Punts racionals en corbes de Shimura sobre cossos quadràtics imaginaris

Carlos de Vera Piquero

Punts racionals en corbes de Shimura sobre cossos quadràtics imaginaris

Autor: Carlos de Vera Piquero

Memòria presentada al Premi Évariste Galois de la SCM, 49a convocatòria.

Índex

Introducció

El problema de resoldre equacions diofàntiques sobre els enters sovint es redueix al problema de trobar el conjunt de punts racionals en una corba algebraica, és a dir, aquells punts de la corba amb coordenades racionals. Malgrat grans esforços que es remunten fins als matemàtics de l'Antiga Grècia, encara no es coneix si existeix un algorisme general que donada l'equació d'una corba retorni el conjunt dels seus punts racionals, en cas que aquest sigui finit. De fet, encara que sapiguem que una certa corba algebraica té infinits punts racionals, calcular un d'ells amb alguna propietat desitjada pot ser una tasca ben complicada. Per exemple, no existeix encara cap algorisme capaç de calcular un punt d'ordre infinit en una corba el·líptica definida sobre $\mathbb{Q}$ de rang positiu, problema que està estretament relacionat amb la famosa i encara oberta Conjectura de Birch i Swinnerton-Dyer.

D'altra banda, donada una corba algebraica X, podem intentar demostrar que no té punts racionals, és a dir, que $X(\mathbb{Q}) = \emptyset$. Com que un punt en $X(\mathbb{Q})$ definiria un punt en $X(\mathbb{Q}_p)$ per a cada primer $p \leq \infty$ (essent $\mathbb{Q}_\infty = \mathbb{R}$ com és habitual), és clar que si $X(\mathbb{Q}_p)$ és buit per algun primer p aleshores $X(\mathbb{Q})$ també ha de ser buit. Quan això passa, es diu que *hi ha una obstrucció de tipus local-global* a l'existència de punts racionals en X. De fet, es diu que una família de corbes satisfà el *principi local-global* (o *principi de Hasse*) si per a tota corba de la família es verifica que $X(\mathbb{Q}) \neq \emptyset$ si, i només si, $X(\mathbb{Q}_p) \neq \emptyset$ per a tot primer $p \leq \infty$. Quan X satisfà el principi de Hasse, es coneixen algorismes per decidir si el conjunt $X(\mathbb{Q})$ és buit o no en un nombre finit de passos. Per exemple, d'acord amb el Teorema de Hasse-Minkowski sabem que tota corba definida per una equació quadràtica sobre un cos de nombres satisfà el principi de Hasse. Tanmateix, hi ha molts contraexemples al principi de Hasse en la literatura. En els anys 1940, Lindt i Reichardt, independentment, van trobar una de les primeres corbes per a les quals el principi de Hasse no es verifica. Aquesta corba ve definida per l'equació afí

$$y^2 = x^4 - 17.$$

D'altra banda, Selmer va provar uns anys més tard que la corba definida per l'equació $3x^3 + 4y^3 + 5z^3 = 0$ és també un contraexemple al principi de Hasse. Actualment, aquesta corba es coneix com la *cúbica de Selmer*.

En aquest treball ens centrem en les corbes de Shimura, que durant les darreres dècades han esdevingut un objecte clau en diverses qüestions de modularitat, relacionades per exemple amb l'Últim Teorema de Fermat. Avui en dia, són també un dels ingredients emprats en diferents

contribucions a la Conjectura de Birch i Swinnerton-Dyer. L'objectiu modest d'aquest treball és revisar els treballs de B. W. Jordan [**Jor86**] i A. N. Skorobogatov [**Sko05**] sobre l'existència de punts racionals en corbes de Shimura sobre cossos quadràtics imaginaris, i portar un dels seus resultats un pas més enllà (vegeu els comentaris més avall, i el Teorema 5.1).

Suposem doncs que B_D és una àlgebra de quaternions racional i indefinida de discriminant $D > 1$, i considerem la corba de Shimura $X_D/\mathbb{Q}$ associada. Segons la interpretació modular de X_D, si $K/\mathbb{Q}$ és un cos quadràtic imaginari, aleshores els punts K-racionals de X_D parametritzen superfícies abelianes amb multiplicació quaterniònica per B_D definides sobre $\bar{\mathbb{Q}}$ i amb *cos de mòduli* K, però que no necessàriament admeten un *model racional* sobre K. D'acord amb el treball de Jordan a [**Jor86**], les superfícies abelianes parametritzades per un punt $P \in X_D(K)$ admeten un model racional sobre K si, i només si, el cos K escindeix B_D (vegeu Teorema 3.2). Sota aquesta hipòtesi, Jordan va donar condicions suficients explícites per tal que $X_D(K) = \emptyset$, produint així exemples de corbes de Shimura sense punts racionals sobre cossos quadràtics imaginaris (vegeu, per exemple, el Teorema 3.5). Per demostrar aquests resultats, Jordan es basa en la interpretació modular de X_D, i utilitza especialment la representació de Galois associada a una superfície abeliana $(A, \iota)/K$ parametritzada per un punt $P \in X_D(K)$, suposant que K escindeix B_D, provinent de l'acció de $\mathrm{Gal}\,(\bar{K}/K)$ en el subgrup canònic de torsió C_p de (A, ι) associat a un primer p dividint D. A més, fent servir l'estudi de Jordan i Livné a [**JL85**] sobre punts locals en corbes de Shimura, el resultat de Jordan pot servir també per produir contraexemples al principi de Hasse sobre cossos quadràtics imaginaris.

Quan el cos quadràtic imaginari K no escindeix B_D, un punt $P \in X_D(K)$ es correspon a la classe d'isomorfisme d'una superfície abeliana amb multiplicació quaterniònica per B_D amb cos de mòduli K que *no* admet un model racional sobre K. Aquest cas és més difícil de tractar, i els resultats de [**Jor86**] no s'hi apliquen. En la terminologia de Jordan, si a més $X_D(K_v) \neq \emptyset$ per a tota plaça v de K (és a dir, si X_D té punts localment arreu sobre K), aleshores es diu que (B_D, K) és un *parell excepcional*. Aquests parells han estat fins ara inaccessibles en la literatura, en el sentit que no hi ha resultats sobre l'existència de punts K-racionals en X_D en aquests casos.

El resultat principal d'aquest treball és el Teorema 5.1, juntament amb el Corol·lari 5.3, que prova un resultat anàleg al Teorema 3.5 de Jordan sense suposar que el cos K escindeixi l'àlgebra B_D. En particular, aquests resultats permeten donar exemples de parells excepcionals (B_D, K) per als quals $X_D(K) = \emptyset$, i que per tant eren desconeguts fins ara. Es tracta, doncs, de parells excepcionals (B_D, K) per als quals X_D és un contraexemple al principi de Hasse sobre K. D'entre els exemples calculats a partir del Corol·lari 5.3, tenim que els parells

$$(B_{2\cdot 23}, \mathbb{Q}(\sqrt{-55})), (B_{2\cdot 31}, \mathbb{Q}(\sqrt{-39}), (B_{2\cdot 43}, \mathbb{Q}(\sqrt{-15}), (B_{2\cdot 59}, \mathbb{Q}(\sqrt{-7}), (B_{2\cdot 67}, \mathbb{Q}(\sqrt{-55})$$

són parells excepcionals violant el principi de Hasse (a la Taula 5.1 es poden trobar més exemples).

La prova del Teorema 5.1 utilitza tècniques similars a les emprades en [**Jor86**] i [**Sko05**]. Tanmateix, com ja hem esmentat, no necessitem suposar que K escindeix B_D, que equival a suposar

que les superfícies abelianes parametritzades per punts K-racionals en X_D admeten un model racional sobre el seu cos de mòduli. Usant una idea d'Ellenberg i Skinner introduïda a [**ES01**], enlloc de considerar les representacions de Galois usuals associades a una superfície abeliana (A, ι) amb QM parametritzada per X_D, presentem certes representacions de $\mathrm{Gal}\,(\bar{K}/K)$ *associades a punts K-racionals* en la corba de Shimura X_D, independentment de si aquests punts es corresponen amb superfícies abelianes (A, ι) amb QM admetent un model racional sobre K o no (vegeu el Capítol 4).

Més recentment, Skorobogatov interpretà a [**Sko05**] els resultats de Jordan en termes de descens. El resultat va ser que els contraexemples al principi de Hasse que es dedueixen del treball de Jordan estan explicats per l'obstrucció de Brauer-Manin. És a dir, que sota les hipòtesis de treball de Jordan (per exemple, al resultat citat al Teorema 3.5), no solament $X_D(K) = \emptyset$, sinó que el conjunt de Brauer $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ és buit. Els resultats de Skorobogatov relacionen el treball de Jordan i de Jordan-Livné amb una conjectura de B. Poonen, segons la qual l'obstrucció de Brauer-Manin és l'única obstrucció al principi de Hasse sobre cossos de nombres per a certes famílies de corbes algebraiques (vegeu [**Poo06**]). Com veiem a la Proposició 5.4, els contraexemples al principi de Hasse que sorgeixen del Corol·lari 5.3 també estan explicats per l'obstrucció de Brauer-Manin.

Aquest treball està estructurat de la següent manera. En el primer capítol, fem un breu repàs de les nocions bàsiques sobre dos temes centrals al llarg de tot el treball: les varietats abelianes i les àlgebres de quaternions. En el Capítol 2, presentem la construcció de la corba de Shimura X_D associada a una àlgebra de quaternions B_D, i exposem la seva interpretació modular en termes de superfícies abelianes amb multiplicació quaterniònica. També fem un petit incís sobre el cas de les varietats de Shimura de dimensió superior.

Ja en el Capítol 3, presentem els treballs de Jordan [**Jor86**] i Skorobogatov [**Sko05**], que són les llavors d'aquest treball. D'aquest capítol cal destacar dos objectes: el subgrup canònic de torsió C_p d'una superfície abeliana amb QM parametritzada per X_D i el recobridor de Shimura associats a un primer p dividint D.

El capítol quart està dedicat a introduir la nova eina que ens permetrà demostrar el resultat principal d'aquest treball: les representacions de Galois associades a punts en corbes de Shimura. Tanmateix, les idees que presentem en aquest capítol s'emmarquen en un context força més general. A continuació, en el Capítol 5, provem el Teorema 5.1 i expliquem algunes de les seves conseqüències, entre les que destaquen els Corol·laris 5.2 i 5.3, amb els quals produïm exemples de parells excepcionals violant el principi de Hasse.

Per últim, hem afegit un apèndix en el Capítol 6 on provem un petit resultat sobre l'existència de punts racionals en quocients d'Atkin-Lehner de corbes de Shimura.

Agraïments. Voldria agrair molt sincerament al Víctor Rotger el seu suport durant l'elaboració d'aquest treball.

CAPíTOL 1

Preliminars

En aquest primer capítol revisem les nocions bàsiques respecte a dos temes que són centrals i cabdals al llarg de tot el treball: les varietats abelianes i les àlgebres de quaternions. Al llarg del treball també es fa un ús considerable de nocions elementals de geometria algebraica i aritmètica, per a les quals el lector pot consultar alguna referència clàssica, com ara [**Har77**]. Per a aspectes més tècnics, com ara punts racionals, tècniques de descens i obstruccions a l'existència de punts racionals, recomanem al lector [**Poo**].

1. Varietats abelianes

En aquesta secció revisem les nocions bàsiques sobre varietats abelianes, amb especial atenció a l'estudi dels anells d'endomorfismes d'aquestes varietats.

Per a una teoria analítica, en la qual les varietats abelianes s'identifiquen amb els tors complexos polaritzables, una referència estàndard és [**BL92**]. Aquí hem preferit presentar un enfoc algebraic, per al qual referim al lector interessat a [**Mum70**] i [**Mil08**], per exemple.

1.1. Definicions i propietats bàsiques.

Definició 1.1. *Una* varietat abeliana definida sobre un cos k *és una varietat algebraica completa* A *definida sobre* k*, junt amb un punt* k*-racional* $o \in A(k)$ *i morfismes* $m : A \times A \to A$*,* $i : A \to A$ *definits sobre* k *satisfent els axiomes de grup.*

Recordem que una varietat algebraica V es diu *completa* si per a qualsevol varietat algebraica W, la projecció $q : V \times W \to W$ és tancada. La propietat de completesa és l'anàloga en la categoria de les varietats algebraiques a la propietat de compacitat en la categoria dels espais topològics Hausdorff.

És un fet conegut que la completesa de A implica que la llei de grup és abeliana. Per això, normalment s'escriu per $+$, i l'element identitat s'acostuma a denotar per 0. A més, les varietats abelianes són no singulars. I de fet, la no singularitat ens permet identificar divisors de Weil i feixos invertibles.

Recordem que un *divisor de Weil en* A és una suma formal $D = \sum n_Y Y$ amb $n_Y \in \mathbb{Z}$ i subvarietats Y de A de codimensió 1. Aleshores, s'escriu

$$\mathrm{CH}^1(A) = \{\text{divisors de Weil en } A\}/\{\text{divisors principals en } A\}$$

per denotar el *primer grup de Chow* de A. D'altra banda, un *feix invertible en* A és un feix localment lliure $\mathcal{L}$ de rang 1 en A. El conjunt $\mathrm{Pic}(A)$ de classes d'isomorfisme de feixos invertibles en A té

estructura natural de grup amb el producte tensorial de feixos, per a la qual el feix estructural $\mathcal{O}_A$ de A és l'element identitat. Per ser A no singular, es té un isomorfisme

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

i escrivim $\mathcal{L} = \mathcal{O}_A(D)$ per denotar el feix invertible associat al divisor de Weil D en A.

Sigui $\mathcal{L} \in \mathrm{Pic}(A)$ un feix invertible, i escrivim $\mathcal{L} = \mathcal{O}_A(D)$ amb D un divisor de Weil. Aleshores, si el k-espai vectorial de seccions globals

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

té una k-base $\{s_1, \ldots, s_n\}$, $\mathcal{L}$ indueix un morfisme

$$\begin{array}{rccc} \Psi_{\mathcal{L}} : & A & \longrightarrow & \mathbb{P}^{n-1} \\ & a & \longmapsto & \{s_1(a), \ldots, s_n(a)\}. \end{array}$$

Definició 1.2. *Es diu que $\mathcal{L}$ és un feix invertible* ample *si $\Psi_{\mathcal{L}}$ indueix una immersió tancada. I diem que $\mathcal{L}$ és un feix invertible* molt ample*, o una* polarització*, si $\mathcal{L}^{\otimes n}$ és molt ample per algun $n \geq 1$.*

Un teorema de S. Lefschetz afirma que si $\mathcal{L}$ és un feix invertible ample, aleshores $\mathcal{L}^{\otimes n}$ és molt ample per a tot $n \geq 3$. Quan $\mathcal{L}$ és una polarització, les seccions globals $s \in \mathrm{H}^0(A, \mathcal{L})$ s'anomenen *funcions theta* de A respecte de $\mathcal{L}$, i diem que el parell $(A, \mathcal{L})$ és una *varietat abeliana polaritzada.* De les definicions se segueix que:

Proposició 1.3. *Una varietat abeliana és projectiva si, i només si, admet una polarització.*

Com a varietat complexa, $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$, on $\Lambda \subseteq \mathbb{C}^g$ és un reticle complet. Aleshores, la primera classe de Chern $c_1(\mathcal{L})$ d'un feix invertible $\mathcal{L} \in \mathrm{Pic}(A)$ es pot considerar com una forma hermítica

$$H : \mathbb{C}^g \times \mathbb{C}^g \longrightarrow \mathbb{C}$$

tal que $\mathrm{Im}H(\Lambda \times \Lambda) \subseteq \mathbb{Z}$. Equivalentment, com una forma $\mathbb{R}$-bilineal alternada

$$E = \mathrm{Im}H : \mathbb{C}^g \times \mathbb{C}^g \longrightarrow \mathbb{R}$$

que és integral sobre el reticle $\Lambda \times \Lambda$ i tal que

$$E(\sqrt{-1}x, \sqrt{-1}y) = E(x, y) \quad \forall\, x, y \in \mathbb{C}^g.$$

Per un teorema de Lefschetz, $\mathcal{L}$ és una polarització si, i només si, H és definida positiva, i en tal cas el *grau* de $\mathcal{L}$ es defineix com

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

que coincideix amb la dimensió de $\mathrm{H}^0(A, \mathcal{L})$ com a espai vectorial complex.

Amb les mateixes notacions, suposem que $(A, \mathcal{L})$ és una varietat abeliana polaritzada, i escollim una base simplèctica del reticle Λ. És a dir, una $\mathbb{Z}$-base de Λ per a la qual l'expressió matricial de E és de la forma

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

per alguna $D = \mathrm{diag}(d_1, d_2, \ldots, d_g)$, $d_i \in \mathbb{N}$, amb $d_j | d_{j+1}$ per $j = 1, \ldots, g-1$. L'existència d'una tal base està garantida pel Teorema del Divisor Elemental. Aleshores, la g-tupla $(d_1, d_2, \ldots, d_g)$ s'anomena *tipus* de la polarització $\mathcal{L}$, no depèn de la base simplèctica escollida, i el grau de $\mathcal{L}$ és $\deg(\mathcal{L}) = d_1 \cdots d_g$. La polarització $\mathcal{L}$ s'anomena *primitiva* si $d_1 = 1$, i és *principal* si $d_1 = \cdots = d_g = 1$.

Exemple 1.4. *Les corbes el·líptiques són varietats abelianes de dimensió 1.* Sobre el cos $\mathbb{C}$ dels nombres complexos, és ben conegut que tota corba el·líptica és isomorfa a un tor complex $A_\tau = \mathbb{C}/\Lambda_\tau$, amb $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$, per algun $\tau \in \mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. A més, tots els tors complexos 1-dimensionals són polaritzables, de manera que tots els tors complexos de dimensió 1 són corbes el·líptiques. Tanmateix, en dimensió superior això no és cert, i un tor *genèric* de dimensió $g > 1$ no és algebraic.

