

CORBES DE SHIMURA I APLICACIONS

Montserrat Alsina
Àngela Arenas
Pilar Bayer
(eds.)



UNIVERSITAT DE BARCELONA



CORBES DE SHIMURA I APLICACIONS

Introducció de Ron Livné

Edició a cura de

Montserrat Alsina
Àngela Arenas
Pilar Bayer

Amb contribucions de

Montserrat Alsina
Àngela Arenas
Pilar Bayer
Riccardo Re
Anna Rio
Víctor Rotger
Artur Travesa
Núria Vila
Xavier Xarles

CORBES DE SHIMURA I APLICACIONS

Montserrat Alsina
Àngela Arenas
Pilar Bayer
(eds.)

Publicacions i Edicions



UNIVERSITAT DE BARCELONA



Prefaci

Aquest llibre ofereix una introducció a l'estudi de les corbes de Shimura definides sobre el cos dels racionalis 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	v
Introducció	
R. LIVNÉ	vii
1 Aritmètica d'àlgebres de quaternions	
A. RIO	1
1.1 Definicions i exemples	1
1.2 Formes quadràtiques	7
1.3 Grup de Brauer	8
1.4 Extensió d'escalars	10
1.5 Cas aritmètic. Ideals i ordres.	11
1.6 Cas local	13
1.7 Cas global	16
1.8 Tipus i classes	20
1.9 Interpretació modular	21
2 Superfícies abelianes	
amb multiplicació quaterniònica	
V. ROTGER	25
2.1 Superfícies abelianes QM sobre un cos k qualsevol . . .	29

2.2	Superfícies abelianes QM sobre $\mathbb{C}$	33
2.3	Superfícies abelianes QM sobre un cos finit	38
2.4	Superfícies abelianes QM sobre un cos de nombres . . .	41
3	Uniformització p-àdica de corbes de Shimura	
	X. XARLES	49
3.1	Corbes de Mumford	50
3.2	El semiplà superior no arquimedià	52
3.3	Uniformització de corbes de Mumford	58
3.4	El teorema de Čerednik-Drinfeld	60
4	Integral models of Shimura curves	
	(after K. Buzzard)	
	R. RE	67
4.1	The functorial point of view on Shimura curves	67
5	Operadors de Hecke. Fórmula de les traces	
	A. ARENAS	75
5.1	Operadors de Hecke	75
5.2	Fórmula de les traces	82
6	Congruències d'Eichler-Shimura	
	A. TRAVESA	91
6.1	Definicions i notacions	91
6.1.1	Divisors elementals	92
6.2	Sèries de Dirichlet formals	93
6.2.1	Productes d'Euler formals	94
6.3	Sèries de Dirichlet a l'anell de Hecke	95
6.3.1	Definició i propietats	95

6.3.2	Producte d'Euler	97
6.4	Operadors de Hecke	98
6.4.1	Caracterització de l'anell de Hecke	98
6.4.2	Formes modulars	99
6.4.3	Operadors de Hecke i sèries de Dirichlet	101
6.4.4	Correspondències modulars	106
6.4.5	Fórmula de congruència	106
6.5	Reducció de les corbes de Shimura	107
6.6	El teorema de comparació	108
7	Racionalitat de punts de corbes de Shimura	
	M. ALSINA	113
7.1	Punts reals de corbes de Shimura	114
7.2	Punts locals de corbes de Shimura	116
7.2.1	Punts de corbes de Shimura sobre $\mathbb{Q}_p$	117
7.2.2	Punts de corbes de Shimura sobre cossos locals	119
7.2.3	Classes de divisors racionals sobre cossos locals	120
7.3	Punts de corbes de Shimura sobre cossos de nombres .	122
7.3.1	Interpretació modular dels punts K -racionals .	124
7.3.2	Altres resultats de finitud	126
8	Models explícits de corbes de Shimura deguts a Kurihara	
	V. ROTGER	131
8.1	Introducció	131
8.2	Models de corbes de Shimura coneguts	132
8.3	Punts CM i la teoria de cossos de classes	134
8.4	El mètode d'Ihara i de Kurihara	135

9 Aplicacions de les corbes de Shimura. Teoremes de Ribet	
A. ARENAS, N. VILA	143
9.1 Teorema de Ribet de la isogènia	143
9.2 Corbes de Shimura i la conjectura ε de Serre	147
9.2.1 La conjectura ε	147
9.2.2 Representacions modulars	148
9.2.3 L'abaixament del nivell	149
9.2.4 Resultats clau	150
9.2.5 La corba de Shimura	151
9.2.6 Prova dels teoremes clau	153
10 Corbes de Shimura i codis de Goppa	
P. BAYER	157
10.1 Superfícies de Shimura	159
10.2 Interpretació modular local	162
10.3 Mòduls formals	164
10.4 Esquemes abelians especials	167
10.5 El teorema de Zink	168
10.6 El teorema de Tsfasman-Vlăduț-Zink	169
Bibliografia general	175

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, Piatetskii-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*, Leipzig, 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. $A = M(2, K)$ 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. $M(2, K)$ és una K -àlgebra de quaternions.

