 1979, pp. 247–289.

[Deu68] M. Deuring, *Algebren*, Springer, 1968.

[DI95] F. Diamond, J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[Dia89] F. Diamond, *On congruence modules associated to λ-adic forms*, Compositio Math. **71** (1989), num. 1, 49–83.

[Dia91] F. Diamond, *Congruence primes for cusp forms of weight $k \geq 2$*, Astérisque (1991), num. 196-197, 6, 205–213 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Dia96] F. Diamond, *On deformation rings and Hecke rings*, Annals of Math. **144** (1996), num. 1, 137–166.

[Dia97a] F. Diamond, *Congruences between modular forms: raising the level and dropping Euler factors*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), 11143–11146, Elliptic curves and modular forms (Washington, DC, 1996).

[Dia97b] F. Diamond, *An extension of Wiles' results*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, 1997, pp. 475–489.

[Dia97c] F. Diamond, *The refined conjecture of Serre*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Internat. Press, 1997, pp. 22–37.

[Dia97d] F. Diamond, *The Taylor-Wiles construction and multiplicity one*, Invent. Math. **128** (1997), num. 2, 379–391.

[Dia98] F. Diamond, *On the Hecke action on the cohomology of Hilbert-Blumenthal surfaces*, Number theory (Tiruchirapalli, 1996), Amer. Math. Soc., 1998, pp. 71–83.

[Die03] L. Dieulefait, *Modularity of abelian surfaces with quaternionic multiplication*, Math. Res. Lett. **10** (2003), num. 2-3, 145–150.

[DK95] F. Diamond, K. Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. **2** (1995), 299–304.

[DK97] F. Diamond, K. Kramer, *Appendix: classification of $\overline{\rho}_{E,l}$ by the j-invariant of E*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, 1997, pp. 491–498.

[DN67] K. Doi, H. Naganuma, *On the algebraic curves uniformized by arithmetical automorphic function*, Ann. of Math. **86** (1967), 449–460.

[DP98] W. Dicks, J. Porti, *Expressing a number as the sum of two coprime squares*, Collect. Math. **49** (1998), num. 2-3, 283–291.

[DR73] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Antwerp, 1972), Lecture Notes in Math., vol. 349, Springer, 1973, pp. 143–316.

[DR97] F. Diamond, K. Ribet, *l-adic modular deformations and Wiles's "main conjecture"*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, 1997, pp. 357–371.

[DR04] L. Dieulefait, V. Rotger, *The arithmetic of QM-abelian surfaces through their Galois representations*, J. Algebra **281** (2004), num. 1, 124–143.

[Dri76] V. G. Drinfeld, *Coverings of p-adic symmetric regions*, Funct. Anal. Appl. **10** (1976), 107–115.

[DT94a] F. Diamond, R. Taylor, *Lifting modular mod l representations*, Duke Math. J. **74** (1994), num. 2, 253–269.

[DT94b] F. Diamond, R. Taylor, *Nonoptimal levels of mod l modular representations*, Invent. Math. **115** (1994), num. 3, 435–462.

[Edi95] B. Edixhoven, *On the prime-to-p part of the groups of connected components of Néron models*, Compositio Math. **97** (1995), num. 1-2, 29–49, Special issue in honour of Frans Oort.

[Eic37] M. Eichler, *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, J. Reine Angew. Math. **176** (1937), 192–202.

[Eic38] M. Eichler, *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Z. **43** (1938), 481–494.

[Eic55a] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156–171.

[Eic55b] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151.

[Eic57] M. Eichler, *Eine Verallgemeinerung der Abelschen Integrale*, Math. Z. **67** (1957), 267–298.

[Eic58] M. Eichler, *Quadratische Formen und Modulfunktionen*, Acta Arith. **4** (1958), 217–239.

[Elk98] N. Elkies, *Shimura curve computations*, Algorithmic number theory ANTS-3 (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, 1998, pp. 1–47.

[ELL96] B. Edixhoven, Q. Liu, D. Lorenzini, *The p-part of the group of components of a Néron model*, J. Algebraic Geom. **5** (1996), num. 4, 801–813.

[EY03] B. Edixhoven, A. Yafaev, *Subvarieties of Shimura varieties*, Ann. of Math. **157** (2003), num. 2, 621–645.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), num. 3, 349–366.

[FC90] G. Faltings, C-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer, Berlin, 1990, With an appendix by David Mumford.

[FJ95] G. Faltings, B. Jordan, *Crystalline cohomology and* GL(2, $\mathbb{Q}$), Israel J. Math. **90** (1995), num. 1-3, 1–66.

[FK97] R. Fricke, F. Klein, *Vorlesungen über die Theorie der automorphen Funktionen*, Leipizig, 1897, Bibliotheca Mathematica Teubneriana, Johnson Reprint Corp., New York; B. G. Teubner Verlagsgesellschaft, Stuttgart 1965.

[Fly90a] E. Flynn, *The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Camb. Phil. Soc. **107** (1990), 425–441.

[Fly90b] E. Flynn, *Large rational torsion on abelian varieties*, Journal of Number Theory **36** (1990), num. 3, 257–265.

[Fly91] E. Flynn, *Sequences of rational torsions on abelian varieties*, Invent. Math. **106** (1991), 433–442.

[Fly93] E. Flynn, *The group law on the Jacobian of a curve of genus 2*, J. Reine Angew. Math. **439** (1993), 45–69.

[Fly94] E. Flynn, *Descent via isogeny in dimension 2*, Acta Arith. **66** (1994), num. 1, 23–43.