Exemple 1.5. *La Jacobiana d'una corba.* Si C és una corba irreductible i no singular de gènere g sobre un cos k, aleshores $\mathrm{Pic}^0(C_{\bar{k}})$, el subgrup dels feixos invertibles invariants per translació, s'identifica amb el conjunt de punts $\bar{k}$-racionals d'una varietat abeliana de dimensió g, *la varietat Jacobiana de* C, i ve dotada d'una polarització principal:

$$\Theta = \{D \in \mathrm{Pic}^0(C_{\bar{k}}) : h^0(\mathcal{O}_C(D)) = \ell(D) > 0\}$$

és un divisor de Weil ample de $\mathrm{Pic}^0(C_{\bar{k}})$.

1.2. Homomorfismes i isogènies. Suposem que A i B són dues varietats abelianes sobre k. Un morfisme regular de varietats algebraiques $A \to B$ sobre k es diu que és un *homomorfisme* si l'aplicació induïda $A(\bar{k}) \to B(\bar{k})$ és un homomorfisme de grups. El conjunt de tots els homomorfismes de A en B definits sobre k es denota per $\mathrm{Hom}_k(A, B)$, i té una estructura natural de grup.

El cas $\mathrm{End}_k(A) := \mathrm{Hom}_k(A, A)$ és d'especial interès. La llei de grup en A proporciona una estructura natural de grup en $\mathrm{End}_k(A)$, que és lliure de torsió i finitament generat com a $\mathbb{Z}$-mòdul. A més, $\mathrm{End}_k(A)$ admet una estructura natural d'anell, en la qual el producte és la composició d'endomorfismes. Així, $\mathrm{End}_k(A)$ és l'anomenat *anell d'endomorfismes* de A. Serà també important més endavant considerar l'*àlgebra d'endomorfismes* $\mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ de A.

Remarca 1.6. És important observar que, si k no és algebraicament tancat, poden existir homomorfismes $A \to B$ que no estiguin definits sobre k, sinó sobre alguna extensió de cossos K/k. En aquest sentit, escriurem $\mathrm{Hom}_K(A, B)$ per denotar $\mathrm{Hom}_K(A_K, B_K)$, on $A_K = A \times_k K$, i similarment per B_K. Anàlogament, $\mathrm{End}_K(A)$ denotarà $\mathrm{End}_K(A_K)$.

A més, és un fet conegut que donades A i B existeix una extensió finita de cossos K/k tal que K és el mínim cos de definició de tots els homomorfismes de A en B (vegeu [**Sil92**]).

Suposem ara que $f : A \to B$ és un homomorfisme de varietats abelianes definit sobre k. Aleshores es diu que f és una *isogènia* si f és exhaustiu i té nucli finit. Si és el cas, l'extensió de cossos de funcions donada pel morfisme induït $f^* : k(B) \to k(A)$ és finita, i el seu grau $\deg(f) = [k(A) : k(B)]$ és per definició el *grau* de f. Per tant, el grau d'una isogènia és clarament multiplicatiu: si $g : B \to C$ és una altra isogènia, llavors $\deg(g \circ f) = \deg(g)\deg(f)$. Si existeix una isogènia $f : A \to B$ sobre k, es diu que A i B són *isògenes* sobre k, i es denota per $A \sim_k B$.

Una propietat important de les isogènies és la següent: si $f : A \to B$ és una isogènia, existeix una segona isogènia $g : B \to A$ i un enter positiu n tals que $f \circ g = n_B$ és la multiplicació per n en B. Aquest fet implica que les isogènies són elements invertibles en $\mathrm{End}_k^0(A)$, i per tant isomorfismes en la categoria de varietats abelianes sobre k llevat d'isogènia.

Els primers exemples d'isogènies són les aplicacions 'multiplicació per n' en una varietat abeliana A. Per a un enter positiu n, la multiplicació per n en A es denota habitualment per $n_A : A \to A$, i ve donada per $x \to nx$ usant la llei de grup. L'endomorfisme n_A és una isogènia de grau n^{2g}, on $g = \dim(A)$. La importància d'aquestes isogènies rau en el fet que proporcionen informació sobre la part de torsió del grup $A(\bar{k})$ de punts $\bar{k}$-racionals de A. Si k^s és una clausura separable de k, aleshores l'estructura de grup del nucli $A[n]$ de n_A és la següent:

$$\begin{cases} A[n](k^s) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g} & \text{si } \mathrm{char}(k) \nmid n, \\ A[p^m](k^s) \simeq (\mathbb{Z}/p^m\mathbb{Z})^i & \text{si } p = \mathrm{char}(k), \text{ per algun enter } 0 \leq i \leq g. \end{cases}$$

Com que n_A està definida sobre k, es té una acció natural del grup de Galois $\mathrm{Gal}\,(k^s/k)$ en $A[n](k^s)$: si $x \in A[n](k^s)$, aleshores per a qualsevol $\sigma \in \mathrm{Gal}\,(k^s/k)$ també es té ${}^\sigma x \in A[n](k^s)$.

1.3. Mòduls de Tate i representacions ℓ-àdiques. Sigui ℓ un nombre primer. Les aplicacions naturals $A[\ell^{n+1}](k^s) \to A[\ell^n](k^s)$ induïdes per l'aplicació ℓ_A de multiplicació per ℓ fan de $\{A[\ell^n](k^s)\}_{n\geq 1}$ un sistema projectiu. Aleshores, el límit projectiu $T_\ell(A) = \varprojlim A[\ell^n](k^s)$ és l'anomenat *mòdul de Tate ℓ-àdic* de A. Un element $a = (a_n) \in T_\ell(A)$ és una successió de punts $a_n \in A(k^s)$ tals que $\ell a_1 = 0$ i $\ell a_n = a_{n-1}$ per a tot enter $n > 1$.

Si $\ell \neq \mathrm{char}(k)$, $T_\ell(A)$ és un $\mathbb{Z}_\ell$-mòdul lliure de rang $2g$, i sovint és convenient considerar el $\mathbb{Q}_\ell$-espai vectorial $2g$-dimensional $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. A més, si E és un subcós de $\mathrm{End}_k^0(A)$, l'acció de E en $V_\ell(A)$ dóna una estructura de $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-mòdul lliure de rang $2g/[E : \mathbb{Q}]$ en $V_\ell(A)$.

Considerem de nou un homomorfisme $f : A \to B$. De manera natural, f indueix un homomorfisme de grups $A[n](k^s) \to A[n](k^s)$ per a qualsevol enter n, i per tant un $\mathbb{Z}_\ell$-homomorfisme $T_\ell(f) : T_\ell(A) \to T_\ell(B)$. Així, s'obté una aplicació

$$\mathrm{Hom}_k(A, B) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

que envia $f \in \mathrm{Hom}_k(A,B)$ a $T_\ell(f)$. Si $\ell \neq \mathrm{char}(k)$, es pot provar que aquesta aplicació és injectiva, i s'estén a una aplicació

$$\mathrm{Hom}_k^0(A,B) \longrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), V_\ell(B)).$$

En particular, quan $A = B$ aquest argument dóna lloc a un monomorfisme d'anells

$$T_\ell : \mathrm{End}_k(A) \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq \mathrm{M}_{2g}(\mathbb{Z}_\ell),$$

on l'isomorfisme depèn de l'elecció d'una $\mathbb{Z}_\ell$-base de $T_\ell(A)$. En conseqüència, $\mathrm{End}_k(A)$ té com a molt rang $4g^2$ com a $\mathbb{Z}$-mòdul.

Si $\ell \neq \mathrm{char}(k)$ i $\phi \in \mathrm{End}_k(A)$, el polinomi característic $P_\phi(T)$ de $T_\ell(\phi)$ té coeficients enters i, a més, no depèn del primer ℓ, de manera que té sentit anomenar-lo *polinomi característic* de ϕ. Aleshores, el *grau* i la *traça* de ϕ es defineixen de la manera usual en termes de $P_\phi(T)$.

Treballant amb la representació ℓ-àdica $V_\ell : \mathrm{End}_k^0(A) \to \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{M}_{2g}(\mathbb{Q}_\ell)$ de $\mathrm{End}_k^0(A)$, les nocions de polinomi característic, grau i traça es poden estendre naturalment a elements $\phi \in \mathrm{End}_k^0(A)$.

I finalment, l'acció de $\mathrm{Gal}\,(k^s/k)$ en cadascun dels grups $A[\ell^n](k^s)$ indueix una acció contínua en $T_\ell(A)$. En altres paraules, obtenim una *representació ℓ-àdica* de $\mathrm{Gal}\,(k^s/k)$, això és, un homomorfisme continu

$$\mathcal{R}_\ell : \mathrm{Gal}\,(k^s/k) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell),$$

on de nou l'isomorfisme depèn de l'elecció d'una $\mathbb{Z}_\ell$-base de $T_\ell(A)$.

1.4. La varietat abeliana dual i la involució de Rosati. Degut a la imporància de la varietat abeliana dual i la involució de Rosati en l'estudi de l'àlgebra d'endomorfismes d'una varietat abeliana, recordem breument les nocions bàsiques relatives a aquests dos conceptes. Si A és una varietat abeliana sobre k, sigui $\mathrm{Pic}(A)$ el grup dels feixos invertibles en A, i denotem per $\mathrm{Pic}^0(A)$ el subgrup dels feixos invertibles invariants per translació:

$$\mathrm{Pic}^0(A) = \{\mathcal{L} \in \mathrm{Pic}(A) : t_a^*\mathcal{L} \simeq \mathcal{L} \text{ on } A_{\bar{k}} \text{ per a tot } a \in A(\bar{k})\}.$$

La varietat abeliana *dual* de A és una varietat abeliana $A^\vee$ sobre k tal que $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$, on aquesta identificació ve donada per l'anomenat *feix de Poincaré* $\mathcal{P}$: és un feix invertible en $A \times A^\vee$ tal que per a tot $a \in A^\vee(\bar{k})$, la restricció $\mathcal{P}_{|A\times a}$ representa a en $\mathrm{Pic}^0(A_{\bar{k}})$.

Com és d'esperar, la varietat abeliana $A^\vee$ té la mateixa dimensió que A, $A^{\vee\vee}$ és canònicament isomorfa a A, i tot homomorfisme de varietats abelianes $f : A \to B$ sobre k indueix un homomorfisme $f^\vee : B^\vee \to A^\vee$ sobre k.

Tot feix invertible $\mathcal{L}$ en $A_{\bar{k}}$ indueix un homomorfisme $\varphi_\mathcal{L} : A_{\bar{k}} \to A_{\bar{k}}^\vee$ donat per $\varphi_\mathcal{L}(a) = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$. Un resultat conegut estableix que donar una polarització de A és equivalent a donar una isogènia $\lambda : A \to A^\vee$ sobre k tal que, sobre $\bar{k}$, és de la forma $\varphi_\mathcal{L}$ per algun feix ample $\mathcal{L}$ en $A_{\bar{k}}$. Aleshores, el parell (A,λ) s'anomena també *varietat abeliana polaritzada*.

Associada a la polarització $\lambda = \varphi_{\mathcal{L}}$ d'una varietat abeliana A definida sobre k existeix una (anti-)involució canònica en l'àlgebra d'endomorfismes $\mathrm{End}_k^0(A)$, l'anomenada *involució de Rosati*. Aquesta involució ve definida per l'aplicació

$$\begin{array}{ccc} \mathrm{End}_k^0(A) & \longrightarrow & \mathrm{End}_k^0(A) \\ \phi & \longmapsto & \phi' = \lambda^{-1} \circ \phi^\vee \circ \lambda. \end{array}$$

Es comprova fàcilment que en efecte es tracta d'una involució, i.e. $\phi'' = \phi$ per a tot $\phi \in \mathrm{End}_k^0(A)$, i a més satisfà

$$(\phi + \alpha)' = \phi' + \alpha', (a\phi)' = a\phi' \text{ i } (\phi \circ \alpha)' = \alpha' \circ \phi' \text{ per a tot } \phi, \alpha \in \mathrm{End}_k^0(A), a \in \mathbb{Q}.$$

Una de les propietats més importants de la involució de Rosati és que és *definida positiva*. És a dir, per a qualsevol $\phi \in \mathrm{End}_k^0(A)$, $\phi \neq 0$, es té $\mathrm{Tr}(\phi \circ \phi') > 0$. Aquí, $\mathrm{Tr}(\phi \circ \phi')$ és la traça de $\phi \circ \phi'$ com a endomorfisme, en el sentit que hem esmentat anteriorment.

1.5. L'àlgebra d'endomorfismes d'una varietat abeliana. Una varietat abeliana definida sobre k es diu que és *simple* sobre k (o k-simple) si no existeix cap varietat abeliana $B \subseteq A$ definida sobre k, llevat de la subvarietat trivial 0 i la mateixa varietat A. Si K/k és una extensió de cossos, es diu que A és simple sobre K si A_K és simple sobre K d'acord amb la definició anterior. En particular, noti's que una varietat abeliana k-simple pot no ser-ho sobre K. Finalment, es diu que A és *absolutament simple* si A és simple sobre $\bar{k}$.

El primer punt clau en l'estudi de l'àlgebra d'endomorfismes d'una varietat abeliana és el següent resultat de descomposició:

Teorema 1.7. *Sigui A una varietat abeliana definida sobre k. Existeixen varietats abelianes k-simples $A_1, \ldots, A_r$, no isògenes dues a dues, i enters positius $n_1, \ldots, n_r$ tals que*

$$A \sim_k A_1^{n_1} \times \cdots \times A_r^{n_r}.$$

A més, les varietats abelianes A_i estan unívocament determinades llevat de k-isogènia i permutació, i els enters associats n_i estan unívocament determinats.

Suposem ara que A/k és simple sobre k, i sigui $\phi \in \mathrm{End}_k(A)$. La component connexa del nucli $\ker(\phi)$ contenint l'element identitat 0 és una varietat abeliana definida sobre k, de manera que ha de ser o bé 0 o bé A, ja que A és k-simple. En conseqüència, tot endomorfisme no nul de A és una isogènia, i per tant és un element invertible en $\mathrm{End}_k^0(A)$. En altres paraules, per a una varietat abeliana k-simple A, $\mathrm{End}_k^0(A)$ és una àlgebra de divisió de dimensió finita sobre $\mathbb{Q}$. Clarament, si n és un enter positiu, l'àlgebra d'endomorfismes de A^n és llavors isomorfa a $\mathrm{M}_n(\mathrm{End}_k^0(A))$. I d'altra banda, si A i B són varietats abelianes no isògenes sobre k, aleshores $\mathrm{Hom}_k^0(A, B) = 0$ i $\mathrm{End}_k^0(A \times B) \simeq \mathrm{End}_k^0(A) \times \mathrm{End}_k^0(B)$. Aplicant el teorema anterior i aquestes observacions, es dedueix el següent resultat:

Proposició 1.8. *Sigui A una varietat abeliana definida sobre k, i considerem la seva descomposició llevat d'isogènia en varietats k-simples com en el Teorema 1.7. Aleshores,*

$$\mathrm{End}_k^0(A) \simeq \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r),$$

on D_i és l'àlgebra de divisió $\mathrm{End}_k^0(A_i)$.

En conseqüència, l'àlgebra d'endomorfismes d'una varietat abeliana és una àlgebra semisimple de dimensió finita sobre $\mathbb{Q}$. La naturalesa de les àlgebres de divisió D_i ens permet usar la classificació d'Albert, com expliquem tot seguit.

Com abans, suposem que A és una varietat abeliana k-simple amb àlgebra d'endomorfismes $D = \mathrm{End}_k^0(A)$, i admetent una polarització sobre k. Com que la traça reduïda $\mathrm{Tr}_{D/\mathbb{Q}}$ de D sobre $\mathbb{Q}$ és un múltiple positiu de Tr, la positivitat de la involució de Rosati $'$ en D associada a una polarització significa que $\mathrm{Tr}_{D/\mathbb{Q}}(\phi \circ \phi') > 0$ per a tot $\phi \neq 0$ en D. La classificació de les àlgebres simples involutives deguda a Albert pot aplicar-se al parell $(D,')$ per tal d'obtenir el següent teorema d'estructura per a les àlgebres d'endomorfismes de les varietats abelianes simples:

Teorema 1.9. *Sigui A una varietat abeliana k-simple de dimensió g. Sigui F el centre de $D = \mathrm{End}_k^0(A)$, i sigui $F_0 = \{x \in D : x' = x\}$ el subcós fix per la involució de Rosati associada a una k-polarització prèviament fixada. Definim $d = [D : F]^{1/2}$, $e = [F : \mathbb{Q}]$, $e_0 = [F_0 : \mathbb{Q}]$. Aleshores la classe d'isomorfisme de D es correspon amb un dels següents tipus:*

Tipus I: *$D = F = F_0$ és un cos de nombres totalment real, i la involució de Rosati és la identitat. En aquest cas, $e|g$.*

Tipus II: *$F = F_0$ és un cos de nombres totalment real i D és una àlgebra de quaternions totalment indefinida i de divisió sobre F, i.e. per a qualsevol embedding $\sigma : F \to \mathbb{R}$, es té $D \otimes_\sigma \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$. En aquest cas $2e|g$.*

Tipus III: *$F = F_0$ és un cos de nombres totalment real i D és una àlgebra de quaternions totalment definida i de divisió sobre F, i.e. per a qualsevol embedding $\sigma : F \to \mathbb{R}$, es té $D \otimes_\sigma \mathbb{R} \simeq \mathbb{H}$, l'àlgebra de quaternions de Hamilton. En aquest cas $e^2|g$.*

Tipus IV: *F_0 és un cos de nombres totalment real, F és una extensió CM de F_0 (és a dir, una extensió quadràtica totalment imaginària de F_0) i D és una àlgebra de divisió amb centre F. En aquest cas, $e_0 d^2|g$ si $\mathrm{char}(k) = 0$, i $e_0 d|g$ si $\mathrm{char}(k) > 0$.*

Observem que, en tots els casos, F_0 és un cos de nombres totalment real i F és o bé F_0 o bé una extensió CM de F_0. Es diu que la varietat abeliana A és de *primera* (resp. *segona*) *classe* si es dona el primer (resp. segon) cas.