La teoria de K -àlgebres centrals i simples permet donar una altra 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, dona 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 $\text{Aut}(A) = \{\gamma_u(x) = uxu^{-1}, u \in A^*\} = \text{Inn}(A) \simeq A^*/K^*$.*

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 Corollari. *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. $\square$

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, $A \simeq M(2, K)$.
2. $F = K(i)$ és una extensió quadràtica de K .

En aquest cas, atès que l'automorfisme $i \rightarrow -i$ 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 $\text{car}(K) \neq 2$, una **K -àlgebra de quaternions** és una K -àlgebra de dimensió 4 sobre K amb una K -base $\{1, i, j, k\}$ tal que

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

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:

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

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

$$\begin{aligned} 0 &= [i, x] = 2ax_3j + 2x_2k, \\ 0 &= [j, x] = -2bx_3i - 2x_1k. \end{aligned}$$

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

$$\begin{aligned} [j, [i, x]] &= -4bx_2i \in J, \\ [k, [j, x]] &= 4abx_3j \in J, \\ [i, [k, x]] &= -4ax_1k \in J, \end{aligned}$$

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

$$M(2, K) = (1, 1)_K.$$

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 $M(2, K)$ 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 $M(2, \mathbb{R})$ 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 una 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 $H = M(2, K)$. 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 $M(2, K)$. 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 $M(2, \mathbb{R})$ 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:*

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

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

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

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

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

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*

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

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

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

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:

$$Cl(H) \in Br_2(K).$$

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

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

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

1.4.2 Definicions.

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

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

1.4.3 Exemple.

$$(a, b)_K \hookrightarrow M_2(K(\sqrt{a}, \sqrt{b}))$$

$$x \mapsto \begin{pmatrix} x_0 + x_1\sqrt{a} & \sqrt{b}(x_2 + x_3\sqrt{a}) \\ \sqrt{b}(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{pmatrix}$$

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

$$(a, b)_K \hookrightarrow M_2(K(\sqrt{a}))$$

$$x \mapsto \begin{pmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{pmatrix}$$

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

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

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

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

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 $M = (t(e_i e_j))$, 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:

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

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 $M(2, K)$.*

Si R és l'anell d'enters de K , π és un uniformitzant, F/K és l'única extensió quadràtica no ramificada i $\sigma \in \text{Gal}(F/K)$ 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

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

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

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

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 $M(2, \mathbb{Q}_p)$ són $M(2, \mathbb{Z}_p)$ i tots els seus conjugats.*

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

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

Per a un ordre $\mathcal{O}$ de l'àlgebra $M(2, \mathbb{Q}_p)$, 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 $H \not\cong M(2, \mathbb{Q}_p)$, 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 $\text{Ram}(H)$. 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 $\text{Ram}(H)$ té cardinal parell.

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

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

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:

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

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

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

Si substituïm $\mathbb{Q}$ 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 $\mathbb{Q}$.*

$$1. H_1 \simeq H_2 \Leftrightarrow \text{Ram}(H_1) = \text{Ram}(H_2).$$

$$2. H_1 \simeq H_2 \Leftrightarrow d_{H_1} = d_{H_2}.$$

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

$$1. H \simeq M(2, \mathbb{Q}) \Leftrightarrow H_p \simeq M(2, \mathbb{Q}_p) \quad \forall p \Leftrightarrow d_H = 1.$$

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 $\text{Ram}(H) = S$.*

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,

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

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:

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

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

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

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

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. $p \nmid ND \Rightarrow \mathcal{O}_p \simeq M(2, \mathbb{Z}_p)$.
2. $p \mid D \Rightarrow \mathcal{O}_p \simeq$ *únic ordre maximal de H_p (que és $\neq M(2, \mathbb{Q}_p)$).*
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. $d(\mathcal{O}) = DN$.

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 $N \Leftrightarrow d(\mathcal{O}) = DN$.
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'estudi 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:

$$\text{Ideals} \leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash H_{\mathbf{A}}^*,$$

$$\text{Ideals bilàters} \leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash N(\mathcal{O}_{\mathbf{A}}),$$

$$\text{Classes d'ideals} \leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash H_{\mathbf{A}}^* / H_K^*,$$

$$\text{Classes d'ideals bilàters} \leftrightarrow \mathcal{O}_{\mathbf{A}}^* \backslash N(\mathcal{O}_{\mathbf{A}}) / (H_K^* \cap N(\mathcal{O}_{\mathbf{A}})),$$

$$\text{Tipus d'ordres} \leftrightarrow H_K^* \backslash H_{\mathbf{A}}^* / N(\mathcal{O}_{\mathbf{A}}).$$

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 dona 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

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

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

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

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

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

Fent la identificació

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

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

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

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

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, Grundle. math. Wiss., 1967.