[For51] L. Ford, *Automorphic functions*, 2na ed., Chelsea, 1951.

[Fri93] R. Fricke, *Zur gruppentheoretischen Grundlegung der automorphen Functionen*, Math. Ann. **42** (1893), 564–597.

[Gau01] C. F. Gauss, *Disquisicions aritmètiques*, Gerh. Fleischer, Lipsiae, 1801, Traducció a cura de G. Pascual, Inst. Estudis Catalans, Soc. Cat. Mat,1996.

[Gek95] E. Gekeler, *Improper Eisenstein series on Bruhat-Tits trees*, Manuscripta Math. **86** (1995), num. 3, 367–391.

[Ger79] P. Gerardin, *Algèbres de quaternions*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 145–155.

[GGR] J. González, J. Guardia, V. Rotger, *Abelian surfaces of* GL_2*-type as jacobians of curves*, per aparèixer a Acta Arithmetica.

[GH81] B. Gross, J. Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), num. 2, 157–182.

[Gir79] J. Giraud, *Modules de variétés abeliennes et variétés de Shimura*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 21–42.

[GKZ87] B. Gross, W. Kohnen, D. Zagier, *Heegner points and derivatives of L-series II*, Math. Ann. **278** (1987), 497–562.

[GL00] J. Guàrdia, J. C. Lario (eds.), *Varietats abelianes amb multiplicació complexa*, Notes del Seminari de teoria de nombres (UB-UAB-UPC), vol. 6, STNB, Barcelona, 2000.

[Gon91] J. González, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier (Grenoble) **41** (1991), 779–795.

[GR04] J. González, V. Rotger, *Equations of Shimura curves of genus two*, Int. Math. Res. Not. (2004), num. 14, 661–674.

[Gra02] H. Granath, *On quaternionic Shimura surfaces*, Tesi doctoral, Chalmers Goteborg University, 2002.

[Gro82] B. Gross, *Heegner points on* $X_0(11)$, Séminaire de Théorie des Nombres 1981-82, Univ. Bordeaux I, 1982.

[GvdP80] L. Gerritzen, M. van der Put, *Schottky groups and Mumford curves*, Lecture Notes in Math., vol. 817, Springer, Berlin, 1980.

[GZ85] B. Gross, D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

[GZ86] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[Hay68] T. Hayashida, *Class number associated with the product of an elliptic curve with itself*, J. Math. Soc. Japan **20** (1968), 26–43.

[Hec40] E. Hecke, *Analytische Arithmetik der positiven quadratischen Formen*, Danske Vid. Selsk. Math.-Fys. Medd. **17** (1940), num. 12, 1–134.

[HH90] K. Horie, M. Horie, *CM-fields and exponents of their ideal class groups*, Acta Arith. **55** (1990), 157–170.

[HHM99] Y. Hasegawa, K. Hashimoto, F. Momose, *Modular conjecture for* $\mathbf{Q}$*-curves and QM-surfaces*, International J. Math. **10** (1999), 1011–1036.

[Hij74] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(n)$, J. Math. Soc. Japan. **26** (1974), num. 1, 56–82.

[HL89] K. Harada, M-L. Lang, *Some elliptic curves arising from the Leech lattice*, J. Algebra **125** (1989), 298–310.

[HM95] K. Hashimoto, N. Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of*

QM-curves of genus two, Tohoku Math. J. **47** (1995), num. 2, 271–296.

[HN65] T. Hayashida, M. Nishi, *Existence of curves of genus two on a product of two elliptic cuves*, J. Math. Soc. Japan **17** (1965), 1–16.

[How00] E. W. Howe, *Plane quartics with jacobians isomorphic to a hyperelliptic jacobian*, Proc. Amer. Math. Soc. **129** (2000), 1647–1657.

[HPS89] H. Hijikata, A. Pizer, T. Shemanske, *Orders in quaternion algebras*, J. Reine Angew. Math. **394** (1989), 59–106.

[HS36] H. Hasse, O. Schilling, *Die Normen aus einer normalen divisionsalgebra*, J. Reine Angew. Math. **174** (1936), 248–252.

[HS91] J. Harris, J. H. Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), 347–356.

[HT99] K. Hashimoto, H. Tsunogai, *On the Sato-Tate conjecture for QM-curves of genus two*, Math. Computation **68** (1999), 1649–1662.

[HT01] M. Harris, R. Taylor, *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, vol. 151, Princeton University Press, 2001.

[Hul35] R. Hull, *The maximal orders in rational cyclic algebras of odd prime degree*, Trans. AMS. **38** (1935), 515–530.

[Hul36] R. Hull, *The maximal orders of generalized quaternion division algebras*, Trans. AMS. **40** (1936), 1–11.

[Hul39] R. Hull, *On the units of indefinite quaternion algebras*, Amer. Journ. of Math. **61** (1939), 365–374.

[Hum93] G. Humbert, *Théorie générale des surfaces hyperelliptiques*, J. Math. Sér. **IV, 9** (1893), 29–170 and 361–475.

[Hum19] M.G. Humbert, *Sur la formation du domaine fondamental d'un groupe automorphe*, C.R. Acad. Sci. **169** (1919), 205–211.

[HZ76] F. Hirzebruch, D. Zagier, *Intersection Numbers of Curves on Hilbert Modular Surfaces and modular of Nebentypus*, Invent. Math. **36** (1976), 57–113.

[Ibu82] T. Ibukiyama, *On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings*, Nagoya Math. J. **88** (1982), 181–195.

[Igu60] J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. **72** (1960), num. 3, 612–649.