En general, per a una varietat abeliana A no necessàriament simple sobre k de dimensió g, es diu que A té *multiplicació complexa* (CM) sobre k si la seva àlgebra d'endomorfismes $\mathrm{End}_k^0(A)$ conté una àlgebra commutativa semisimple de dimensió $2g$ sobre $\mathbb{Q}$, que és la màxima dimensió que pot tenir una tal subàlgebra. Si $\mathrm{char}(k) = 0$ i A és k-simple, aleshores A té CM sobre k si, i només si, $\mathrm{End}_k^0(A)$ és un cos de nombres CM de grau $2g$.

2. Àlgebres de quaternions

Sigui k un cos. L'estudi de les àlgebres de quaternions sobre k pot emmarcar-se dins la teoria de les àlgebres simples i centrals sobre k. Per a un bon tractat sobre aquesta teoria general, es pot consultar [**GS06**] i [**Pie82**]. De fet, les classes d'isomorfisme de les àlgebres de quaternions sobre k es corresponen amb els elements de 2-torsió del grup de Brauer $\mathrm{Br}(k)$ de k.

Per a la teoria específica de les àlgebres de quaternions, la referència bàsica és [**Vig80**].

2.1. Definicions bàsiques i resultats. Comencem recordant algunes generalitats sobre àlgebres de quaternions sobre un cos k.

Definició 1.10. *Una* àlgebra de quaternions B *sobre* k *és una àlgebra central i simple de rang* 4 *sobre* k*.*

Existeixen dues construccions clàssiques ben conegudes per descriure àlgebres de quaternions. Pel que fa a la primera, sigui L una àlgebra separable quadràtica sobre k, [1] sigui τ la involució no trivial de L sobre k i sigui $m \in k^\times$ un element invertible qualsevol. Aleshores, l'àlgebra

$$B = L + Lu, \tag{1}$$

on $u \in B$ és tal que

$$u^2 = m \quad \text{i} \quad ux = {}^\tau x u \text{ per a tot } x \in L,$$

és una àlgebra de quaternions sobre k, i es denota per $B = \{L, u\}$. A més, tota àlgebra de quaternions sobre k es pot expressar d'aquesta manera (cf. [**Vig80**]).

Per a la segona construcció, que és vàlida només si $\mathrm{char}(k) \neq 2$, siguin $a, b \in k^\times$, i denotem per

$$B = \left(\frac{a,b}{k}\right) = k + ki + kj + kij \tag{2}$$

l'àlgebra de dimensió 4 sobre k que té per base els elements $1, i, j, ij$, amb

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Aleshores, B és de nou una àlgebra de quaternions sobre k, i també és cert que qualsevol àlgebra de quaternions sobre k admet una presentació d'aquesta forma (si $\mathrm{char}(k) \neq 2$). De fet, observem que $(\frac{a,b}{k}) = \{k(i), b\}$. Suposarem d'ara en endavant que $\mathrm{char}(k) \neq 2$, de manera que podem treballar indistintament amb les construccions (1) i (2).

Remarca 1.11. Clarament, els elements $a, b \in k^\times$ no estan unívocament determinats per la classe d'isomorfisme de l'àlgebra de quaternions $(\frac{a,b}{k})$. El lector interessat trobarà a [**Pie82**, §1.7] una discussió sobre quan dues àlgebres de quaternions $(\frac{a,b}{k})$ i $(\frac{a',b'}{k})$ són isomorfes.

[1] És a dir, o bé una extensió quadràtica separable de k o bé $k \oplus k$.

A partir de la definició, és immediat veure que si B és una àlgebra de quaternions sobre k llavors B té una anti-involució canònica, anomenada *conjugació* i que es denota per $\beta \mapsto \bar{\beta}$. Usant la descripció (1), la conjugació es defineix estenent τ a B mitjançant $\bar{u} = -u$. Prenent la descripció (2), si $\beta = x + yi + zj + tij$ aleshores $\bar{\beta} = x - yi - zj - tij$. Dir que $\beta \mapsto \bar{\beta}$ és una anti-involució significa que si $\alpha, \beta \in B$ i $x, y \in k$ aleshores

$$\overline{x\alpha + y\beta} = x\bar{\alpha} + y\bar{\beta}, \quad \bar{\bar{\alpha}} = \alpha, \quad \overline{\alpha\beta} = \bar{\beta}\bar{\alpha}.$$

En particular, tot element $\beta \in B$ és arrel del polinomi quadràtic

$$(X - \beta)(X - \bar{\beta}) = X^2 - \mathrm{tr}(\beta)X + \mathrm{n}(\beta),$$

on

$$\mathrm{tr}(\beta) = \beta + \bar{\beta} \quad \text{and} \quad \mathrm{n}(\beta) = \beta\bar{\beta}$$

són per definició la *traça reduïda* i la *norma reduïda* de β, respectivament. De fet, per a tot $\beta \in B^\times \setminus k^\times$ es té que $k(\beta)/k$ és una extensió quadràtica. A més, la conjugació en B restringida a $k(\beta)$ coincideix amb el k-automorfisme no trivial de $k(\beta)$, la qual cosa implica que $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in k$ per a tot $\beta \in B$, i llavors el polinomi anterior és un element de $k[X]$. Intuïtivament, una àlgebra de quaternions sobre k és una col·lecció d'extensions quadràtiques disposades de forma no commutativa.

Exemple 1.12. L'àlgebra de matrius $\mathrm{M}_2(k)$ sobre k és una àlgebra de quaternions. De fet, per a qualsevol $b \in k^\times$ l'assignació

$$i \mapsto I := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto J := \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

defineix un isomorfisme $(\frac{1,b}{k}) \simeq \mathrm{M}_2(k)$. Si una àlgebra de quaternions B sobre k és isomorfa a l'àlgebra de matrius $\mathrm{M}_2(k)$ aleshores es diu que B és l'àlgebra *escindida* (en anglès, *split*), en contraposició al cas d'una àlgebra de divisió.

L'exemple de l'àlgebra de matrius és un cas important. De fet, tal i com es prova a [**Vig80**, Corollaire I.2.4], una àlgebra de quaternions sobre k és o bé una àlgebra de divisió o bé isomorfa a $\mathrm{M}_2(k)$. Per aquest motiu, es defineix l'*invariant de Hasse* d'una àlgebra de quaternions B com

$$\varepsilon(B) = \begin{cases} -1 & \text{si } B \text{ és de divisió,} \\ 1 & \text{altrament.} \end{cases}$$

A més, aquesta dicotomia es pot traduir en el llenguatge de les formes quadràtiques, teoria que està per tant estretament lligada a la de les àlgebres de quaternions. No és difícil comprovar (vegeu [**Pie82**, §1.6]) que l'àlgebra de quaternions $B = (\frac{a,b}{k})$ és de divisió si, i només si, la forma

quadràtica $ax^2 + by^2 - z^2 = 0$ només admet la solució trivial $x = y = z = 0$ en k^3. Si $a, b \in k$, es defineix el *símbol de Hilbert* del parell (a, b) sobre k com

$$(a,b)_k = \begin{cases} 1 & \text{si } ax^2 + by^2 - z^2 = 0 \text{ té solucions no trivials en } k^3, \\ -1 & \text{altrament.} \end{cases}$$

Aleshores, pel resultat citat anteriorment $(a, b)_k = \varepsilon((\frac{a,b}{k}))$.

Remarca 1.13. Pel que fa a la relació entre àlgebres de quaternions i formes quadràtiques, pot trobar-se una bona exposició a [**AB04**], on, des de l'estudi de punts CM en corbes de Shimura, es presenta una classificació de les formes quadràtiques binàries amb coeficients algebraics per l'acció de grups Fuchsians aritmètics, recuperant la teoria de Gauss sobre la classificació de formes quadràtiques binàries amb coeficients enters per l'acció del grup modular.

Les àlgebres de matrius també juguen un paper important en la noció de *cos de descomposició* (en anglès, *splitting field*): es diu que una extensió de cossos K/k descomposa (o *escindeix*) una àlgebra de quaternions B sobre k si l'àlgebra de quaternions $B \otimes_k K$ sobre K obtinguda per extensió d'escalars és escindida (i.e. isomorfa a $\mathrm{M}_2(K)$). Per [**Vig80**, Théorème I.2.8], una extensió quadràtica K/k escindeix l'àlgebra B si, i només si, K és isomorf a un subcós maximal de B. Si un cos K escindeix B, aleshores mitjançant la inclusió natural $B \hookrightarrow B \otimes_k K \simeq \mathrm{M}_2(K)$ la traça i la norma reduïdes d'un element $\beta \in B$ es poden calcular en $\mathrm{M}_2(K)$ com la traça i el determinant usuals, respectivament.

Donat un cos k, és natural estudiar el problema de classificar les classes d'isomorfisme d'àlgebres de quaternions sobre k. Per la remarca que segueix l'Exemple 1.12, és suficient classificar les àlgebres de quaternions de divisió sobre k. Presentem primer dos exemples importants:

Exemple 1.14. En 1843, W. R. Hamilton descobrí que l'àlgebra real $\mathbb{H}$ de rang 4 generada per dos elements i, j satisfent $i^2 = j^2 = -1$, $ij = -ji$, és una àlgebra de divisió no commutativa. En la nostra notació, aquesta àlgebra es correspon amb l'àlgebra $(\frac{-1,-1}{\mathbb{R}})$. Pel Teorema de Frobenius ([**Vig80**, Corollaire I.2.5], [**Pie82**, Corollary 13.1.c]), l'àlgebra dels quaternions de Hamilton $\mathbb{H}$ és l'única àlgebra de divisió de dimensió finita i no commutativa sobre $\mathbb{R}$, llevat d'isomorfisme. Per tant, qualsevol altra àlgebra de quaternions sobre $\mathbb{R}$ és isomorfa o bé a $\mathrm{M}_2(\mathbb{R})$ o bé a $\mathbb{H}$.

Exemple 1.15. Si k és algebraicament tancat, el Teorema de Wedderburn sobre la classificació d'àlgebres simples implica que tota àlgebra central i simple sobre k és isomorfa a $\mathrm{M}_n(k)$ per algun enter $n \geq 1$ (vegeu [**GS06**, Theorem 2.1.3] i [**GS06**, Corollary 2.1.7]). Així, per exemple, l'única àlgebra de quaternions sobre el cos $\mathbb{C}$ dels nombres complexos (llevat d'isomorfisme) és $\mathrm{M}_2(\mathbb{C})$.

2.2. Ordres i ideals. La no commutativitat de les àlgebres de quaternions fa que la teoria dels ordres sigui lleugerament més subtil que el seu anàleg en cossos de nombres. Presentarem les definicions bàsiques i els resultats essencials pel que fa a ordres i ideals en àlgebres de quaternions.

En tot el que segueix, sigui R un domini de Dedekind amb cos de fraccions k, i sigui B una àlgebra de quaternions sobre k.

Com en el cas dels cossos de nombres, es diu que un element $\beta \in B$ és *enter* si $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in R$. Tanmateix, en el cas de les àlgebres de quaternions no és cert en general que el conjunt d'elements enters de B sigui un anell. Un exemple senzill que il·lustra aquest fet ve donat per les dues matrius següents en l'àlgebra $\mathrm{M}_2(\mathbb{Q})$:

$$A = \begin{pmatrix} \frac{1}{2} & -3 \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & \frac{1}{5} \\ 5 & 0 \end{pmatrix}.$$

Tant A com B són elements enters, però ni $A+B$ ni AB ho són.

Per tant, la noció d'*ordre* es generalitza al context de les àlgebres de quaternions de la següent manera:

Definició 1.16. *Un* ordre $\mathcal{O} \subset B$ *sobre* R *és un* R*-reticle complet que també és un anell. Equivalentment, és un anell format per elements enters de* B*, finitament generat com a* R*-mòdul i tal que* $\mathcal{O} \otimes_R k = B$*. Es diu que un ordre* $\mathcal{O}$ *en* B *és un* ordre maximal *si és maximal respecte la inclusió, i es diu que* $\mathcal{O}$ *és un* ordre d'Eichler *si és la intersecció de dos ordres maximals.*

Recordem que un R-reticle en B és un R-mòdul lliure $\Lambda \subseteq B$. Llavors, un R*-ideal* (o simplement un *ideal*) és un R-reticle I en B tal que $I \otimes_R k \simeq B$. Es diu que un ideal és *enter* si tots els seus elements ho són. D'acord amb la definició anterior, un ordre és un ideal que és alhora un anell. Per exemple, si $\{v_1, v_2, v_3, v_4\}$ és una k-base de B, llavors $R[v_1, v_2, v_3, v_4]$ és un ideal i un ordre en B.

Per a un ideal I de B, es defineixen els seus *ordres per l'esquerra* i *per la dreta* com

$$\mathcal{O}_\ell(I) = \{\beta \in B : \beta I \subseteq I\}, \quad \mathcal{O}_r(I) = \{\beta \in B : I\beta \subseteq I\},$$

respectivament. Un ideal I és *bilateral* si $\mathcal{O}_\ell(I) = \mathcal{O}_r(I)$, i és fàcil veure que

$$I \text{ és integral} \iff II \subseteq I \iff I \subseteq \mathcal{O}_\ell(I), \mathcal{O}_r(I).$$

Es diu que un ideal I és *principal* si existeix un element $\beta \in B$ tal que $I = \mathcal{O}_\ell(I)\beta = \beta\mathcal{O}_r(I)$. Per a ideals bilaterals I, J, el seu producte IJ es pot definir de la manera usual, i l'invers d'un ideal bilateral I es defineix com $I^{-1} = \{\beta \in B : I\beta I \subseteq I\}$, i satisfà

$$II^{-1} \subseteq \mathcal{O}_\ell(I), \quad I^{-1}I \subseteq \mathcal{O}_r(I).$$

A més, tenim una noció d'equivalència entre ideals. Dos ideals I, J són *equivalents per l'esquerra* si $I = \beta J$ per algun $\beta \in B$. Com en el cas dels cossos de nombres, és fàcil comprovar que l'equivalència d'ideals és realment una relació d'equivalència. Per tant, com que els ordres són ideals, per a un ordre $\mathcal{O}$ denotarem per $\mathrm{Pic}_\ell(\mathcal{O})$ el conjunt d'ideals I per als quals $\mathcal{O}_r(I) = \mathcal{O}$ mòdul equivalència per l'esquerra. Anàlogament, podríem definir $\mathrm{Pic}_r(\mathcal{O})$ com el conjunt d'ideals I per als quals $\mathcal{O}_\ell(I) = \mathcal{O}$ mòdul equivalència per la dreta, que està en bijecció natural amb $\mathrm{Pic}_\ell(\mathcal{O})$.

Per a un ordre $\mathcal{O}$, s'anomena *nombre de classes de* $\mathcal{O}$ al cardinal $|\mathrm{Pic}_\ell(\mathcal{O})|$. No és difícil comprovar que tots els ordres maximals tenen el mateix nombre de classes, de manera que té sentit definir el *nombre de classes* de B com $h(B) = |\mathrm{Pic}_\ell(\mathcal{O})|$, on ara $\mathcal{O}$ és qualsevol ordre maximal en B.

Donat un ordre $\mathcal{O}$, podem conjugar $\mathcal{O}$ per un element $\beta \in B^\times$ per obtenir de nou un ordre. Es diu que dos ordres són del mateix *tipus* si són conjugats per algun $\beta \in B^\times$. Aleshores, es defineix el *nombre de tipus* $t(B)$ de B com el nombre de classes de conjugació d'ordres maximals de B. El nombre de tipus és sempre menor o igual al nombre de classes, $t(B) \leq h(B)$.

Finalment, per a un ideal I, denotarem per $\mathrm{n}(I)$ el R-ideal fraccionari generat per les normes reduïdes dels elements de I. Per a un ordre $\mathcal{O}$, el *diferent* $d(\mathcal{O})$ és l'ideal fraccional definit per $d(\mathcal{O}) = (\mathcal{O}^*)^{-1}$, on $\mathcal{O}^* = \{\beta \in B : \mathrm{tr}(\beta\mathcal{O}) \subseteq R\}$. Aleshores, el *discriminant* $D(\mathcal{O})$ de l'ordre $\mathcal{O}$ es defineix com la norma del diferent, $D(\mathcal{O}) = \mathrm{n}(d(\mathcal{O}))$. Si $\{v_i\}$ és una R-base de l'ordre $\mathcal{O}$, llavors $D(\mathcal{O})^2$ és l'ideal principal $R\det(\mathrm{tr}(v_i v_j))$.

2.3. Àlgebres de quaternions sobre cossos locals. Ara ens centrem en les àlgebres de quaternions sobre cossos locals. Recordem que un cos k és un *cos local* si és una extensió finita d'un dels següents cossos:

- $\mathbb{R}$, el cos dels nombres reals,
- $\mathbb{Q}_p$, el cos dels nombres p-àdics, per algun primer p, o
- $\mathbb{F}_p[[T]]$, el cos de sèries formals en una variable sobre el cos finit $\mathbb{F}_p$ de p elements, per algun primer p.

Els cossos locals $\mathbb{R}$ i $\mathbb{C}$ s'anomenen *arquimedians*, mentre que als altres se'ls anomena *no arquimedians*.

La classificació de les àlgebres de quaternions sobre cossos locals és particularment senzilla. A l'Exemple 1.15 ja hem esmentat que l'única àlgebra de quaternions (llevat d'isomorfisme) sobre $\mathbb{C}$ és l'àlgebra de matrius $\mathrm{M}_2(\mathbb{C})$. I segons hem vist a l'Exemple 1.14, existeix només una àlgebra de quaternions de divisió sobre $\mathbb{R}$ llevat d'isomorfisme, l'àlgebra de quaternions de Hamilton $\mathbb{H}$. Amb aquests casos coberts, suposarem d'ara en endavant que k és un cos local no arquimedià.