[Iha68a] Y. Ihara, *The congruence monodromy problem*, J. Math. Soc. Japan **20** (1968), 107–121.

[Iha68b] Y. Ihara, *On congruence monodromy problems. Vol. 1*, Lecture Notes, num. 1, Department of Mathematics, University of Tokyo, Tokyo, 1968.

[Iha69] Y. Ihara, *On congruence monodromy problems. Vol. 2*, Lecture Notes, num. 2, Department of Mathematics, University of Tokyo, Tokyo, 1969.

[Iha74] Y. Ihara, *Schwarzian equations*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), 97–118.

[Iha75] Y. Ihara, *Some fundamental groups in the arithmetic of algebraic curves over finite fields*, Proc. Nat. Acad. Sci. U.S.A. **72** (1975), 3281–3284.

[Iha79a] Y. Ihara, *Automorphic forms, representations and l-functions*, Proceedings of Symposia in Pure Mathematics, num. XXXIII, cap. Congruence relations and Shimura curves, pp. 291–311, Amer. Math. Soc., 1979.

[Iha79b] Y. Ihara, *Congruence relations and Shimura curves. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), num. 3, 301–361.

[Iha81] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), num. 3, 721–724.

[Iha99] Y. Ihara, *Shimura curves over finite fields and their rational points*, Applications of curves over finite fields (Seattle, WA, 1997), Contemp. Math., vol. 245, Amer. Math. Soc., Providence, RI, 1999, pp. 15–23.

[IKO86] T. Ibukiyama, T. Katsura, F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127–152.

[IM75] Y. Ihara, H. Miki, *Criteria related to potential unramifiedness and reduction of unramified coverings of curves*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **22** (1975), num. 2, 237–254.

[Ish73] H. Ishikawa, *On the trace formula for Hecke operators*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 217–238.

[Ish75] N. Ishii, *An application of the Fricke formula for quaternion groups*, Mathematica Japonicae **20** (1975), 171–177.

[Jar04] F. Jarvis, *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math. **213** (2004), num. 2, 267–280.

[Ji98] S. Ji, *Analogs of $\Delta(z)$ for triangular Shimura curves*, Acta Arith. **85** (1998), num. 3, 97–108.

[JL85] B. Jordan, R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985), num. 2, 235–248.

[JL86] B. Jordan, R. Livné, *On the Néron model of jacobians of Shimura curves*, Compositio Math. **60** (1986), num. 2, 227–236.

[JL87] B. Jordan, R. Livné, *Divisor classes on Shimura curves rational over local fields*, J. Reine Angew. Math. **378** (1987), 46–52.

[JL89] B. Jordan, R. Livné, *Conjecture epsilon for weight $k > 2$*, Bull. Amer. Math. Soc. **21** (1989), num. 1, 51–56.

[JL99] B. Jordan, R. Livné, *On Atkin-Lehner quotients of Shimura curves*, Bull. London Math. Soc. **31** (1999), 681–685.

[JLV03] Bruce W. Jordan, Ron Livné, Yakov Varshavsky, *Local points of twisted Mumford quotients and Shimura curves*, Math. Ann. **327** (2003), num. 3, 409–428.

[JM94] B. Jordan, D. Morrison, *On the Néron models of abelian surfaces with quaternionic multiplication*, J. Reine Angew. Math. **447** (1994), 1–22.

[Joh97] S. Johansson, *Traces in arithmetic fuchsian groups*, J. of Number Theory **66** (1997), 251–270.

[Joh98] S. Johansson, *Genera of arithmetic Fuchsian groups*, Acta Arith. **86** (1998), num. 2, 171–191.

[Jon67] B. Jones, *The arithmetic theory of quadratic forms*, The mathematical association of America, 1967.

[Jor81] B. Jordan, *On the diophantine arithmetic of Shimura curves*, Tesi doctoral, Harvard University, 1981.

[Jor84] B. Jordan, *p-adic points on Shimura curves*, Séminaire de théorie des nombres de Paris 1982-83 (M.J. Bertin, C. Goldstein, eds.), Progress in Math., vol. 51, Birkhäuser, 1984, pp. 135–142.

[Jor86] B. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[JY82] C. Jensen, N. Yui, *Polynomials with D_p as Galois Group*, J. of Number Theory **15** (1982), num. 3, 347–375.

[JY88] C. Jensen, N. Yui, *Quaternion extensions*, Algebraic geometry and commutative algebra, Vol. I, Kinokuniya, Tokyo, 1988, pp. 155–182.

[Kam90] S. Kamienny, *Points on Shimura curves over fields of even degree*, Math. Ann. **286** (1990), num. 3, 731–734.

[Kap69] I. Kaplansky, *Submodules of quaternion algebras*, Proc. London Math. Soc. **19** (1969), num. 3, 219–232.

[Kas04] P. Kassaei, *P-adic modular forms over Shimura curves over totally real fields*, Compos. Math. **140** (2004), num. 2, 359–395.

[Kid96] M. Kida, *On a characterization of Shimura's elliptic curve over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. **77** (1996), num. 2, 157–171.

[Kit93] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge Tracts in Mathematics, num. 106, Cambrigde University Press, 1993.

[KL01] Ch. Khare, S. Ling, *Maps between Jacobians of Shimura curves and congruence kernels*, Math. Ann. **319** (2001), num. 2, 383–394.

[KM85] N. M. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[KM88] M. Kenku, F. Momose, *Automorphisms groups of the modular curves* $X_0(N)$, Compositio Math. **65** (1988), 51–80.

[Kot79] R. Kottwitz, *Combinatorics and Shimura varieties* mod p *(based on lectures by Langlands)*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 185–192.