Com es demostra a [**Vig80**, §I.1], el Teorema de Frobenius s'estén al cas no arquimedià, és a dir, existeix només una àlgebra de quaternions de divisió sobre k llevat d'isomorfisme. Per tal de fer precís aquest enunciat, necessitem introduir notacions. Denotarem per R_k l'anell d'enters de k, i π denotarà un element primer en R_k, i.e., un generador de l'ideal maximal de R_k, de manera que R_k/π és el cos residual de k. També denotem per L_{nr} l'única extensió quadràtica no ramificada de k dins d'una clausura separable k^s de k prèviament fixada. Aleshores,

(a) π és un element primer en L_{nr},
(b) $R_k^\times = \mathrm{n}(R_L^\times)$, on R_L és l'anell d'enters de L_{nr}, i
(c) $[R_L/\pi : R_k/\pi] = 2$, on R_L/π és el cos residual de L_{nr}.

Amb aquestes notacions, el teorema de classificació que hem citat anteriorment admet el següent enunciat explícit (cf. [**Vig80**, Théorème II.1.3]):

Teorema 1.17. *L'àlgebra de quaternions $H = \{L_{nr}, \pi\}$ és l'única àlgebra de quaternions de divisió sobre k llevat d'isomorfisme. A més, una extensió de cossos K/k escindeix H si, i només si, el seu grau $[K : k]$ és parell.*

Aquesta senzilla classificació de les àlgebres de quaternions sobre cossos locals facilita l'estudi dels ordres i ideals en aquestes àlgebres.

Suposem primer que B és l'àlgebra de matrius $B \simeq \mathrm{M}_2(k)$. Aleshores, podem pensar B com l'àlgebra d'endomorfismes d'un k-espai vectorial 2-dimensional V, $B \simeq \mathrm{End}(V)$. Els ordres maximals de $\mathrm{End}(V)$ són els anells $\mathrm{End}(\Lambda)$, on Λ és un R_k-reticle complet de V, i els ideals d'aquests ordres són tots de la forma $\mathrm{Hom}(\Lambda_1, \Lambda_2)$, per a Λ_i R_k-reticles complets de V. En conseqüència:

Proposició 1.18. *Tots els ordres maximals de $\mathrm{M}_2(k)$ són conjugats de $\mathrm{M}_2(R_k)$, i els ideals bilaterals de $\mathrm{M}_2(R_k)$ formen un grup cíclic generat per l'ideal primer $\mathrm{M}_2(R_k)\pi = \pi\mathrm{M}_2(R_k)$.*

En segon lloc, suposem que $B = H$ és l'única (llevat d'isomorfisme) àlgebra de quaternions de divisió sobre k, donada pel Teorema 1.17. Si v és una valoració discreta en k, aleshores v pot ser estesa a una valoració discreta w de B posant $w(\beta) = v(\mathrm{n}(\beta))$ per $\beta \in B$. D'aquesta manera, l'anell de valoració de w és $\mathcal{O} = \{\beta \in B : \mathrm{n}(\beta) \in R_k\}$, que és un ordre maximal, ja que conté tots els elements enters de B.

Proposició 1.19. *Sigui B una àlgebra de quaternions de divisió sobre k. Aleshores B conté un únic ordre maximal, que és $\mathcal{O} = \{\beta \in B : \mathrm{n}(\beta) \in R_k\}$. En particular, és també l'únic ordre d'Eichler. A més, l'ideal πR_k ramifica: $\pi\mathcal{O} = \mathfrak{p}^2$, on $\mathfrak{p}$ és l'únic ideal maximal de $\mathcal{O}$.*

2.4. Àlgebres de quaternions sobre un cos de nombres. A continuació tractarem el cas dels cossos de nombres (més generalment, podríem considerar cossos globals). Sigui doncs F un cos de nombres, i denotem per R_F el seu anell d'enters. Per a cada plaça v de F, escollim un embedding $F \hookrightarrow F_v$, on F_v és la compleció de F en v. Recordem que les places finites estan en bijecció amb els ideals primers de R_F, les places reals es corresponen amb els diferents embeddings reals de F i les places complexes amb els diferents parells d'embeddings complexos conjugats de F.

Si B és una àlgebra de quaternions sobre F, aleshores podem definir $B_v := B \otimes_F F_v$, que és una àlgebra de quaternions sobre el cos local F_v. Considerant aquestes àlgebres B_v per a totes les places v i usant els resultats de l'apartat anterior, podem estudiar propietats globals de l'àlgebra de quaternions B.

Per l'Exemple 1.15, sabem que si v és una plaça complexa de F aleshores $B_v \simeq M_2(\mathbb{C})$. Altrament, si v és una placa real o no arquimediana, el Teorema 1.17 implica que o bé $B_v \simeq M_2(F_v)$ o bé $B_v \simeq \mathbb{H}_v$, on $\mathbb{H}_v$ denota l'única àlgebra de quaternions de divisió sobre F_v. Aquest fet motiva la següent definició:

Definició 1.20. *Sigui v una plaça de F. Es diu que v* escindeix *en B si $B_v \simeq M_2(F_v)$, i es diu que v* ramifica *en B si B_v és de divisió.*

La ramificació en les places reals jugarà un paper important per nosaltres. Es diu que B és *totalment indefinida* sobre F si cap plaça real ramifica en B, i es diu que B és *totalment definida* sobre F si tota plaça real ramifica en B. Per al cas $F = \mathbb{Q}$, simplement diem que B és indefinida o definida, ja que només hi ha una plaça real per comprovar.

En el que segueix, denotarem per $\mathrm{Ram}(B)$ el conjunt de places de F que ramifiquen en B. El següent teorema de classificació, degut a H. Hasse, ens diu que aquest conjunt determina completament B llevat d'isomorfisme (cf. [**Vig80**, Théorème III.3.1]):

Teorema 1.21 (Hasse)**.** *El nombre $|\mathrm{Ram}(B)|$ de places ramificades en una àlgebra de quaternions B sobre F és parell. A més, per a tot conjunt finit S de places de F de cardinalitat parella existeix una única àlgebra de quaternions B sobre F, llevat d'isomorfisme, tal que $\mathrm{Ram}(B) = S$.*

En altres paraules, la classe d'isomorfisme d'una àlgebra de quaternions sobre un cos de nombres està unívocament determinada pel conjunt (finit) de places que hi ramifiquen. Per a una àlgebra de quaternions B sobre F, el *discriminant reduït* $\mathfrak{D} = \mathrm{disc}(B)$ és el producte de les places finites en $\mathrm{Ram}(B)$. Per tant, podem considerar $\mathfrak{D} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ com a ideal de R_F, on $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ són ideals primers de R_F, diferents dos a dos. Quan $F = \mathbb{Q}$, $\mathrm{disc}(B)$ és l'ideal principal generat per $D = p_1 \cdots p_s$, on els p_i són els primers que ramifiquen en B, de manera que identificarem $\mathrm{disc}(B)$ amb l'enter positiu D.

La importància del Teorema 1.21 no rau només en el fet que dóna una classificació clara i precisa de les àlgebres de quaternions sobre F, sinó també en les importants conseqüències que se'n deriven. Resumim breument algunes d'elles a continuació (vegeu [**Vig80**, pp. 75-76] per a més detalls).

El primer corol·lari que presentem és l'anomenat *Principi de Hasse per formes quadràtiques*, que pot ser provat utilitzant el Teorema 1.21:

Corol·lari 1.22. *Si f és una forma quadràtica sobre un cos de nombres F, aleshores f és isòtropa sobre F si, i només si, f és isòtropa sobre F_v, per a tota plaça v de F.*

La següent conseqüència relaciona el símbol de Hilbert $(\cdot,\cdot)_v := (\cdot,\cdot)_{F_v}$ de les complecions de F, i és coneguda com la *llei de reciprocitat del símbol de Hilbert*. De fet, la Llei de Reciprocitat Quadràtica pot deduïr-se a partir d'ella:

Corol·lari 1.23. *Sigui F un cos de nombres, i per a un parell d'elements $a, b \in F^\times$ denotem per $(a,b)_v = (a,b)_{F_v}$ el seu símbol de Hilbert relatiu a F_v. Aleshores es té la* fórmula del producte

$$\prod_v (a,b)_v = 1,$$

on el producte és sobre totes les places v de F.

Observem que el producte en la fórmula anterior és de fet un producte finit, ja que pel Teorema 1.21 només un nombre finit de símbols de Hilbert són $\neq 1$. En el cas en què $F = \mathbb{Q}$, una aplicació del darrer corol·lari és el càlcul dels símbols de Hilbert locals. Si $a, b \in \mathbb{Q}$ i p és un primer senar, el símbol de Hilbert $(a, b)_p$ es pot calcular fàcilment seguint la recepta en [**Vig80**, p. 37], i llavors per la fórmula del producte obtenim

$$(a, b)_2 = \prod_{v \neq 2} (a, b)_v.$$

Del Teorema 1.21 es dedueixen també dues propietats que són ben importants per elles mateixes. La primera d'elles és la paritat del nombre de places ramificades en una àlgebra de quaternions, i la segona és una caracterització de l'àlgebra de matrius: una àlgebra de quaternions B sobre F és isomorfa a $\mathrm{M}_2(F)$ si, i només si, $B_v \simeq \mathrm{M}_2(F_v)$ per a tota plaça v de F. Aquestes propietats condueixen als següents dos corol·laris respecte a normes en extensions quadràtiques de F i els cossos de descomposició de l'àlgebra B.

Corol·lari 1.24. *Sigui F un cos de nombres, L/F una extensió quadràtica i $\theta \in F^\times$. Aleshores θ és la norma d'un element en L si, i només si, θ és la norma d'un element en $L_v := L \otimes F_v$ per a tota plaça v de F, excepte per possiblement una.*

Corol·lari 1.25. *Sigui B una àlgebra de quaternions sobre un cos de nombres F. Una extensió finita L/F és un cos de descomposició per B si, i només si, L_w és un cos de descomposició per B_v, per a tota plaça $w|v$ de L.*

Abans de passar a l'estudi d'ordres i ideals, és important esmentar el següent resultat caracteritzant els subcossos quadràtics de B, conegut sovint com *criteri de Hasse*:

Teorema 1.26. *Una extensió quadràtica L/F és un subcós de l'àlgebra de quaternions B si, i només si, $L_v = L \otimes F_v$ és un cos per a tota plaça $v \in \mathrm{Ram}(B)$.*

Particularitzem el cas $F = \mathbb{Q}$ en el següent corol·lari:

Corol·lari 1.27. *Sigui B una àlgebra de quaternions racional, i sigui $K/\mathbb{Q}$ un cos quadràtic. Si K és real i B és definida, aleshores K no escindeix B. Altrament, K escindeix B si, i només si, per a tot primer p dividint el discriminant de B, p no descomposa en K.*

Darrera de la demostració de tots aquests resultats, hi ha la idea de treballar "adèlicament". Per a l'estudi dels ordres i ideals és també una eina clau, que descrivim breument a continuació.

Comencem escollint un conjunt finit S de places de F, incloent totes les infinites, i sigui

$$R = R_{(S)} = \bigcap_{v \notin S} (R_v \cap F),$$

on $R_v := R_{F_v}$. Llavors R és un domini de Dedekind, i serà considerat com l'anell d'elements que són enters fora de S.

Aleshores, considerem donats un grup localment compacte G_v per a cada placa v de F, i també un subgrup compacte obert C_v de G_v per a cada plaça $v \notin S$.

Definició 1.28. *Amb les notacions anteriors, el* producte restringit $G_{\mathbb{A}}$ *dels grups* G_v *respecte els subgrups* C_v *és*

$$G_{\mathbb{A}} = \{x = (x_v) \in \prod_v G_v : x_v \in C_v \text{ per a quasi tota } v \notin S\}.$$

El grup $G_{\mathbb{A}}$ pot dotar-se d'una topologia per a la qual esdevé un grup topològic localment compacte, que a més no depèn de S. Aquesta situació ocorre quan G és un grup algebraic definit sobre F. Aleshores, G_v és el conjunt $G(F_v)$ de punts F_v-racionals, i es pren C_v com el conjunt $G(R_v)$ de punts R_v-racionals per v fora del conjunt finit de places S. Llavors, el grup $G_{\mathbb{A}}$ s'anomena *grup dels adèles* de G.

Exemple 1.29. L'*anell dels adèles* $\mathbb{A}_F$ de F esdevé d'aquesta manera quan s'escull $G_v = F_v$, $S = \infty$ el conjunt de places infinites i $C_v = R_v$. El grup d'elements invertibles en $\mathbb{A}_F$ és el *grup dels idèles* $\mathbb{A}_F^\times$ de F, i esdevé quan s'escull $G_v = F_v^\times$, $S = \infty$ i $C_v = R_v^\times$.

Exemple 1.30. Una àlgebra de quaternions B sobre F també dóna lloc a certs grups d'adèles de manera similar. L'*anell dels adèles* $B_{\mathbb{A}}$ de B es defineix escollint $G_v = B_v$, $S \supseteq \infty$ i $C_v = \mathcal{O}_v$, on $\mathcal{O}$ és un ordre de B sobre l'anell $R = R_{(S)}$ i $\mathcal{O}_v = \mathcal{O} \otimes_R R_v$. Aleshores $B_{\mathbb{A}}$ és isomorf al producte tensorial $\mathbb{A}_F \otimes_F B$. Com és d'esperar, el grup $B_{\mathbb{A}}^\times$ d'elements invertibles de $B_{\mathbb{A}}$ s'obté prenent $G_v = B_v^\times$, $S \supseteq \infty$ i $C_v = \mathcal{O}_v^\times$.

Ara fixem un conjunt de places S del cos de nombres F, contenint les infinites. Si $S = \infty$, aleshores observi's que $R = R_\infty$ és l'anell d'enters R_F de F.

Per tal d'usar les propietats locals d'ideals i ordres, si Y és un R-reticle de B, aleshores posarem $Y_v = Y \otimes_R R_v$. Quan $v \in S$, llavors $R_v = F_v$ i $Y_v = B_v$. El punt clau és que un R-reticle Y està unívocament determinat pels reticles locals $(Y_v)_{v \notin S}$ (vegeu [**Vig80**, Proposition III.5.1]). Per tant, tenim la noció de *propietat local* d'ideals (o reticles). És a dir, una propietat $\star$ és local si un ideal I satisfà $\star$ si, i nomes si, I_v satisfà $\star$ per a tot $v \notin S$. Alguns exemples de propietats locals són: ésser un ideal, ésser un ideal enter, ésser un ordre i ésser un ordre maximal, entre d'altres.

Tanmateix, la propietat de ser un ideal principal no és una propietat local, i aquest és un dels motius principals per treballar en el llenguatge adèlic. En el que segueix, identificarem un R-reticle Y amb les seves localitzacions $(Y_v)_{v \notin S}$ i escriurem

$$Y_{\mathbb{A}} = \prod_v Y_v, \quad \text{amb } Y_v = B_v \text{ si } v \in S.$$

Ens restringirem ara als ordres maximals en B. Com que els ideals amb ordres per l'esquerra i per la dreta maximals són localment principals ([**Vig80**, p. 86]), suposarem que tots els ideals que considerarem són localment principals. Fixat un ordre maximal $\mathcal{O}$ de B, li podem doncs associar els següents objectes adèlics:

(i) $\mathcal{O}_{\mathbb{A}}$, l'anell dels adèles de $\mathcal{O}$,

(ii) $\mathcal{O}_{\mathbb{A}}^{\times}$, el grup d'unitats de $\mathcal{O}_{\mathbb{A}}$,

(iii) $N(\mathcal{O}_{\mathbb{A}})$, el normalitzador de $\mathcal{O}_{\mathbb{A}}$ en $B_{\mathbb{A}}^{\times}$.

Aleshores, mitjançant l'aplicació $(x_v) \in B_{\mathbb{A}}^{\times} \mapsto I$, on I és l'ideal tal que $I_v = \mathcal{O}_v x_v$ si $\notin S$, el conjunt dels $\mathcal{O}$-ideals per l'esquerra està en bijecció amb $\mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}$. Per tant, el conjunt de $\mathcal{O}$-ideals bilaterals està en bijecció amb $\mathcal{O}_{\mathbb{A}}^{\times} \setminus N(\mathcal{O}_{\mathbb{A}})$. Pel que fa als ordres maximals, estan en bijecció amb els elements de $N(\mathcal{O}_{\mathbb{A}})/B_{\mathbb{A}}^{\times}$: un element $(x_v) \in B_{\mathbb{A}}^{\times}$ es correspon amb l'ordre $\mathcal{O}'$ determinat per $\mathcal{O}'_v = x_v^{-1}\mathcal{O}_v x_v$ per $v \notin S$.

D'aquesta manera, tenim el següent diccionari global-adèlic:

$$\begin{aligned} \mathcal{O}\text{-ideals per l'esquerra} &\leftrightarrow \mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}, \\ \mathcal{O}\text{-ideals bilaterals} &\leftrightarrow \mathcal{O}_{\mathbb{A}}^{\times} \setminus N(\mathcal{O}_{\mathbb{A}}), \\ \text{ordres maximals} &\leftrightarrow N(\mathcal{O}_{\mathbb{A}})/B_{\mathbb{A}}^{\times}, \\ \mathrm{Pic}_{\ell}(\mathcal{O}) &\leftrightarrow \mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}/B^{\times}, \\ \text{tipus d'ordres maximals} &\leftrightarrow B^{\times} \setminus B_{\mathbb{A}}^{\times}/N(\mathcal{O}_{\mathbb{A}}). \end{aligned}$$

En analogia al cas commutatiu, sembla natural esperar que aquests conjunts siguin finits, i que la seva cardinalitat estigui relacionada amb el nombre de classes de F, és a dir, l'ordre de $R_{F,\mathbb{A}}^{\times} \setminus \mathbb{A}_F/F^{\times}$.

De fet, l'estudi de la interpretació anterior amb classes laterals dels ordres maximals té com a conseqüència la finitud del nombre de classes de B:

Teorema 1.31. *Sigui $\mathcal{O}$ un ordre maximal en B. Aleshores $\mathrm{Pic}_{\ell}(\mathcal{O})$ és finit, de manera que el nombre de classes i el tipus de B són finits.*

En alguns casos, és possible fer un pas més enllà encara. Sigui F_B el conjunt dels elements de F que són positius en totes les places reals ramificant en B. Pel Teorema de la Norma (vegeu [**Vig80**, Théorème III.4.1]), $F_B = \mathrm{n}(B)$. Denotem també per P_B el subgrup del grup $Frac(F)$ d'ideals fraccionals de F que consisteix en els ideals principals generats per un element de F_B, i sigui h_B l'ordre del quocient $Frac(F)/P_B$. Notem que $h(F) \leq h_B \leq h^+(F)$, on $h(F)$ i $h^+(F)$ són, respectivament, el nombre de classes i el nombre de classes estricte de F.

Aleshores, la norma reduïda indueix una aplicació entre conjunts de classes laterals dobles

$$\mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}/B \longrightarrow R_{\mathbb{A}}^{\times} \setminus \mathbb{A}_F^{\times}/F_B.$$

Usant el Teorema Fort d'Aproximació, aquesta aplicació resulta ser una bijecció (vegeu [**Vig80**, III.4.3]), i ens porta al següent resultat, que és conseqüència d'un teorema degut a M. Eichler:

Teorema 1.32. *Sigui $\mathcal{O}$ un ordre maximal en una àlgebra de quaternions B no totalment definida sobre F. La norma reduïda indueix una bijecció $\mathrm{Pic}_{\ell}(\mathcal{O}) \to Frac(F)/P_B$. En particular, el nombre de classes de B és h_B.*

Quan B és totalment indefinida, la condició que defineix P_B és buida, de manera que $P_B = P$, el grup d'ideals principals de F, i $h_B = h(F)$ coincideix amb el nombre de classes de F. Si a més B és racional, com que $h(\mathbb{Q}) = 1$:

Corol·lari 1.33. *El nombre de classes d'una àlgebra de quaternions racional i indefinida és 1. A més, tots els ordres maximals en una àlgebra de quaternions racional i indefinida són conjugats entre ells.*

CAPíTOL 2

Corbes de Shimura: interpretació modular

En aquest capítol introduïm les corbes de Shimura, seguint essencialment [**Jor81**]. En la primera secció definim la corba de Shimura X_D associada a una àlgebra de quaternions racional i indefinida B_D de discriminant D, i expliquem la seva interpretació en termes de mòduli per a superfícies abelianes amb multiplicació quaterniònica. La segona secció està dedicada a presentar el grup d'Atkin-Lehner de X_D, que és un grup d'involucions naturalment definides en X_D, i expliquem també la interpretació modular de l'acció d'aquestes involucions. Finalment, en la darrera secció donem algunes indicacions de com la noció de corba de Shimura es generalitza a dimensions superiors.

1. Corbes de Shimura i multiplicació quaterniònica

Sigui B_D una àlgebra de quaternions racional i indefinida de discriminant D, i sigui $\mathcal{O}_D \subseteq B_D$ un ordre maximal en B_D, que recordem que és únic llevat de conjugació pel Corol·lari 1.33. Fixem també un isomorfisme $B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R})$. Aleshores, mitjançant aquest isomorfisme tenim una inclusió natural del subgrup $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D^\times : \mathrm{n}(\gamma) = 1\} \subseteq \mathcal{O}_D$ d'unitats de norma 1 en $\mathcal{O}_D^\times$ en el subgrup $\mathrm{SL}_2(\mathbb{R}) \subseteq \mathrm{M}_2(\mathbb{R})$,

$$\mathcal{O}_D^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R}).$$

La imatge de $\mathcal{O}_D^1$ en $\mathrm{PSL}_2(\mathbb{R})$ és un subgrup discret que actua de manera discontínua en el semiplà de Poincaré $\mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Per tant, podem considerar la superfície de Riemann $V_D = \mathfrak{H} \setminus \mathcal{O}_D^1$. Com que tots els ordres maximals de B_D són conjugats, notem que la classe d'isomorfisme de V_D no depèn de l'elecció de $\mathcal{O}_D$, i tampoc de l'isomorfisme fixat $B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R})$, en virtud del Teorema de Noether-Skolem (vegeu [**Pie82**, §12.6]). A més:

Teorema 2.1 (Poincaré)**.** *La superfície de Riemann V_D és compacta si, i només si, $B_D \not\simeq \mathrm{M}_2(\mathbb{R})$.*

En altres paraules, V_D és compacta si, i només si, B_D és de divisió. Per a l'àlgebra de matrius $\mathrm{M}_2(\mathbb{R})$, recuperem el cas de les corbes modulars clàssiques, les quals es poden compactificar afegint noves singularitats, les anomenades *punxes* (en anglès, *cusps*). El fet que V_D sigui compacta per a $D > 1$ fa que l'estudi de l'aritmètica de les corbes de Shimura sigui significativament més complicat, ja que en el cas clàssic les *punxes* codifiquen molta informació aritmètica sobre les corbes modulars. A partir d'ara, doncs, considerarem que l'àlgebra B_D és de divisió. En aquest cas, el grup $\mathcal{O}_D^1$ d'unitats de norma 1 és un subgrup discret compacte de $\mathrm{PSL}_2(\mathbb{R})$. El gènere de la superfície de

Riemann V_D ve donat per la següent expressió (vegeu [**Vig80**]):

$$g(V_D) = 1 + \frac{1}{12}\prod_{p|D}(p-1) - \frac{1}{4}\prod_{p|D}(1-(\frac{\mathbb{Q}(\sqrt{-1})}{p})) - \frac{1}{3}\prod_{p|D}(1-(\frac{\mathbb{Q}(\sqrt{-3})}{p})),$$

on per a un cos quadràtic K posem

$$(\frac{K}{p}) = \begin{cases} -1 & \text{si } p \text{ és inert en } K, \\ 0 & \text{si } p \text{ ramifica en } K, \\ 1 & \text{si } p \text{ descomposa en } K. \end{cases}$$

Shimura va provar que les superfícies de Riemann V_D, construïdes mitjançant grups Fuchsians aritmètics de primera espècie, tenen de fet una interpretació modular. Per descriure-la, necessitem introduir la noció de multiplicació quaterniònica per a superfícies abelianes.

Comencem fixant una tripleta $(B_D, \mathcal{O}_D, \varrho)$, on B_D és una àlgebra de quaternions racional i indefinida, $\mathcal{O}_D \subseteq B_D$ és un ordre maximal, i $b \mapsto b^\varrho$ és una (anti-)involució positiva en B_D. Gràcies al Teorema de Noether-Skolem, la involució ϱ és conjugada de la involució canònica $b \mapsto \bar{b}$. Per tant, existeix un element $\mu \in B_D^\times$ tal que $b^\varrho = \mu^{-1}\bar{b}\mu$ per a tot $b \in B_D$. I de fet, la positivitat de ϱ implica (vegeu [**Rot03**]) que $\mathrm{tr}(\mu) = 0$ i $\mathrm{n}(\mu) > 0$, per tant μ satisfà $\mu^2 + \delta = 0$ per algun $\delta \in \mathbb{Q}^\times$, $\delta > 0$. Així, sovint denotarem $\varrho = \varrho_\mu$ si volem fer referència a l'element μ, que està determinat llevat multiplicació per elements de $\mathbb{Q}^\times$. Notem també que podem suposar que $\mu \in \mathcal{O}_D$, és a dir, que $\delta \in \mathbb{Z}_{>0}$. Un cop fixada la tripleta $(B_D, \mathcal{O}_D, \varrho)$:

Definició 2.2. *Una* superfície abeliana amb multiplicació quaterniònica *(o* amb QM*, per abreviar) per* $(B_D, \mathcal{O}_D, \varrho)$ *és una tripleta* $(A, \iota, \mathcal{L})$ *on:*

- A *és una superfície abeliana,*
- $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ *és un monomorfisme d'àlgebres,*
- $\mathcal{L}$ *és una polarització feble en* A *tal que la involució de Rosati* $\dagger$ *associada a* $\mathcal{L}$ *satisfà* $\iota(b)^\dagger = \iota(b^\varrho)$ *per a tot* $b \in B_D$*.*

Recordem que una polarització feble en A és una classe d'equivalència racional de polaritzacions en A, on dues polaritzacions $\mathcal{L}_1$ i $\mathcal{L}_2$ són racionalment equivalents si existeixen enters positius m, n tals que $m\mathcal{L}_1 = n\mathcal{L}_2$. Observem que dues polaritzacions racionalment equivalents indueixen la mateixa involució de Rosati.

Amb aquestes notacions, suposem que tenim dues superfícies abelianes $(A, \iota, \mathcal{L})$ i $(A', \iota', \mathcal{L}')$ amb QM (respecte a $(B_D, \mathcal{O}_D, \varrho)$). Aleshores, un morfisme $\varphi : (A, \iota, \mathcal{L}) \to (A', \iota', \mathcal{L}')$ és simplement un morfisme $\varphi : A \to A'$ entre les superfícies abelianes subjacents tal que $\mathcal{L} = \varphi^*(\mathcal{L}')$ i $\varphi \circ \iota(\beta) = \iota'(\beta) \circ \varphi$ per a tot $\beta \in \mathcal{O}_D$. Aquesta darrrera condició es pot reescriure demanant que el diagrama

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ {\scriptstyle \iota(\beta)}\downarrow & & \downarrow{\scriptstyle \iota'(\beta)} \\ A & \xrightarrow{\varphi} & A' \end{array}$$

commuti per a tot $\beta \in \mathcal{O}_D$.

Aleshores, el que provà Shimura (vegeu [**Shi63**], [**Shi67**]) és que V_D és la solució al problema de mòduli (groller) sobre $\mathbb{Q}$ de classificar les classes d'isomorfisme de superfícies abelianes $(A, \iota, \mathcal{L})$ amb QM per $(B_D, \mathcal{O}_D, \varrho)$. A més, Shimura va demostrar que la superfície de Riemann V_D admet un model sobre $\mathbb{Q}$. És a dir, va construir un model $X_D/\mathbb{Q}$ de manera que V_D s'identifica canònicament amb els punts complexos de X_D, $X_D(\mathbb{C}) \simeq V_D$.

Definició 2.3. *Anomenarem* corba de Shimura associada a B_D *a la corba algebraica definida pel model $X_D/\mathbb{Q}$ construït per Shimura.*

Com que hem suposat que B_D és de divisió, X_D és doncs una corba alebraica projectiva. Encara des d'un punt de vista complex, cal remarcar que Shimura donà també una aplicació d'uniformització per a $X_D(\mathbb{C})$, que ve descrita per:

$$\begin{aligned} \mathfrak{H} &\longrightarrow X_D(\mathbb{C}) \\ \tau &\longmapsto P_\tau = [(A_\tau, \iota_\tau, \mathcal{L}_\tau)] \end{aligned}$$

on denotem per $[(A_\tau, \iota_\tau, \mathcal{L}_\tau)]$ la classe d'isomorfisme de la superfície abeliana amb QM $(A_\tau, \iota_\tau, \mathcal{L}_\tau)$ donada per

- $A_\tau = \mathbb{C}^2/\mathcal{O}_D \cdot v_\tau$ amb $v_\tau = (\tau, 1)^t$,
- $\iota_\tau : \mathcal{O}_D \hookrightarrow \mathrm{End}(A_\tau)$ l'aplicació natural,
- $\mathcal{L}_\tau$ la polarització feble induïda per la forma de Riemann E_τ definida per

$$E_\tau(x \cdot v_\tau, y \cdot v_\tau) = \mathrm{tr}(\mu x \bar{y}), \quad \text{per a tot } x, y \in \mathcal{O}_D.$$

L'aplicació anterior satisfà que donats $\tau, \tau' \in \mathfrak{H}$ qualssevol, aleshores $P_\tau = P_{\tau'}$ si, i només si, τ i τ' són equivalents per l'acció de $\mathcal{O}_D^1$ en $\mathfrak{H}$. Per tant, l'aplicació d'uniformització de Shimura realitza l'isomorfisme $V_D = \mathcal{O}_D^1 \setminus \mathfrak{H} \simeq X_D(\mathbb{C})$.

Respecte a la interpretació modular de X_D, volem emfatitzar el fet que la polarització feble $\mathcal{L}$ en la definició d'una superfície abeliana amb QM queda completament determinada per $(B_D, \mathcal{O}_D, \varrho)$. Concretament, tenim el següent resultat degut a Milne (vegeu [**Mil79**]):

Proposició 2.4 (Milne)**.** *Suposem que $(B_D, \mathcal{O}_D, \varrho)$ és una tripleta com abans, i sigui A una superfície abeliana equipada amb un monomorfisme d'anells $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$. Aleshores, existeix una única polarització feble $\mathcal{L}$ en A tal que $(A, \iota, \mathcal{L})$ és una superfície abeliana amb QM respecte a $(B_D, \mathcal{O}_D, \varrho)$.*

Per tant, en el que segueix considerarem les superfícies abelianes amb QM simplement com parells $(A, \iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A))$, i farem esment de la polarització feble $\mathcal{L}$ únicament quan sigui rellevant.

Per acabar la secció, sigu k un cos de característica zero, i fixem una clausura algebraica $\bar{k}$ de k. Necessitem les següents definicions per traslladar la interpretació modular de X_D a l'estudi de punts k-racionals de X_D:

Definició 2.5. *Suposem que $(A,\iota)/\bar{k}$ és una superfície abeliana amb QM per $(B_D,\mathcal{O}_D,\varrho)$. Aleshores, el* cos de mòduli *(A,ι) és el mínim cos $k\subseteq k_{(A,\iota)}\subseteq\bar{k}$ tal que el parell (A,ι) és isomorf a ${}^{\sigma}(A,\iota)$ per a tot $\sigma\in\mathrm{Gal}\,(\bar{k}/k_{(A,\iota)})$. En altres paraules, $k_{(A,\iota)}=\bar{k}^H$ és el cos fix per*

$$H=\{\sigma\in\mathrm{Gal}\,(\bar{k}/k):{}^{\sigma}(A,\iota)\simeq(A,\iota)\}\subseteq\mathrm{Gal}\,(\bar{k}/k).$$

Direm que (A,ι) admet un model racional *sobre k si existeix una superfície abeliana $(A',\iota')/k$ amb QM per $(B_D,\mathcal{O}_D,\varrho)$ tal que $(A'\times\bar{k},\iota'\times\bar{k})\simeq(A,\iota)$. En tal cas, direm que k és* un cos de definició *per (A,ι).*

Clarament, el cos de mòduli d'un parell $(A,\iota)/\bar{k}$ és únic, i està contingut en qualsevol cos de definició per (A,ι).

Com que X_D està definida sobre $\mathbb{Q}$ i k és un cos de característica zero ($k\supseteq\mathbb{Q}$), té sentit considerar el conjunt $X_D(k)$ de punts k-racionals de X_D. És a dir, el conjunt de punts de X_D amb coordenades a k. Per la interpretació modular de X_D, un punt $P\in X_D(k)$ es correspon amb la classe d'isomorfisme d'una superfície abeliana $(A,\iota)/\bar{k}$ amb QM per $(B_D,\mathcal{O}_D,\varrho)$ i cos de mòduli $k_P=k_{(A,\iota)}$ contingut en k. Així doncs, i més en general, per a qualsevol extensió de cossos $k\subseteq K\subseteq\bar{k}$, tenim que

$$X_D(K)=\{P\in X_D(\bar{k}):k_P\subseteq K\}.$$

En particular, si $(A,\iota)/\bar{k}$ admet un model racional sobre K aleshores $P=[(A,\iota)]\in X_D(K)$, però el recíproc no és cert en general. El problema d'estudiar l'obstrucció per a una superfície abeliana (A,ι) amb QM a admetre un model racional sobre el seu cos de mòduli va ser estudiat i resolt per Jordan a [**Jor86**] (vegeu el Teorema 3.2 al següent capítol): una superfície abeliana (A,ι) amb QM parametritzada per un punt $P\in X_D(K)$ admet un model racional sobre K si, i només si, K escindeix B_D.

Exemple 2.6. Sigui B_6 l'àlgebra de quaternions racional (indefinida i de divisió) de discriminant 6. A. Kurihara va provar que el model canònic de X_D sobre $\mathbb{Q}$ ve descrit per l'equació afí $x^2+y^2+3=0$. Directament d'aquesta equació veiem que $(\sqrt{-7},2)\in X_6(\mathbb{Q}(\sqrt{-7}))$. Això implica l'existència d'una superfície abeliana (A,ι) amb multiplicació quaterniònica per B_6 amb cos de mòduli $\mathbb{Q}(\sqrt{-7})$. Però, d'acord amb el resultat de Jordan, aquesta superfície abeliana no pot admetre un model racional sobre $\mathbb{Q}(\sqrt{-7})$, ja que $\mathbb{Q}(\sqrt{-7})$ no escindeix B_6.

2. El grup d'Atkin-Lehner

Un cop definida la corba de Shimura X_D associada a una àlgebra de quaternions B_D, així com la seva interpretació modular, en aquesta secció presentem un grup d'involucions en X_D que vénen

definides de manera natural a partir de la construcció de la superfície de Riemann V_D. Són les anomenades involucions d'Atkin-Lehner.

Mitjançant la inclusió $B_D \hookrightarrow B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$, el grup multiplicatiu $B_{D,+}^{\times}$ d'elements invertibles de norma reduïda positiva actua en $\mathfrak{H}$ per transformacions de Moebius. I llavors, és immediat comprovar que l'acció d'un element $\alpha \in B_{D,+}^{\times}$ indueix una acció en $V_D = \mathcal{O}_D^1 \setminus \mathfrak{H}$ si, i només si, $\alpha \in \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)$, on

$$\mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1) = \{\beta \in B_{D,+}^{\times} : \beta^{-1}\mathcal{O}_D\beta = \mathcal{O}_D\}$$

és el normalitzador de $\mathcal{O}_D^1$ en $B_{D,+}^{\times}$.