[Kot92a] R. Kottwitz, *On the* λ*-adic representations associated to some simple Shimura varieties*, Invent. Math. **108** (1992), num. 3, 653–665.

[Kot92b] R. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), num. 2, 373–444.

[KR00] S. Kudla, M. Rapoport, *Height pairings on Shimura curves and p-adic uniformization*, Invent. Math. **142** (2000), num. 1, 153–223.

[Kud97] S. Kudla, *Central derivatives of Eisenstein series and height pairings*, Ann. of Math. **146** (1997), 545–646.

[Kuh88] R. M. Kuhn, *Curves of genus 2 with split jacobian*, Trans. Amer. Math. Soc. **307** (1988), 41–49.

[Kün00] K. Künnemann, *Uniformization of Shimura curves by the p-adic upper half plane*, Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., vol. 187, Birkhäuser, Basel, 2000, pp. 121–128.

[Kur79] A. Kurihara, *On some exemples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Tokyo **25** (1979), num. 3, 277–300.

[Kur94] A. Kurihara, *On p-adic Poincaré series and Shimura curves*, Internat. J. Math. **5** (1994), 747–763.

[KV03] D. Kohel, H. Verrill, *Fundamental domains for Shimura curves*, J. Théor. Nombres Bordeaux **15** (2003), num. 1, 205–222, Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[KY90] E. Kaltofen, N. Yui, *Number Theory, New-York Seminar 1989-1990*, cap. Explicit Construction of the Hilbert class fields of imaginary quadratic . . ., pp. 149–202, Springer-Verlag, 1990.

[KY91] E. Kaltofen, N. Yui, *Explicit Construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction*, J. of Number Theory (1991), 149–202.

[Lab79a] J-P. Labesse, *Fonction zêta locale et fonctions L de formes automorphes*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 83–130.

[Lab79b] J-P. Labesse, *Introduction aux fonctions L des variétés de Shimura*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 11–20.

[Lan76] R. Langlands, *Some contemporary problems with origins in the Jugendtraum*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, R. I., 1976, pp. 401–418.

[Lan77] R. Langlands, *Shimura varieties and the Selberg trace Formula*, Canad. J. Math. **29** (1977), num. 5, 1292–1299.

[Lan79a] R. Langlands, *Automorphic representations, Shimura varieties, and motives. Ein Märchen*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., 1979, pp. 205–246.

[Lan79b] R. Langlands, *On the zeta function of some simple Shimura varieties*, Canad. J. Math. **31** (1979), 1121–1216.

[Lan79c] R. Langlands, *Sur la mauvaise réduction d'une variété de Shimura*, Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Vol. III, Astérisque, vol. 65, Soc. Math. France, Paris, 1979, pp. 125–154.

[Lan83] S. Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften, vol. 255, Springer, 1983.

[Lan88] H. Lange, *Abelian varieties with several principal polarizations*, Duke Math. J. **55** (1988), 617–628.

[Lat36] C. Latimer, *The quadratic subfields of a generalized quaternion algebra*, Duke Math. J. **2** (1936), num. 2, 681–684.

[Lat37] C. Latimer, *The classes of integral sets in a quaternion algebra*, Duke Math. J. **3** (1937), 237–247.

[Lee95] M. Lee, *Twisted torus bundles over arithmetic varieties*, Proc. Amer. Math. Soc. **123** (1995), num. 7, 2251–2259.

[Leh64] J. Lehner, *Discontinuous groups and automorphic functions*, Mathematical Surveys n.8, num. 8, American Mathematical Society, 1964.

[Leh92] J. Lehman, *Levels of positive definite ternary quadratic forms*, Math. of Computation **58** (1992), 399–417.

[Lin93] S. Ling, *Shimura subgroups of jacobians of Shimura curves*, Proceedings of the Amer. Math. Soc. **118** (1993), num. 2, 385–390.

[Liu91] Q. Liu, *La réduction stable des courbes de genre* 2 *et le schéma de modules* $\overline{\mathcal{M}}_2$, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), num. 2, 95–98.

[Llo00] P. Llorente, *Correspondencia entre formas ternarias enteras y órdenes cuaterniónicos*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), num. 3, 397–416.

[LN64] J. Lehner, M. Newman, *Weierstrass points of* $\Gamma_0(N)$, Ann. of Math. **79** (1964), 360–368.

[LO91] S. Ling, J. Oesterle, *Courbes modulaires et courbes de Shimura*, Astérisque, vol. 196-197, cap. The Shimura subgroup of $J_0(N)$, pp. 45–158, Soc. Math. de France, 1991.

[Log01] D. Logachev, *Action of Hecke correspondences on Heegner curves on a Siegel threefold*, J. Algebra **236** (2001), num. 1, 307–348.

[LR87] R. Langlands, M. Rapoport, *Shimuravarietäten und Gerben*, J. Reine Angew. Math. **378** (1987), 113–220.

[Lüt90] W. Lütkebohmert, *Formal-algebraic and rigid-analytic geometry*, Math. Ann. **286** (1990), 341–371.

[Mag74] W. Magnus, *Noneuclidean tesselations and their groups*, Academic Press, 1974.

[Man81] Y. Manin, *What is the maximum number of points on a curve over* F_2*?*, Journal of Faculty of Science University of Tokyo **28** (1981), 915–720.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), num. 47, 33–186 (1978).

[Maz78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[McC98] J. McConnell, *Division algebras—beyond the quaternions*, Amer. Math. Monthly **105** (1998), num. 2, 154–162.