És clar que $\mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)$ sempre conté els elements de $\mathbb{Q}^{\times}\mathcal{O}_D^1$, que indueixen l'automorfisme trivial en $V_D = \mathcal{O}_D^1 \setminus \mathfrak{H}$ de manera que és natural considerar el grup quocient

$$\mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1.$$

És un resultat ben conegut que $\mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1 \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$, on $2r$ és el nombre de factors primers de D (vegeu per exemple [**Jor81**, Proposition 1.2.4]). Tractant-se d'un 2-grup, els seus elements són doncs involucions de $V_D = \mathcal{O}_D^1 \setminus \mathfrak{H}$. A més, un sistema complet de representants per a $\mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1$ ve donat per qualsevol conjunt $\{\alpha_d\}_{d|D}$, format per un element $\alpha_d \in \mathcal{O}_D$ de norma reduïda d per a cada divisor positiu d de D. Seguint les notacions habituals, si $m|D$, denotarem per ω_m la involució de V_D induïda per l'acció de qualsevol element $\alpha_m \in \mathcal{O}_D$ de norma reduïda m en $\mathfrak{H}$. Aquestes involucions formen un grup $W_D \subseteq \mathrm{Aut}(V_D)$. Si $m, m'|D$, aleshores es pot comprovar que $\omega_m \cdot \omega_{m'} = \omega_{mm'/(m,m')^2}$, la qual cosa prova que W_D està generat per les involucions w_p, on p recorre els factors primers de D.

L'acció de les involucions ω_m admet una interpretació modular en termes de superfícies abelianes amb QM. Considerem la superfície abeliana $(A, \iota, \mathcal{L})_\tau = (A_\tau, \iota_\tau, \mathcal{L}_\tau)$, per algun $\tau \in \mathfrak{H}$. Aleshores, si la involució ω_m ve representada per un element $\alpha_m \in \mathcal{O}_D$ de norma reduïda m, fent servir la uniformització de Shimura, ω_m envia la classe d'isomorfisme $P_\tau = [(A, \iota, \mathcal{L})_\tau]$ a $P_{\alpha_m\tau} = [(A, \iota, \mathcal{L})_{\alpha_m\tau}]$. Ara bé, observem que la multiplicació per α_m^{-1} indueix un isomorfisme

$$g : A_{\alpha_m\tau} = \mathbb{C}^2/\mathcal{O}_D \cdot v_{\alpha_m\tau} \simeq \mathbb{C}^2/\mathcal{O}_D\alpha_m \cdot v_\tau \xrightarrow{\alpha_m^{-1}} \mathbb{C}^2/\mathcal{O}_D \cdot v_\tau = A_\tau.$$

A més, és senzill comprovar que aquest isomorfisme satisfà $g \circ \iota_{\alpha_m\tau}(\beta) = \iota_\tau(\alpha_m^{-1}\beta\alpha_m) \circ g$ per a tot $\beta \in \mathcal{O}_D$. Més en general, per a $a \in \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)$, denotarem per $\iota_a : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ el monomorfisme donat per $\iota_a(\beta) = \iota(a^{-1}\beta a)$. Per la Proposició 2.4, per a cada $a \in \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)$ existeix una única polarització feble $\mathcal{L}_a$ tal que $(A, \iota_a, \mathcal{L}_a)$ és una superfície abeliana amb QM. De fet, es comprova que $\mathcal{L}_a = a^*(\mathcal{L})$ (vegeu [**Jor81**, p. 12]).

Per tant, l'acció de les involucions modulars ω_m ve descrita de la següent manera:

Proposició 2.7. *Sigui $\alpha_m \in \mathcal{O}_D$ un element de norma m, per algun divisor positiu m de D. Aleshores, si $(A, \iota, \mathcal{L})$ és una superfície abeliana amb QM i ω_m és la involució induïda per α_m, es*

té

$$\omega_m([(A,\iota,\mathcal{L})]) = [(A,\iota_{\alpha_m},\alpha_m^*(\mathcal{L}))].$$

Mitjançant la interpretació modular, veiem doncs que el grup W_D actua per involucions en la corba de Shimura X_D. A més, com que la solució a un problema de mòduli és única, resulta que les involucions $\omega_m \in W_D$ són racionals:

Definició 2.8. *W_D és el* grup d'Atkin-Lehner *de X_D, i es té $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$. Els elements de W_D s'anomenen* involucions d'Atkin-Lehner*.*

Seguint la notació tradicional, sovint identificarem $\omega_m \in W_D$ amb un representant seu en $\mathrm{N}_{B_{D,+}^\times}(\mathcal{O}_D^1) \cap \mathcal{O}_D$ de norma m.

Exemple 2.9. A [**BFGR06**, Table 1] es poden trobar equacions explícites per algunes corbes de Shimura, i es donen també les involucions d'Atkin-Lehner en termes d'aquestes equacions. Per exemple, si X_6 és la corba de Shimura definida per l'àlgebra de quaternions racional B_6 de discriminant 6, hem vist a l'Exemple 2.6 que una equació afí per a X_6 és

$$x^2 + y^2 + 3 = 0.$$

En termes d'aquesta equació, $\omega_2(x,y) = (-x,-y)$ i $\omega_3(x,y) = (x,-y)$. Per tant, $\omega_6(x,y) = \omega_2 \cdot \omega_3(x,y) = (-x,y)$.

3. Varietats de Shimura de dimensió superior

Per tancar el capítol, volem presentar breument com les corbes de Shimura admeten anàlegs en dimensió superior. En aquesta secció, F denotarà un cos de nombres totalment real de grau $n = [F:\mathbb{Q}]$, i escriurem R_F per denotar el seu anell d'enters.

Considerem una àlgebra de quaternions B sobre F totalment indefinida. En particular, tenim que $B \otimes_F F_v \simeq \mathrm{M}_2(F_v)$ per a tota plaça arquimediana v de F (que es corresponen amb els diferents n embeddings reals $F \hookrightarrow \mathbb{R}$ de F). Denotarem el discriminant reduït de B per $\mathfrak{D} = \mathfrak{p}_1 \cdots \mathfrak{p}_{2r}$, on els $\mathfrak{p}_i$ són ideals primers de R_F diferents dos a dos.

Fixem ara una tripleta $(\mathcal{O},\mathcal{I},\varrho)$, on $\mathcal{O}$ és un ordre maximal de B, $\mathcal{I}$ és un ideal per l'esquerra de $\mathcal{O}$ (o millor la seva classe en $\mathrm{Pic}_\ell(\mathcal{O})$) i ϱ és una (anti-)involució positiva en B.

Remarca 2.10. De nou, pel Teorema de Noether-Skolem Theorem, la involució ϱ és conjugada de la involució canònica en B, que denotem per $\beta \mapsto \bar{\beta}$. Per tant, existeix un element $\mu \in B^\times$ tal que $\beta^\varrho = \mu^{-1}\bar{\beta}\mu$ per a tot $\beta \in B$. A més, la positivitat de ϱ implica (vegeu [**Rot03**]) que $\mathrm{tr}(\mu) = 0$ i $\mathrm{n}(\mu) \in F_+^\times$, de manera que μ satisfà una equació de la forma $\mu^2 + \delta = 0$ per algun $\delta \in F_+^\times$. Com aquest element μ està determinat llevat de multiplicació per unitats de F, podem denotar ϱ per ϱ_μ.

Un cop fixada la tripleta $(\mathcal{O},\mathcal{I},\varrho)$:

Definició 2.11. *Una* varietat abeliana polaritzada amb multiplicació quaterniònica per $(\mathcal{O}, \mathcal{I}, \varrho)$ *(o simplement amb QM per $\mathcal{O}$, per abreviar) és una tripleta $(A, \iota, \mathcal{L})$ on*

- *A és una varietat abeliana de dimensió $g = 2n$,*
- *$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ és un monomorfisme d'anells tal que $\mathrm{H}_1(A, \mathbb{Z}) \simeq \mathcal{I}$ com a $\mathcal{O}$-mòduls,*
- *$\mathcal{L}$ és una polarització primitiva en A tal que la involució de Rosati $\dagger$ definida per $\mathcal{L}$ en $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ coincideix amb ϱ en $\iota(\mathcal{O})$, és a dir $\iota(\beta)^\dagger = \iota(\beta^\varrho)$ per a tot $\beta \in \mathcal{O}$.*

Amb aquesta definició, un isomorfisme entre dues varietats abelianes polaritzades $(A_1, \iota_1, \mathcal{L}_1)$ i $(A_2, \iota_2, \mathcal{L}_2)$ amb QM per $\mathcal{O}$ és simplement un isomorfisme $\varphi : A_1 \to A_2$ entre les varietats abelianes subjacents tal que $\varphi \circ \iota_1(\beta) = \iota_2(\beta) \circ \varphi$ per a tot $\beta \in \mathcal{O}$ i $\varphi^*(\mathcal{L}_2) = \mathcal{L}_1$.

Aleshores, associat a la tripleta $(\mathcal{O}, \mathcal{I}, \varrho)$ tenim el problema de mòduli sobre $\mathbb{Q}$ de classificar les classes d'isomorfisme de varietats abelianes primitivament polaritzades amb QM per $\mathcal{O}$. Pel treball de Shimura, el functor corresponent a aquest problema de mòduli ve representat (*grollerament*) per un esquema quasi-projectiu reduït i irreductible $X_B/\mathbb{Q} = X_{(\mathcal{O},\mathcal{I},\varrho)}/\mathbb{Q}$ sobre $\mathbb{Q}$ de dimensió n. A més, si B és de divisió aleshores X_B és una varietat completa (vegeu [**Shi63**], [**Shi67**]).

Definició 2.12. *$X_{(\mathcal{O},\mathcal{I},\varrho)}$ és la* varietat de Shimura *definida per la tripleta $(\mathcal{O}, \mathcal{I}, \varrho)$. Si $(\mathcal{O}, \mathcal{I}, \varrho)$ és clara pel context o no és rellevant, escriurem simplement X_B per denotar el seu model sobre $\mathbb{Q}$ donat per Shimura, i direm que és la varietat de Shimura definida per B.*

Remarca 2.13. Quan prenem l'àlgebra de matrius $B \simeq \mathrm{M}_2(F)$, les varietats X_B que obtenim són les *varietats modulars de Hilbert-Blumenthal* clàssiques. Aquestes no són completes, però, com en el cas 1-dimensional de les corbes modulars, poden construir-se certes compactificacions al preu de produir noves singularitats (les *punxes*).

D'altra banda, si B és de divisió, com ja hem dit les varietats X_B són projectives. Encara que això pugui semblar un avantatge, aquest fet fa que l'estudi de l'aritmètica de X_B sigui significativament més complicat que en el cas clàssic, ja que en el cas de les varietats modulars de Hilbert-Blumenthal molta informació aritmètica està codificada en les punxes.

Com a varietats complexes, les varietats X_B es poden descriure com a quocients de dominis simètrics per l'acció de certs subgrups de congruència, i pel treball de W. L. Baily i A. Borel ([**BB66**]), esdevenen varietats algebraiques complexes quasi-projectives. Concretament, la varietat complexa $X_B(\mathbb{C})$ es pot construir com el quocient de n còpies del semiplà de Poincaré $\mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ per l'acció discontínua d'un grup discret. De fet, com que B és totalment indefinida, podem escollir un embedding $B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \oplus \overset{n)}{\cdots} \oplus \mathrm{M}_2(\mathbb{R})$, i el grup $\mathcal{O}^1 = \{\gamma \in \mathcal{O}^\times : \mathrm{n}(\gamma) = 1\}$ d'unitats de norma 1 en $\mathcal{O}$ es pot identificar amb la seva imatge $\Gamma_B \subseteq \mathrm{M}_2(\mathbb{R})^n$ per aquest embedding, que és un subgrup discret de $\mathrm{SL}_2(\mathbb{R})^n$. Així, un element $\gamma = (\gamma_1, \ldots, \gamma_n) \in \Gamma_B$

actua en el producte cartesià $\mathfrak{H}^n$ per transformacions de Moebius:

$$\gamma \cdot (\tau_1, \ldots, \tau_n)^t = \left(\frac{a_1\tau_1 + b_1}{c_1\tau_1 + d_1}, \ldots, \frac{a_n\tau_n + b_n}{c_n\tau_n + d_n} \right)^t, \quad \text{on } \gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Aleshores,

$$X_B(\mathbb{C}) \simeq \Gamma_B \setminus \mathfrak{H}^n. \tag{3}$$

Des d'aquest punt de vista analític, també es pot veure que el quocient $\Gamma_B \setminus \mathfrak{H}^n$ és compacte quan B és de divisió (vegeu [**Kat92**, Theorem 5.4.1], [**BHC62**]).

Per ser X_B una solució a l'anterior problema de mòduli, els punts complexos de X_B (o, equivalentment, les Γ_B-òrbites de $\mathfrak{H}^n$) admeten la següent interpretació:

$$X_B(\mathbb{C}) = \{(A, \iota, \mathcal{L})/\mathbb{C} \text{ varietat abeliana amb QM per } \mathcal{O}\}_{/\simeq}.$$

De nou, aquesta interpretació de mòduli admet una aplicació d'uniformització

$$\begin{array}{rcl} \mathfrak{H}^n & \longrightarrow & X_B(\mathbb{C}) \\ \tau = (\tau_1, \ldots, \tau_n) & \longmapsto & [(A_\tau, \iota_\tau, \mathcal{L}_\tau)], \end{array}$$

per a la descripció de la qual referim el lector a [**Rot03**].

Per al cas del conjunt $X_B(K)$, on $K/\mathbb{Q}$ és un cos de nombres, la interpretació en termes de mòduli és anàloga a la que hem exposat anteriorment en el cas de corbes de Shimura. Recordem que en aquesta interpretació juguen un paper fonamental els conceptes de *cos de mòduli* i *cos de definició* d'una varietat abeliana amb QM, que es generalitzen sense dificultat per a aquest cas a partir de la Definició 2.5.

Pel que fa a la generalització del grup d'Atkin-Lehner al cas de varietats de Shimura de dimensió superior, referim el lector interessat a [**Rot04**], on s'estudien certs morfismes naturals de varietats de Shimura a varietats modulars de Hilbert-Blumenthal i espais de mòduli de varietats abelianes polaritzades. L'estudi d'aquests morfismes, que consisteixen en 'oblidar' la multiplicació quaterniònica, donen lloc a una interpretació modular del quocient d'una varietat de Shimura per certs subgrups del grup d'involucions d'Atkin-Lehner.

CAPíTOL 3

Els treballs de Jordan i Skorobogatov

Aquest capítol està dedicat a exposar els treballs de Jordan [**Jor86**] i Skorobogatov [**Sko05**] sobre l'existència de punts racionals sobre cossos quadràtics imaginaris en corbes de Shimura. Els resultats principals per a l'objectiu d'aquest treball són el Teorema 3.5 i el Teorema 3.25.

De cara als capítols posteriors, els subgrups canònics de torsió introduïts en la segona secció, així com els caràcters d'isogènia associats, jugaran un paper fonamental. També seran dos ingredients essencials el recobridor de Shimura $Z_{D,p} \to X_D$ associat a un factor primer p de D i el X_D-torsor $f_p : Y_{D,p} \to X_D$ introduït per Skorobogatov, que es presenten en les seccions tercera i quarta, respectivament.

1. Punts racionals en corbes de Shimura

Sigui B_D una àlgebra de quaternions racional i indefinida de discriminant reduït D, i denotem per $X_D = X_D/\mathbb{Q}$ el model canònic sobre $\mathbb{Q}$ de la corba de Shimura definida per una tripleta prèviament fixada $(B_D, \mathcal{O}_D, \varrho)$, com en el capítol anterior. Per a l'estudi dels punts racionals en la corba X_D sobre certs cossos, és de gran importància el següent resultat clàssic degut a Shimura (vegeu [**Shi75**, Theorem 0]):

Teorema 3.1 (Shimura)**.** *Si l'àlgebra de quaternions racional i indefinida B_D és de divisió, aleshores la corba de Shimura X_D no té punts reals. És a dir, si $D > 1$ aleshores $X_D(\mathbb{R}) = \emptyset$.*

De fet, Shimura provà aquest resultat també per varietats de Shimura de dimensió superior. Com a conseqüència d'aquest teorema, tenim que X_D no té punts K-racionals per a cap cos de nombres K totalment real. En particular, $X_D(\mathbb{Q}) = \emptyset$.

Jordan va estudiar a [**Jor86**] el problema d'identificar els cossos de nombres K tals que $X_D(K) = \emptyset$, amb especial interès en el cas dels cossos quadràtics imaginaris (el següent pas després del Teorema 3.1). En altres paraules, Jordan cercava una descripció del conjunt

$$\mathrm{D} = \left\{ (B_D, K) \;\middle|\; \begin{array}{l} B_D \text{ àlgebra de quaternions racional,} \\ \text{indefinida i de divisió,} \\ K \text{ cos de nombres, } X_D(K) = \emptyset \end{array} \right\}.$$

Aquest és clarament un problema sobre l'aritmètica de les corbes de Shimura, estretament relacionat amb l'estudi del principi local-global (o principi de Hasse) en aquestes corbes. De fet,

un subconjunt obvi de D és

$$\mathrm{D}_{\mathrm{local}} = \left\{ (B_D, K) \in \mathrm{D} \;\middle|\; \begin{array}{l} \text{existeix una plaça } v \text{ de } K \text{ tal que} \\ X_D(K_v) = \emptyset, \text{ on } K_v \text{ és la compleció} \\ \text{de } K \text{ respecte a } v \end{array} \right\}.$$

El Teorema 3.1 juntament amb els resultats de Jordan i Livné a [**JL85**] (vegeu també [**Jor86**, Theorem 0]) per al cas no arquimedià determinen el conjunt $\mathrm{D}_{\mathrm{local}}$, de manera que Jordan centra el seu estudi en el conjunt $\mathrm{D}_{\mathrm{global}} = \mathrm{D} \setminus \mathrm{D}_{\mathrm{local}}$, que es pot considerar com una mesura de l'error del principi de Hasse en X_D.