[Mes91] J-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules, effective methods in algebraic geometry*, Progr. Math. **94** (1991), 313–334.

[Mic81a] J-F. Michon, *Courbes de Shimura de genre 1*, Séminaire Delange-Pisot-Poitou (1981), 1.

[Mic81b] J-F. Michon, *Courbes de Shimura hyperelliptiques*, Bull. Soc. Math. France **109** (1981), 217–225.

[Mic84a] J-F. Michon, *Codes de Goppa*, Séminaire de Théorie des Nombres de Talence, 1983–1984, Univ. Bordeaux I, 1984, pp. 7.1–7.17.

[Mic84b] J-F. Michon, *Courbes de Shimura*, Séminaire de Théorie des Nombres de Paris 1982-83 (M.J. Bertin, C. Goldstein, eds.), Progr. Math., num. 51, Birkhäuser, 1984, pp. 185–197.

[Mil79a] J. Milne, *Etude d'une classe d'isogénie*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 73–81.

[Mil79b] J. Milne, *Points on Shimura varieties mod p*, Automorphic forms, representations and L-functions, Proc. XXXII Sympos. Pure Math. (1977), Amer. Math. Soc., 1979, pp. 165–184.

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry, Springer, 1986, pp. 167–212.

[Mil92] J. Milne, *The points on a Shimura variety modulo a prime of good reduction*, The zeta functions of Picard modular surfaces, Univ. Montréal, 1992, pp. 151–253.

[Miy71] T. Miyake, *On automorphic forms on* GL_2 *and Hecke operators*, Ann. of Math. **94** (1971), 174–189.

[Miy76] T. Miyake, *Modular forms*, Springer, Berlin, 1976.

[Mor70] Y. Morita, *Ihara's conjectures and moduli space of abelian varieties*, Thesis, Univ. Tokyo, 1970.

[Mor80] Y. Morita, *Classification of a family of abelian varieties parametrized by reduction modulo* $\mathfrak{p}$ *of a Shimura curve*, Proc. Japan Acad. Ser. A Math. Sci. **56** (1980), num. 7, 338–341.

[Mor81] Y. Morita, *Reduction mod* $\mathfrak{p}$ *of Shimura curves*, Hokkaido Math. J. **10** (1981), num. 2, 209–238.

[Mor92] A. Mori, *Explicit period matrices of abelian surfaces with quaternionic multiplications*, Boll. Un. Mat. Ital. A (7) **6** (1992), num. 2, 197–208.

[Mor95] A. Mori, *Power series expansions of modular forms at CM points*, Rend. Sem. Mat. Univ. Pol. Torino **53** (1995), 361–374.

[MR77] B. Mazur, M. Rapoport, *Behavior of the Néron model of the jacobian of* $X_0(n)$ *at bad primes*, Publ. Math. I.H.E.S. **47** (1977), 173–186.

[MR91] B. Mazur, K. Ribet, *Courbes modulaires et courbes de Shimura*, Astérisque, vol. 196-197, cap. Two-dimensional representations in the arithmetic of modular curves, pp. 215–255, Soc. Math. de France, 1991.

[Mum70] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research, Bombay, Oxford University Press, 1970.

[Mum72] D. Mumford, *An analytic construction of degenerating curves over complete local rings*, Compositio Math. **24** (1972), 129–174.

[Neu92] J. Neukirch, *Algebraische Zalentheorie*, Springer, 1992.

[Neu99] J. Neukirch, *Algebraic number theory*, Grundl. math. Wiss., 1999.

[NN81] M. S. Narasimhan, M. V. Nori, *Polarizations on an abelian variety*, Proc. Indian Acad. Sci. Math. Sci. **90** (1981), 125–128.

[Noo01] R. Noot, *On Mumford's families of abelian varieties*, J. Pure Appl. Algebra **157** (2001), 87–106.

[Oes88] J. Oesterlé, *Nouvelles approches du "théorème"de Fermat*, Séminaire Bourbaki 40é année 1987-88, Astérisque, num. 161-162, Société mathematique de France, 1988, pp. 165–186.

[Ogg69] A. Ogg, *Modular forms and Dirichlet series*, Mathematics Lecture Note Series, W.A. Benjamin, Inc., 1969.

[Ogg71] A. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. **12** (1971), 105–111.

[Ogg74] A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. math. France **102** (1974), 449–462.

[Ogg77] A. Ogg, *Über die Automorphismengruppe von* $X_0(N)$, Math. Ann. **228** (1977), 279–292.

[Ogg78] A. Ogg, *On the Weierstrass points of* $X_0(N)$, Illinois J. Math. **22** (1978), num. 1, 31–35.

[Ogg83] A. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, 1983, pp. 277–307.

[Ogg85] A. Ogg, *Mauvaise réduction des courbes de Shimura*, Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser, 1985, pp. 199–217.

[Oht74] M. Ohta, *On ℓ-adic representations of Galois groups obtained from certain two dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo **21** (1974), 299–308.

[Oht82] M. Ohta, *On l-adic representations attached to automorphic forms*, Japan. J. Math. (N.S.) **8** (1982), num. 1, 1–47.

[O'M00] O. O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer, Berlin, 2000, Reprint of the 1973 edition.

[Pa89] *PARI programming package*, anonymous ftp from the site megrez.ceremab.u-bordeaux.fr, 1989.

[Pet69] M. Peters, *Ternäre and quaternäre quadratische formen und quaternionenalgebren*, Acta Arithmetica (1969), 329–365.

[Pie82] R. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer, New York, 1982, Studies in the History of Modern Science, 9.