Com ja hem indicat abans, la noció de cos de mòduli juga un paper important en l'estudi dels punts racionals en X_D. Concretament, si k és un cos de característica zero i $P \in X_D(k)$, aleshores podem representar P per un parell $(A, \iota)/\bar{k}$ tal que el seu cos de mòduli k_P està contingut en k, però que no necessàriament admet un model racional sobre k. En aquesta direcció, un dels principals resultats en [**Jor86**] és la següent caracterització de quan una superfície abeliana amb multiplicació quaterniònica admet un model racional sobre el seu cos de mòduli:

Teorema 3.2 (Jordan)**.** *Sigui k un cos de característica zero, i (A, ι) una superfície abliana amb QM parametritzada per un punt $P \in X_D(k)$, de manera que el cos de mòduli k_P de (A, ι) està contingut en k. Aleshores, (A, ι) admet un model racional sobre k si, i només si, k escindeix B_D.*

La necessitat de la condició pot explicar-se de manera breu: si (A', ι') és un model racional sobre k per (A, ι), aleshores l'acció de $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ en l'espai de 1-formes holomorfes dóna lloc a un embedding $B_D \hookrightarrow \mathrm{End}_k(\mathrm{H}^0(A', \Omega^1_{/k})) \simeq \mathrm{M}_2(k)$, i per tant k escindeix B_D. Per al recíproc, Jordan utilitza la descomposició de l'espai cotangent $\mathrm{H}^0(A, \Omega^1_{/k})$ induïda pel fet que k escindeix B_D, i un resultat clàssic de Shimura (vegeu [**Jor86**, §1]).

Un cop el Teorema 3.2 queda establert, el problema de decidir si un parell donat (B_D, K) pertany a D es converteix en un problema sobre l'aritmètica de les superfícies abelianes amb QM per B_D. A més, del mateix Teorema 3.2 sorgeixen dos casos clarament diferenciats per tractar:

(1) K escindeix B_D,
(2) K no escindeix B_D.

En el segon cas, $(B_D, K) \notin \mathrm{D}$ si, i només si, existeix una superfície abeliana amb QM (A, ι) amb cos de mòduli contingut en K, però que no admet un model racional sobre K. Suposem doncs que K no escindeix B_D. Seguint l'argument en [**Jor86**, p. 93], usant el Teorema 3.1 i els resultats de Jordan i Livné [**JL85**] resulta que llavors $(B_D, K) \in \mathrm{D}_{\mathrm{local}}$, llevat que o bé $D = 2p$ amb $p \equiv 1 \mod 4$ o bé $D = 2q_1 \cdots q_{2r-1}$ per alguns primers q_i satisfent $q_i \equiv 3 \mod 4$, $1 \leq i \leq 2r-1$. D'acord amb la terminologia introduïda per Jordan, direm que (B_D, K) és un *parell excepcional* si K no escindeix B_D i $(B_D, K) \notin \mathrm{D}_{\mathrm{local}}$. Fins ara, aquests parells semblen haver estat inaccessibles en la literatura existent. Tanmateix, el resultat principal que presentem en aquest treball permet

produir exemples de parells excepcionals (vegeu Teorema 5.1). Cal remarcar que aquells parells excepcionals (B_D, K) per als quals $X_D(K) = \emptyset$ són contraexemples al principi de Hasse sobre K.

Pel que fa al primer cas, $(B_D, K) \notin$ D si, i només si, existeix una superfície abeliana amb QM (A, ι) definida sobre K. L'estratègia seguida per Jordan en aquest cas consisteix en donar condicions necessàries per a l'existència de superfícies abelianes amb QM definides sobre el cos K. Aleshores, sempre que es pugui provar la impossibilitat de satisfer aquestes condicions se seguirà que $X_D(K) = \emptyset$, assumint que K escindeix B_D. En aquesta direcció, el següent resultat va ser provat en [**Jor86**]:

Teorema 3.3 (Jordan)**.** *Si K és un cos quadràtic imaginari amb nombre de classes més gran que 1, aleshores només existeix un nombre finit d'àlgebres de quaternions racionals i indefinides B_D (llevat d'isomorfisme) tals que K escindeix B_D i $X_D(K) \neq \emptyset$.*

Remarca 3.4. Per un resultat de Shimura, el cas de nombre de classes 1 és més senzill: si K és un cos quadràtic imaginari amb nombre de classes 1 i K escindeix B_D, aleshores $X_D(K) \neq \emptyset$.

Per a la prova del Teorema 3.3, un dels punts clau és entendre els subgrups canònics de torsió C_p d'una superfície abeliana amb QM (A, ι) associats als factors primers p de D, així com els caràcters d'isogènia corresponents. Aquests objectes ja van ser introduïts en la tesi de Jordan ([**Jor81**]), i algunes de les seves propietats s'estableixen usant la teoria de superfícies abelianes amb QM sobre cossos finits i sobre cossos locals (vegeu les seccions 2 i 3 de [**Jor86**]). A partir d'aquestes propietats, Jordan prova que la funció L d'una superfície abeliana amb QM satisfà certes congruències que condueixen finalment a la prova del Teorema 3.3. Val la pena esmentar també que la prova d'aquest resultat deguda a Jordan fou inspirada en el valuós treball de B. Mazur en [**Maz78**].

Hi ha una altra aplicació del treball de Jordan que mostra explícitament com l'aritmètica de B_D pot decidir si $X_D(K)$ és buit o no, que és en la que estem més interessats en aquest treball. Usant les notacions de [**Sko05**], per a un nombre primer q, sigui $P(q)$ el conjunt finit de tots els factors primers dels enters no nuls en el conjunt $\{a, a \pm q, a \pm 2q, a^2 - 3q^2\}_{|a| \leq 2q}$. Per exemple, tenim $P(2) = \{2, 3, 5, 7, 11\}$. D'altra banda, si $q \neq 2$, definim $\mathcal{B}(q)$ com el conjunt d'àlgebres de quaternions racionals i indefinides que no són escindides per $\mathbb{Q}(\sqrt{-q})$, i definim també $\mathcal{B}(2)$ com el conjunt d'àlgebres de quaternions racionals i indefinides que no són escindides ni per $\mathbb{Q}(\sqrt{-2})$ ni per $\mathbb{Q}(\sqrt{-1})$. Finalment, definim $\mathcal{C}(q) \subset \mathcal{B}(q)$ com el conjunt d'àlgebres en $\mathcal{B}(q)$ amb discriminant reduït divisible per algun primer $p \notin P(q)$, i observem que $\mathcal{B}(q) \setminus \mathcal{C}(q)$ és finit. Aleshores, el següent resultat és [**Jor86**, Theorem 6.3]:

Teorema 3.5 (Jordan)**.** *Sigui q un nombre primer. Si K és un cos quadràtic imaginari en el qual q ramifica i $B_D \in \mathcal{C}(q)$ és escindida per K, aleshores $X_D(K) = \emptyset$.*

Exemple 3.6. Considerem l'àlgebra de quaternions racional B_{39} de discriminant 39. D'una banda, es té que ni $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-2})$ escindeixen B_{39}, i d'altra banda $\mathbb{Q}(\sqrt{-13})$ escindeix B_{39}. Per

tant, aplicant el Teorema 3.5 per a $q = 2$, obtenim que $X_{39}(\mathbb{Q}(\sqrt{-13})) = \emptyset$. De fet, es pot provar que $(B_{39}, \mathbb{Q}(\sqrt{-13})) \in \mathrm{D}_{\mathrm{global}}$, de manera que X_{39} és un contraexemple al principi de Hasse sobre $\mathbb{Q}(\sqrt{-13})$.

2. Subgrups canònics de torsió

Ara introduirem els anomenats *subgrups canònics de torsió* d'una superfície abeliana amb QM parametritzada per la corba de Shimura X_D definida per una tripleta fixada $(B_D, \mathcal{O}_D, \varrho)$ com abans. Assumirem doncs que l'àlgebra de quaternions racional i indefinida B_D és de divisió, és a dir, $D = \mathrm{disc}(B) > 1$. El material que presentem en aquesta secció és essencialment una revisió de [**Jor81**, Chapter 4, §3]. Al llarg de la secció, (A, ι) denotarà una superfície abeliana amb QM *definida* sobre un cos k de carcterística zero parametrizada per X_D. Recordem que, en particular, $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}_k(A)$.

Per tal d'entendre els subgrups de torsió de A, és important entendre primer els subgrups $A[\ell]$ de ℓ-torsió de A per a un primer qualsevol ℓ. En aquesta direcció, tenim el següent resultat degut a Morita i que apareix a [**Oht64**]:

Proposició 3.7 (Morita)**.** *Per a qualsevol primer ℓ, el mòdul de Tate ℓ-àdic $T_\ell(A)$ de A és lliure de rang 1 sobre $\mathcal{O}_{D,\ell} = \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. A més, el commutador de $\mathcal{O}_{D,\ell}$ en $\mathrm{End}(T_\ell(A))$ és una subàlgebra de $\mathrm{M}_4(\mathbb{Z}_\ell)$ isomorfa a $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.*

Usarem especialment la següent conseqüència:

Corol·lari 3.8. *Per a qualsevol primer ℓ, $A[\ell]$ és lliure de rang 1 sobre $\mathcal{O}_D/\ell\mathcal{O}_D$.*

Ara fixem un nombre primer p. Aleshores, recordem que $B_{D,p} = B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ és o bé isomorfa a l'única àlgebra de quaternions de divisió sobre $\mathbb{Q}_p$, que denotem per $\mathbb{H}_p$, o bé isomorfa a l'àlgebra de matrius $\mathrm{M}_2(\mathbb{Q}_p)$, depenent de si p divideix D o no, respectivament. Si $L_p/\mathbb{Q}_p$ denota l'única extensió quadràtica no ramificada de $\mathbb{Q}_p$ i $\sigma \in \mathrm{Gal}\,(L_p/\mathbb{Q}_p)$ és l'automorfisme no trivial, $\mathbb{H}_p$ pot considerar-se com a subàlgebra de $\mathrm{M}_2(L_p)$ mitjançant la següent descripció:

$$\mathbb{H}_p \simeq \left\{ \begin{pmatrix} a & b \\ p^\sigma b & {}^\sigma a \end{pmatrix} : a, b \in L_p \right\} \subseteq \mathrm{M}_2(L_p).$$

I amb aquesta presentació, l'únic ordre maximal de $\mathbb{H}_p$ es correspon amb

$$\left\{ \begin{pmatrix} a & b \\ p^\sigma b & {}^\sigma a \end{pmatrix} : a, b \in R_{L_p} \right\},$$

on R_{L_p} és l'anell d'enters de L_p. Aquesta dicotomia es trasllada a l'estructura de $\mathcal{O}_D/p\mathcal{O}_D$:

(i) Si $p \nmid D$, aleshores $\mathcal{O}_D/p\mathcal{O}_D \simeq \mathrm{M}_2(\mathbb{F}_p)$.

(ii) Si $p|D$, aleshores

$$\mathcal{O}_D/p\mathcal{O}_D \simeq \left\{ \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} : a, b \in \mathbb{F}_{p^2} \right\} \subseteq \mathrm{M}_2(\mathbb{F}_{p^2}).$$

A més, aquestes remarques ens permeten donar una descripció explícita dels ideals de la $\mathbb{F}_p$-àlgebra $\mathcal{O}_D/p\mathcal{O}_D$:

Proposició 3.9. *Sigui p un nombre primer.*

(i) *Si $p \nmid D$, aleshores la $\mathbb{F}_p$-àlgebra $\mathcal{O}_D/p\mathcal{O}_D$ té exactament $p+1$ ideals no trivials per l'esquerra, que venen donats per*

$$\mathrm{M}_2(\mathbb{F}_p)\begin{pmatrix} a & 1 \\ a & 1 \end{pmatrix}, \text{ per } a \in \mathbb{F}_p, \quad i \quad \mathrm{M}_2(\mathbb{F}_p)\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

(ii) *Si $p|D$, aleshores la $\mathbb{F}_p$-àlgebra $\mathcal{O}_D/p\mathcal{O}_D$ té exactament un ideal no trivial per l'esquerra, que ve donat per*

$$\left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{F}_{p^2}\right\} \subseteq \left\{\begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} : a, b \in \mathbb{F}_{p^2}\right\} \simeq \mathcal{O}_D/p\mathcal{O}_D.$$

La prova d'aquests enunciats és un exercici senzill en termes de matrius. Ara, l'observació clau és que els ideals no trivials per l'esquerra de la $\mathbb{F}_p$-àlgebra $\mathcal{O}_D/p\mathcal{O}_D$ estan en bijecció amb els $\mathcal{O}_D$-submòduls propis no trivials de $A[p]$, ja que $A[p]$ és un mòdul lliure de rang 1 sobre $\mathcal{O}_D/p\mathcal{O}_D$. Així, la proposició anterior es pot traduir en termes de mòduls i submòduls:

Corol·lari 3.10. *Sigui p un nombre primer i (A, ι) una superfície abeliana amb QM.*

(i) *Si $p \nmid D$, aleshores $A[p]$ té exactament $p+1$ $\mathcal{O}_D$-submòduls propis no trivials.*

(ii) *Si $p|D$, aleshores $A[p]$ té exactament un $\mathcal{O}_D$-submòdul propi no trivial.*

Definició 3.11. *Per a un primer p dividint D, el* subgrup canònic de torsió de (A, ι) en p *és l'únic $\mathcal{O}_D$-submòdul propi no trivial de $A[p]$, i es denota per C_p. El seu ordre és p^2.*

En general, per a qualsevol divisor $d|D$ existeix un únic $\mathcal{O}_D$-submòdul propi no trivial C_d de $A[d]$, que té ordre d^2. És l'anomenat *subgrup canònic de torsió de (A, ι) d'ordre reduït d.*

Proposició 3.12. *Si la superfície abeliana amb QM (A, ι) està definida sobre k i C_d és el seu subgrup canònic de torsió d'ordre reduït d, on d és qualsevol divisor de D, aleshores C_d és racional sobre k.*

Demostració. Més en general, si $\varphi \in \mathrm{Aut}_{\mathcal{O}}(A[d])$ aleshores $\varphi(C_d) \subseteq A[d]$ és un $\mathcal{O}_D$-submòdul propi no trivial d'ordre d^2. Per la unicitat, ha de ser $\varphi(C_d) = C_d$. En particular, això és cert per a qualsevol $\varphi \in \mathrm{Im}(\mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Aut}_{\mathcal{O}}(A[d]))$, d'on se segueix l'enunciat. □

Remarca 3.13. Per a un primer p dividint D i una superfície abeliana amb QM (A, ι), la construcció del subgrup canònic de torsió $C_p \subseteq A[p]$ es pot realitzar des d'una altra perspectiva, tal i com es fa a [**Sko05**]. Per [**Vig80**, p. 86], existeix un únic ideal bilateral $I(p) \subseteq \mathcal{O}_D$ de norma reduïda p, que consisteix exactament en els elements de $\mathcal{O}_D$ de norma reduïda divisible per p.

Aleshores podem considerar el nucli de l'acció de $I(p)$ en A via ι:

$$A[I(p)] = \ker(I(p) : A \to A) = \bigcap_{\beta \in I(p)} \ker(\beta : A \to A) = \{x \in A : \beta \cdot x = 0 \ \forall \beta \in I(p)\},$$

que és un $\mathcal{O}_D$-submòdul de $A[p]$ canònicament isomorf a $\mathcal{O}/I(p) \simeq \mathbb{F}_{p^2}$. Per tant, per la unicitat de C_p és té que $C_p = A[I(p)]$.

Passem ara a definir els caràcters d'isogènia, per als quals necessitem l'acció de Galois en els subgrups de torsió $A[p]$. D'ara en endavant, fixem el primer p dividint D.

La primera observació és que es poden considerar diferents estructures en el subgrup $A[p]$ de p-torsió a l'hora de treballar amb l'acció de Galois. En primer lloc, $A[p]$ és un $\mathcal{O}/p\mathcal{O}$-mòdul lliure de rang 1. D'altra banda, a partir de la descripció

$$\mathcal{O}/p\mathcal{O} \simeq \left\{ \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} : a, b \in \mathbb{F}_{p^2} \right\} \subseteq \mathrm{M}_2(\mathbb{F}_{p^2})$$

podem definir un monomorfisme de $\mathbb{F}_p$-àlgebres

$$\begin{array}{rccc} i : \mathbb{F}_{p^2} & \longrightarrow & \mathcal{O}/p\mathcal{O} \\ a & \longmapsto & \begin{pmatrix} a & 0 \\ 0 & a^p \end{pmatrix} \end{array}$$

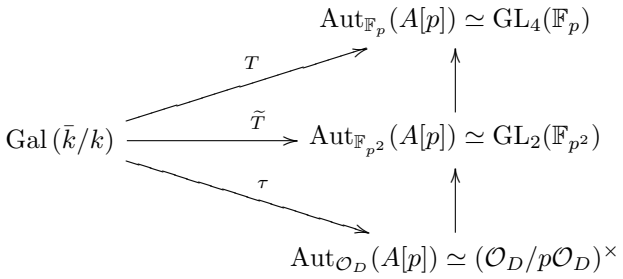
que dóna a $A[p]$ una estructura de $\mathbb{F}_{p^2}$-espai vectorial. Per últim, noti's que $A[p]$ també té una estructura natural de $\mathbb{F}_p$-espai vectorial. Aleshores, les inclusions

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2} \overset{i}{\hookrightarrow} \mathcal{O}/p\mathcal{O}$$

condueixen a inclusions naturals

$$\mathrm{Aut}_{\mathcal{O}}(A[p]) \hookrightarrow \mathrm{Aut}_{\mathbb{F}_{p^2}}(A[p]) \hookrightarrow \mathrm{Aut}_{\mathbb{F}_p}(A[p]).$$

Ara, com que l'acció de $\mathrm{Gal}\,(\bar{k}/k)$ en $A[p]$ commuta amb l'acció de $\mathcal{O}/p\mathcal{O}$, resulta que commuta també amb l'acció de $\mathbb{F}_{p^2}$, de manera que tenim el següent diagrama commutatiu:



Els dos primers isomorfismes se segueixen del fet que $A[p]$ és un espai vectorial sobre $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$) de dimensió 4 (resp. 2). D'altra banda, l'isomorfisme $\mathrm{Aut}_{\mathcal{O}}(A[p]) \simeq (\mathcal{O}/p\mathcal{O})^\times$ es pot construir fàcilment. De fet, com que $A[p]$ és lliure de rang 1 sobre $\mathcal{O}/p\mathcal{O}$, podem escollir $x \in A[p]$ tal que $A[p] = \mathcal{O}/p\mathcal{O} \cdot x$. Llavors, per a tot $f \in \mathrm{Aut}_{\mathcal{O}}(A[p])$ existeix un $m_f \in (\mathcal{O}/p\mathcal{O})^\times$ (unívocament determinat) tal que $f(x) = m_f x$, i llavors l'assignació $f \mapsto m_f$ estableix l'isomorfisme desitjat.