[Piz73] A. Pizer, *Type numbers of Eichler orders*, J. Reine Angew. Math. **264** (1973), 76–102.

[Piz76a] A. Pizer, *On the arithmetic of quaternion algebras I*, Acta Arith. **31** (1976), num. 1, 61–89.

[Piz76b] A. Pizer, *On the arithmetic of quaternion algebras II*, J. Math. Soc. Japan **28** (1976), num. 4, 676–688.

[Piz76c] A. Pizer, *The representability of modular forms by theta series*, J. Math. Soc. Japan **28** (1976), 689–698.

[Piz80] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)^*$, J. Algebra **64** (1980), 340–390.

[Poi87] H. Poincaré, *Les fonctions fuchsiennes et l'arithmétique*, J. Math. **4** (1887), 405–464, en *Ouvres Completes* vol.II.

[Poi95] H. Poincaré, *Œuvres. Tome II*, Les Grands Classiques Gauthier-Villars., Éditions Jacques Gabay, 1995.

[Pol60] B. Pollack, *The equation* $\bar{t}at = b$ *in a quaternion algebra*, Duke Math. J. **27** (1960), 261–271.

[Pra95] D. Prasad, *Ribet's theorem: Shimura-Taniyama-Weil implies Fermat*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., 1995, pp. 155–177.

[PS56] I. Pyatetskii-Shapiro, *The classification of modular groups*, Dokl. Akad. Nauk SSSR **110** (1956), 19–22.

[PS99] B. Poonen, M. Stoll, *On the Cassels-Tate pairing for abelian varieties*, Ann. of Math. **150** (1999), 1109–1149.

[Rap88] M. Rapoport, *On the local zeta function of quaternionic Shimura varieties with bad reduction*, Math. Ann. **279** (1988), 673–697.

[Rap90] M. Rapoport, *On the bad reduction of Shimura varieties*, Automorphic forms, Shimura varieties, and L-functions, Vol. II (Ann Arbor, MI, 1988), Perspect. Math., vol. 11, Academic Press, 1990, pp. 253–321.

[Ray70] M. Raynaud, *Specialisation du foncteur de Picard*, Inst. Hautes Etudes Sci. Publ. Math. **38** (1970), 27–76.

[Ray74] M. Raynaud, *Geometrie analytique rigide d'apres Tate, Kiehl, ...*, Bull. Soc. math. France, Mémoire **39-40** (1974), 319–327.

[RBJ91] K. Ribet, N. Boston, H. Lenstra Jr., *Quotients of group rings arising from two-dimensional representations*, C.R. Acad. Sci. Paris **312** (1991), 323–328.

[Rei52] H. Reimann, *The semi-simple zeta function of quaternionic Shimura varieties*, Lecture Notes in Math., vol. 1657, Springer, 1952.

[Rei70] I. Reiner, *Survey of integral representation theory*, Bull. Amer. Math. Soc. **76** (1970), 159–227.

[Rei75] I. Reiner, *Maximal Orders*, Academic Press, 1975.

[Rha80] G. Rham, *Sur les polygones générateurs de groupes funchsiens*, C.R. Acad. Sci. Paris **291** (1980), num. 2, 121–123.

[RHD70] K. Roggenkamp, Huber-Dyson, *Lattices over Orders I*, Lecture Notes in Math., num. 115, Springer, 1970.

[Rib75] K. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. of Math. **101** (1975), 555–562.

[Rib80] K. Ribet, *Sur les variétés abéliennes à multiplications réelles*, C. R. Acad. Sci. Paris Sér. A-B **291** (1980), num. 2, 121–123.

[Rib88] K. Ribet, *On the component groups and the Shimura subgroup of* $J_0(N)$, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Univ. Bordeaux I, 1988, pp. Exp. No. 6, 10.

[Rib89] K. Ribet, *Bimodules and abelian surfaces*, Advanced Studies in Pure Mathematics **17** (1989), 359–407.

[Rib90a] K. Ribet, *Multiplicities of Galois representations in jacobians of Shimura curves*, Israel Mth. Conf. Proc. **3** (1990), 221–236.

[Rib90b] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), num. 2, 431–476.

[Rib91] K. Ribet, *Lowering the levels of modular representations without multiplicity one*, Duke Math. J. **62** (1991), num. 2, 15–19.

[Rib94a] K. Ribet, *Fields of definition of abelian varieties with real multiplication*, Contemp. Math. **174** (1994), 107–118.

[Rib94b] K. Ribet, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Motives (Seattle, WA, 1991), Amer. Math. Soc., 1994, pp. 639–676.

[Rib95] K. Ribet, *Galois representations and modular forms*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), num. 4, 375–402.

[Rob89] D. Roberts, *Shimura curves analogous to* $X_0(N)$, Tesi doctoral, Harvard University, 1989.

[Rog70] K. Roggenkamp, *Lattices over Orders II*, Lecture Notes in Math., num. 142, Springer, 1970.

[Rot02] V. Rotger, *On the group of automorphisms of Shimura curves and applications*, Compositio Math. **132** (2002), num. 2, 229–241.

[Rot03] V. Rotger, *Quaternions, polarization and class numbers*, J. Reine Angew. Math. **561** (2003), 177–197.

[Rot04a] Victor Rotger, *Modular Shimura varieties and forgetful maps*, Trans. Amer. Math. Soc. **356** (2004), num. 4, 1535–1550.

[Rot04b] Victor Rotger, *Shimura curves embedded in Igusa's threefold*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, 2004, pp. 263–276.

[RT97] K. Ribet, S. Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), 11110–11114, Elliptic curves and modular forms (Washington, DC, 1996).

[Rüc90] H. Rück, *Abelian surfaces and jacobian varieties over finite fields*, Compositio Math. **76** (1990), 351–366.

[Run99] B. Runge, *Endomorphism rings of abelian surfaces and projective models of their moduli spaces*, Tohoku Math. J. (2) **51** (1999), num. 3, 283–303.

[RYZ82] G. Roland, N. Yui, D. Zagier, *A parametric family of quintic plynomials with Galois group D_5*, Journal of Number Theory **15** (1982), num. 1, 137–142.

[RZ82] M. Rapoport, Th. Zink, *über die lokale zetafuncktion von Shimuravarietäten*, Invent. Math. **68** (1982), 21–101.

[RZ96] M. Rapoport, Th. Zink, *Period spaces for p-divisible groups*, Annals of Mathematics Studies, vol. 141, Princeton University Press, 1996.

[Sai72] H. Saito, *On Eichler's trace formula*, J. Math. Soc. Japan **24** (1972), 333–340.

[Sch59] A. Schinzel, *Sur les sommes de trois carrés*, Bull. Acad. Polonaise Sc. **VII 6** (1959), 307–310.

[Sch98] P. Schmutz, *Geometry of Riemann surfaces based on closed geodesics*, Bulletin of the Amer. Math. Soc. **35** (1998), num. 3, 193–214.

[Sch00] T. Schmechta, *Mumford-Tate curves*, Courbes semi-stables et groupe fondamental en géométrie algébrique

(Luminy, 1998), Progr. Math., vol. 187, Birkhäuser, Basel, 2000, pp. 111–119.

[Sel56] A. Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc. **20** (1956), 47–87.

[Ser68] J-P. Serre, *Corps locaux*, Hermann Paris, 1968.

[Ser73] J-P. Serre, *A course in arithmetic*, Graduate texts in Mathematics, num. 7, Springer-Verlag, 1973.

[Ser77] J-P. Serre, *Arbres, Amalgames,* SL_2, Astérisque, num. 46, Société mathematique de France, 1977.

[Ser79] J-P. Serre, *Local fields*, Graduate texts in Mathematics, num. 67, Springer, 1979.

[Ser83a] J-P. Serre, *Nombres des points des courbes algébriques sur* f_q, Journal Séminari de Théorie de Bourdeaux **22** (1983), 1–8.

[Ser83b] J-P. Serre, *Sur le nombre des points rationals d'une courbe algébrique sur un corps fini.*, C.R. Acad. Sc. Paris **296** (1983), 397–402.

[Ser85] C. Series, *The modular surface and continued fractions*, J. London Math. Soc. **31** (1985), 69–80.

[Ser87] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), num. 1, 179–230, *Oeuvres*, vol. IV, Springer, 2000.

[Ser00] J-P. Serre, *Œuvres. Collected papers. IV*, Springer, Berlin, 2000, 1985–1998.

[Shi61] G. Shimura, *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), num. 3, 275–331.

[Shi63a] H. Shimizu, *On discontinuous groups operating on the product of the upper half planes*, Ann. of Math. **77** (1963), 33–71.

[Shi63b] H. Shimizu, *On traces of Hecke operators*, J. Fac. Sci. Univ. Tokyo Sect. I **10** (1963), 1–19 (1963).

[Shi63c] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. **78** (1963), num. 1, 149–192.

[Shi65] H. Shimizu, *On zeta functions of quaternion algebras*, Ann. of Math. **81** (1965), 166–193.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[Shi74] G. Shimura, *On the trace formula for Hecke operators*, Acta-Math. **132** (1974), num. 3-4, 245–281.

[Shi75] G. Shimura, *On the real points of arithmetic quotient of a bounded symetric domain*, Math. Ann. **215** (1975), 135–164.

[Shi02] G. Shimura, *Collected papers. Vol. I-II. 1954–1977*, Springer, 2002.

[Shi03] G. Shimura, *Collected papers. Vol. III-IV. 1978–2001*, Springer, 2003.

[Sie35] C. Siegel, *über die analytische Theorie der quadratischen Formen*, Ann. of Math. **36** (1935), 527–606, en *Gesammelte Abhandlungen*, vol. I, Springer, 1966.

[Sie44] C. Siegel, *On the theory of indefinite quadratic forms*, Ann. of Math. **45** (1944), 577–622, en *Gesammelte Abhandlungen*, vol. II, Springer, 1966.

[Sie45] C. Siegel, *Some remarks on discontinuous groups*, Ann. of Math. **46** (1945), 708–718.

[Sie71] C. Siegel, *Topics in complex function theory vol. II*, Wiley-Interscience, 1971.

[Sil92a] A. Silverberg, *Canonical models and adelic representations*, Amer. J. of Math. **114** (1992), 1221–1241.

[Sil92b] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), 253–262.

[Sil93] A. Silverberg, *Galois representations attached to points on Shimura varieties*, Séminaire de Théorie des Nombres Paris 1990-91, Progress in mathematics, num. 108, Birkhäuser, 1993.

[Sou79] C. Soulé, *Cohomologie des groupes discrets et formes automorphes*, Variétés de Shimura et fonctions L, Publications Mathématiques de l'Université Paris VII, vol. 6, 1979, pp. 131–144.

[Spr79] T. Springer, *Reductive groups*, Proceedings of Symposia in Pure Mathematics **33** (1979), 3–27.

[SS03] S. Siksek, A. Skorobogatov, *On a Shimura curve that is a counterexample to the Hasse principle*, Bull. London Math. Soc. **35** (2003), num. 3, 409–414.

[ST61] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[ST68] J-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[SY79] H. Saito, M. Yamauchi, *Trace formula of certain Hecke operators for* $\Gamma_0(q^\nu)$, Nagoya Math. J. **76** (1979), 1–33.

[SY04] A. Skorobogatov, A. Yafaev, *Descent on certain Shimura curves*, Israel J. Math. **140** (2004), 319–332.

[Tak75] K. Takeuchi, *A characterization of arithmetic fuchsian groups*, J. Math. Soc. Japan **27** (1975), num. 4, 600–612.

[Tak77a] K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), num. 1, 91–106.

[Tak77b] K. Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo, I.A. **24** (1977), 201–212.

[Tak01] S. Takahashi, *Degrees of parametrizations of elliptic curves by Shimura curves*, J. Number Theory **90** (2001), num. 1, 74–88.

[Tat63] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Tat69] J. Tate, *Classes d'isogénie des varietés abéliennes sur un corps fini (d'après T. Honda)*, Sem. Bourbaki (1968-69), 95–110.

[Tat71] J. Tate, *Rigid analytic spaces*, Invent. Math. **12** (1971), 257–289.

[Tei93] J. T. Teitelbaum, *Modular representations of pgl_2 and automorphic forms for Shimura curves*, Invent. Math. **113** (1993), num. 3, 561–580.

[Tit74] J. Tits, *On buildings and their applications*, Proceedings of the International Congress of Mathematicians, vol. 1, 1974, pp. 209–221.

[Tit79] J. Tits, *Reductive groups over local fields*, Proceedings of Symposia in Pure Mathematics **33** (1979), 29–69.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

[TW95] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), num. 3, 553–572.

[Ull01] E. Ullmo, *Sur la constante de Hida des courbes modulaires et des courbes de Shimura*, J. Théor. Nombres Bordeaux **13** (2001), num. 1, 325–337.

[Var98a] Y. Varshavsky, *p-adic uniformization of unitary Shimura varieties*, Inst. Hautes Études Sci. Publ. Math. (1998), num. 87, 57–119.

[Var98b] Y. Varshavsky, *p-adic uniformization of unitary Shimura varieties. II*, J. Differential Geom. **49** (1998), num. 1, 75–113.

[Vat02] V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002), 1–46.

[vdG82] G. van der Geer, *On the geometry of a Siegel modular threefold*, Math. Ann. **260** (1982), num. 3, 317–350.

[vdG87] G. van der Geer, *Hilbert modular surfaces*, vol. 16, Ergebn. Math. Grenz., 1987.

[vdG01] G. van der Geer, *Curves over finite fields and codes*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, 2001, pp. 225–238.

[vdGZ77] G. van der Geer, D. Zagier, *The Hilbert modular group for the field* $\mathbb{Q}(\sqrt{13})$, Invent. Math. **42** (1977), 93–133.

[vdP89] M. van-der Put, *Les courbes de Shimura*, Séminaire de Theorie des Nombres de Bordeaux **1** (1989), 89–102.

[Vig76] M-F. Vigneras, *Invariants numériques des groupes de Hilbert*, Math. Ann. **224** (1976), 189–215.

[Vig80] M-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., num. 800, Springer, 1980.

[VZ] E. Viehweg, K. Zuo, *A characterization of certain Shimura curves in the moduli stack of abelian varietes*, at www.arxiv.gov/math.AG/0207228.

[Wad71] H. Wada, *A table of Hecke operators. I*, United States-Japan Seminar on Modern Methods in Number Theory, Tokyo University, 1971, pp. 1–10.

[Wad73] H. Wada, *A table of Hecke operators. II*, Proc. Japan Acad. **49** (1973), 380–384.

[Was82] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer, New York, 1982.

[Wei67a] A. Weil, *Basic number theory*, vol. 144, Grundl. math. Wiss., 1967.

[Wei67b] A. Weil, *über die bestimmung Dirichletsher reihen durch functionalgleichungen*, Math. Ann. **168** (1967), 149–156.

[Wei82] A. Weil, *Adeles and algebraic groups*, Progress in Math., num. 23, Birkhäuser, 1982.

[Wei95] A. Weil, *Basic number theory*, Classics in Mathematics, Springer, Berlin, 1995, Reprint of the second (1973) edition.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), num. 3, 443–551.

[Wil01] J. Wilson, *Degrees of polarizations on an abelian surface with real multiplication*, Bull. London Math. Soc. **33** (2001), 257–264.

[Yaf01] A. Yafaev, *Special points on products of two Shimura curves*, Manuscripta Math. **104** (2001), num. 2, 163–171.

[Yam71] M. Yamauchi, *On traces of Hecke operators for certain modular gropus*, Nagoya Math. J. **43** (1971), 137–149.

[Yui79] N. Yui, *Formal groups and some arithmetic properties of elliptic curves*, Algebraic geometry (Proc. Summer Meeting, Copenhagen, 1978), Lecture Notes in Math., vol. 732, Springer, 1979, pp. 630–658.

[YZ97] N. Yui, D. Zagier, *On the singular values of Weber modular functions*, Math. Comp. **66** (1997), num. 220, 1645–1662.

[Zag81] D. Zagier, *Zetafunktionen und quadratische Körper*, Hochschultex, Springer, 1981.

[Zha01] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. **153** (2001), num. 1, 27–147.

[Zin82] Th. Zink, *Über die schlechte Reduktion einiger Shimura-mannigfaltigkeiten*, Compositio Math. **45** (1982), num. 1, 15–107.