Sigui ara $\sigma \in \mathrm{Gal}\,(\bar{k}/k)$, i suposem que

$$\tau(\sigma) = \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} \in (\mathcal{O}/p\mathcal{O})^\times.$$

Aleshores, tenim

$$\tau(\sigma)\left[\begin{pmatrix} u & v \\ 0 & u^p \end{pmatrix} \cdot x\right] = \begin{pmatrix} u & v \\ 0 & u^p \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} x \quad \text{per a tot } \begin{pmatrix} u & v \\ 0 & u^p \end{pmatrix} \in \mathcal{O}/p\mathcal{O}.$$

Per tal de descriure la representació $\widetilde{T}$, observem primer que podem escollir com a $\mathbb{F}_{p^2}$-base per a $A[p]$ el parell

$$\left\{x, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x\right\}.$$

Llavors, podem escriure

$$\begin{aligned} \tau(\sigma)x &= \begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} x = i(a)x + i(b)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x, \\ \tau(\sigma)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a^p \end{pmatrix} x = i(a^p)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x. \end{aligned}$$

D'aquí se segueix que, en la base escollida, la representació $\widetilde{T}$ és de la forma

$$\begin{pmatrix} (\alpha_{(A,\iota),p})^p & 0 \\ * & \alpha_{(A,\iota),p} \end{pmatrix}$$

per algun caràcter $\alpha_{(A,\iota),p} : \mathrm{Gal}\,(\bar{k}/k) \longrightarrow \mathbb{F}_{p^2}^\times$. Finalment, observem que aquest caràcter $\alpha_{(A,\iota),p}$ ens dóna l'acció del grup de Galois $\mathrm{Gal}\,(\bar{k}/k)$ en

$$\mathcal{O}_D \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x,$$

que és un $\mathcal{O}_D$-submòdul propi no trivial de $A[p]$, i per tant coincideix amb el subgrup canònic de torsió C_p associat al primer p, que és racional sobre k.

Definició 3.14. *El caràcter* $\alpha_{(A,\iota),p} : \mathrm{Gal}\,(\bar{k}/k) \longrightarrow \mathbb{F}_{p^2}^\times \simeq \mathrm{Aut}_{\mathcal{O}}(C_p)$ *és el* caràcter d'isogènia en p *associat a la superfície abeliana amb QM* (A, ι).

Pel que fa a la representació T, la discussió anterior mostra que el polinomi característic de $T(\sigma) \in \mathrm{Aut}_{\mathbb{F}_p}(A[p])$, per a qualsevol $\sigma \in \mathrm{Gal}\,(\bar{k}/k)$, ve donat per

$$[(X - \alpha_{(A,\iota),p}(\sigma))(X - (\alpha_{(A,\iota),p}(\sigma))^p)]^2.$$

3. Recobridor de Shimura de X_D associat a un factor primer p de D

Com abans, sigui B_D una àlgebra de quaternions racional i indefinida de discriminant reduït $D > 1$, i considerem la corba de Shimura X_D associada a la tria d'una tripleta $(B_D, \mathcal{O}_D, \varrho)$. Tanmateix, en aquesta secció ens interessarà considerar X_D com a superfície de Riemann. Recordem que pel fet que $D > 1$, X_D és compacta.

El primer objectiu d'aquesta secció és descriure breument la construcció de l'anomenat *recobridor de Shimura* de X_D associat a un primer p dividint D, que serà un recobridor *étale* cíclic de X_D. En general, per a una superfície de Riemann X, els recobridors *étale* cíclics de X d'ordre n estan en bijecció amb els subgrups cíclics d'ordre n de $\mathrm{H}^1(X, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\pi_1(X), \mathbb{Q}/\mathbb{Z})$ (cohomologia singular), on $\pi_1(X)$ denota el grup fonamental de X. El lector interessat pot trobar detalls d'aquest fet a [**Jor81**, Chapter 5, §1].

Suposem ara que p és un factor primer de D, sigui L_p l'única extensió quadràtica no ramificada de $\mathbb{Q}_p$, i denotem per σ l'automorfisme no trivial en $\mathrm{Gal}\,(L_p/\mathbb{Q}_p)$. Llavors, fixem un isomorfisme

$$\psi : \mathcal{O}_D \otimes \mathbb{Z}_p \xrightarrow{\simeq} \left\{ \begin{pmatrix} x & y \\ p^\sigma y & {}^\sigma x \end{pmatrix} : x, y \in R_{L_p} \right\} \subseteq \mathrm{M}_2(R_{L_p}),$$

on R_{L_p} és l'anell d'enters de L_p, i posem $\mathrm{P}\mathcal{O}_D^1 := \mathcal{O}_D^1/\{\pm 1\}$, on $\mathcal{O}_D^1$ és el subgrup d'unitats de norma 1 en $\mathcal{O}_D^\times$.

Definició 3.15. *El* caràcter Nebentypus de $\mathcal{O}_D$ en p *és el caràcter*

$$\varepsilon_p' : \mathcal{O}_D \otimes \mathbb{Z}_p \longrightarrow \mathbb{F}_{p^2}$$

definit usant l'isomorfisme ψ per la condició

$$\varepsilon_p'(\gamma) = x \mod p \in \mathbb{F}_{p^2} \quad si \quad \psi(\gamma) = \begin{pmatrix} x & y \\ p^\sigma y & {}^\sigma x \end{pmatrix} \; amb \; x, y \in R_{L_p}.$$

El caràcter Nebentypus de $\mathrm{P}\mathcal{O}_D^1$ en p *és llavors el caràcter*

$$\varepsilon_p : (\mathcal{O} \otimes \mathbb{Z}_p)^\times/\{\pm 1\} \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}$$

induït per ε_p'.

Notem que podem considerar el caràcter ε_p també com a caràcter $\mathrm{P}\mathcal{O}_D^1 \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$.

Remarca 3.16. El caràcter Nebentypus ε_p' de $\mathcal{O}_D$ en p depèn de l'elecció de l'isomorfisme ψ, però el parell $\{\varepsilon_p, \varepsilon_p^p\}$ no depèn de ψ.

Sigui ara $\mathcal{E} \subseteq \mathrm{P}\mathcal{O}_D^1$ el subgrup generat pels elements el·líptics (per a l'acció de $\mathrm{P}\mathcal{O}_D^1$ en $\mathfrak{H}$), i denotem per $\pi_p : \mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ la projecció natural. Com que tot subgrup del grup multiplicatiu $\mathbb{F}_{p^2}^\times \simeq \mathbb{Z}/(p^2-1)\mathbb{Z}$ és cíclic, $\pi_p^{-1}(\varepsilon_p(\mathcal{E})) \subseteq \mathbb{F}_{p^2}^\times$ ha de ser cíclic. El següent resultat ens diu que el seu ordre depèn només de l'aritmètica de B_D. Concretament, depèn de si els cossos quadràtics imaginaris $\mathbb{Q}(\sqrt{-1})$ i $\mathbb{Q}(\sqrt{-3})$ escindeixen B_D o no.

Proposició 3.17. *Amb les notacions anteriors,*

$$\pi_p^{-1}(\varepsilon_p(\mathcal{E})) = \begin{cases} \mu_{12} & \text{si } \mathbb{Q}(\sqrt{-1}) \text{ i } \mathbb{Q}(\sqrt{-3}) \text{ escindeixen } B_D, \\ \mu_6 & \text{si } \mathbb{Q}(\sqrt{-3}) \text{ escindeix } B_D \text{ però } \mathbb{Q}(\sqrt{-1}) \text{ no}, \\ \mu_4 & \text{si } \mathbb{Q}(\sqrt{-1}) \text{ escindeix } B_D \text{ però } \mathbb{Q}(\sqrt{-3}) \text{ no}, \\ \mu_2 & \text{si ni } \mathbb{Q}(\sqrt{-1}) \text{ ni } \mathbb{Q}(\sqrt{-3}) \text{ escindeixen } B_D, \end{cases}$$

on hem posat $\mu_r = \mu_r(\mathbb{F}_{p^2}^\times) = \{\zeta \in \mathbb{F}_{p^2}^\times : \zeta^r = 1\}$.

Demostració. L'enunciat se segueix de l'observació que la traça reduïda d'un element el·líptic és -1, 0 o 1, d'acord a la caracterització estàndard dels elements el·líptics de $\mathrm{PSL}_2(\mathbb{R})$ (vegeu [**Jor81**, Proposition 5.1.3]). □

Si per a un cos quadràtic K posem

$$\left(\frac{B_D}{K}\right) = \begin{cases} 1 & \text{si } K \text{ escindeix } B_D, \\ 0 & \text{si } K \text{ no escindeix } B_D, \end{cases}$$

aleshores és immediat comprovar que l'ordre $e(p, D) = |\pi_p^{-1}(\varepsilon_p(\mathcal{E}))|$ de $\pi_p^{-1}(\varepsilon_p(\mathcal{E}))$ ve donat per la següent expressió:

$$e(p, D) = \begin{cases} 2\left(1 + 2\left(\frac{B_D}{\mathbb{Q}(\sqrt{-3})}\right)\right)\left(1 + \left(\frac{B_D}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{si } p > 3, \\ 2\left(1 + \left(\frac{B_D}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{si } p = 3, \\ 1 + 2\left(\frac{B_D}{\mathbb{Q}(\sqrt{-3})}\right) & \text{si } p = 2. \end{cases}$$

Notem que per a $p \neq 2$ l'enter $e(p, D)$ és sempre parell. I com que per a $p = 2$ el subgrup $\{\pm 1\} \subseteq \mathbb{F}_{p^2}^\times$ esdevé simplement el subgrup trivial $\{1\}$, podem considerar la projecció natural $\mathbb{F}_{p^2}^\times/\{\pm 1\} \to \mathbb{F}_{p^2}^\times/\mu_{e(p,D)} \simeq \mathbb{Z}/n(p, D)\mathbb{Z}$, on $n(p, D) = (p^2 - 1)/e(p, D)$. Finalment, la composició del caràcter Nebentypus de $\mathrm{P}\mathcal{O}_D^1$ en p amb aquesta projecció ens porta a la següent definició:

Definició 3.18. *El* caràcter Nebentypus reduït *de* $\mathrm{P}\mathcal{O}_D^1$ *en* p*, que denotarem per* $\widetilde{\varepsilon}_p$*, es defineix com el caràcter que fa commutatiu el següent diagrama:*

$$\begin{array}{ccc} \mathrm{P}\mathcal{O}_D^1 & \xrightarrow{\varepsilon_p} & \mathbb{F}_{p^2}^\times/\{\pm 1\} \\ & \searrow^{\widetilde{\varepsilon}_p} & \downarrow \\ & & \mathbb{Z}/n(p, D)\mathbb{Z} \end{array}$$

Ara, observem que per la Proposició 3.17, tots els elements en $\varepsilon_p(\mathcal{E}) \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$ provenen de $\mu_{e(p,D)} \subseteq \mathbb{F}_{p^2}^\times$, de manera que el caràcter Nebentypus reduït $\widetilde{\varepsilon}_p$ de $\mathrm{P}\mathcal{O}_D^1$ en p és trivial en $\mathcal{E}$ i el podem considerar com a caràcter en $\mathrm{P}\mathcal{O}_D^1/\mathcal{E}$.

Per últim, necessitem un lema tècnic per arribar a obtenir el recobridor desitjat, la prova del qual es deixa per al lector interessat:

Lema 3.19. $\mathrm{P}\mathcal{O}_D^1/\mathcal{E}$ *és un quocient de* $\pi_1(X_D)$.

Per tant, podem considerar el caràcter Nebentypus reduït com

$$\widetilde{\varepsilon}_p : \pi_1(X) \longrightarrow \mathbb{Z}/n(p,D)\mathbb{Z},$$

és a dir, com a un element de $\mathrm{H}^1(\pi_1(X_D), \mathbb{Z}/n(p,D)\mathbb{Z})$ d'ordre $n(p,D)$. Aleshores, per la bijecció esmentada al principi de la secció, a $\widetilde{\varepsilon}_p$ li correspon un recobridor cíclic *étale*

$$Z_{D,p} \longrightarrow X_D$$

d'ordre $n(p,D)$ de la corba de Shimura X_D.

Definició 3.20. *El recobridor $Z_{D,p} \longrightarrow X_D$ d'ordre $n(p,D)$ és el* recobridor de Shimura en p *de la corba de Shimura X_D.*

El recobridor de Shimura $Z_{D,p} \to X_D$ en p admet una interpretació modular, que mostra la seva estreta relació amb els subgrups canònics de torsió en p de les superfícies abelianes parametritzades per X_D. Considerem el caràcter Nebentypus $\varepsilon_p : \mathrm{P}\mathcal{O}_D^1 \to \mathbb{F}_{p^2}^\times$, i denotem el seu nucli per $\Gamma_D(p) \subseteq \mathrm{P}\mathcal{O}_D^1$. Aleshores, $X_{D,p} := \Gamma_D(p) \setminus \mathfrak{H}$ és un recobridor cíclic de Galois de X_D (cf. [**Sij10**, p. 91]) amb grup d'automorfismes $\mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$.

Aquest subgrup $\Gamma_D(p)$ està estretament relacionat amb l'ideal bilateral $I(p)$. De fet, si $\Gamma'_D(p) \subseteq \mathcal{O}_D^1$ és l'antiimatge de $\Gamma_D(p)$ per la projecció natural $\mathcal{O}_D^1 \to \mathrm{P}\mathcal{O}_D^1$, aleshores $\Gamma'_D(p)$ consisteix en els elements de $\mathcal{O}_D^1$ que són congruents amb 1 mòdul $I(p)$.

En termes de mòduli per a superfícies abelianes amb QM, recordem que X_D parametritza parells $(A, \iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A))$, i que cadascuna d'aquestes superfícies abelianes té associat un subgrup canònic de torsió C_p en p. Aleshores, el recobridor de Galois $X_{D,p}$ és solució del problema de mòduli sobre $\mathbb{Q}$ de classificar les classes d'isomorfisme de tripletes (A, ι, x_p), on (A, ι) és una superfície abeliana amb QM parametritzada per X_D i $x_p \in C_p$ és un generador del subgrup canònic de torsió C_p de (A, ι) com a $\mathcal{O}_D$-mòdul. Aquí, un isomorfisme de tripletes $(A, \iota, x_p) \xrightarrow{\sim} (A', \iota', x'_p)$ és un isomorfisme $(A, \iota) \xrightarrow{\sim} (A', \iota')$ que envia x_p a x'_p. Llavors, el recobridor de Shimura $Z_{D,p} \to X_D$ en p és el subrecobridor *étale* maximal de X_D de $X_{D,p} \to X_D$ (vegeu [**Jor81**, p. 110]).

4. L'aportació de Skorobogatov

Recentment ([**Sko05**]), Skorobogatov va adonar-se que aplicant tècniques de descens a un subrecobridor adequat del recobridor de Shimura $Z_{D,p} \to X_D$ associat a un factor primer p de D, el Teorema 3.5 de Jordan podia ser interpretat en termes de descens. De fet, va concloure que si K és un cos quadràtic imaginari, aleshores sota les mateixes hipòtesis que en el Teorema 3.5, no solament $X_D(K)$ és buit, sinó que de fet el conjunt de Brauer $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ és buit. En particular, els contraexemples al principi de Hasse que sorgeixen del resultat de Jordan (i.e. aquells en els quals es té $X_D(\mathbb{A}_K) \neq \emptyset$) queden explicats per l'obstrucció de Brauer-Manin.

Com ja hem explicat, el treball de Jordan en l'estudi de punts globals sobre cossos quadràtics imaginaris en corbes de Shimura es basa fortament en la interpretació modular, i explota les

propietats dels subgrups canònics de torsió de les superfícies abelianes amb QM i els seus caràcters d'isogènia.

La idea principal d'Skorobogatov passa per considerar el recobridor de Shimura $Z_{D,p} \to X_D$ associat a un factor primer p de D vist en la secció anterior, així com la seva interpretació modular induïda per la interpretació del recobridor de Galois $X_{D,p} \to X_D$. Recordem que $\mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{F}_{p^2}^{\times}/\{\pm 1\} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$, i que $\mathrm{Aut}(Z_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{e(p,D)}$, on $e(p,D)$ és un enter que depèn de l'aritmètica de B_D. De fet, els únics valors possibles de $e(p,D)$ són $1,2,3,4,6,12$. Així, com que per a $p \geq 5$ tenim que 12 divideix $p^2-1 = (p+1)(p-1)$, podem definir $Y_{D,p}$ com el quocient de $X_{D,p}$ per l'acció del grup $\mathbb{Z}/6\mathbb{Z}$, vist com a subgrup de $\mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$. De fet, definint $Y_{D,p}$ d'aquesta manera, tenim que $Y_{D,p}$ és sempre un subrecobridor de $Z_{D,p} \to X_D$, i per tant és *étale*. En resum, tenim una torre de recobridors

$$X_{D,p} \to Z_{D,p} \to Y_{D,p} \to X_D.$$

En termes de descens (vegeu [**Sko05**, Corollary 1.2]):

Corol·lari 3.21. *Per a $p \geq 5$, $Y_{D,p}$ és un X_D-torsor per al grup $\mathbb{F}_{p^2}^{\times 12} \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$.*

Sigui k un cos de característica zero, fixem $\bar{k}$ una clausura algebraica de k i sigui $Q \in X_D(k)$ un punt k-racional de X_D. Per especialització del torsor $f_p : Y_{D,p} \to X_D$ en Q tenim associat al punt Q un caràcter $\phi_Q : \mathrm{Gal}\,(\bar{k}/k) \to \mathbb{F}_{p^2}^{\times 12}$ mitjançant el qual el grup de Galois $\mathrm{Gal}\,(\bar{k}/k)$ actua en la fibra de $Y_{D,p} \to X_D$ en Q.

La traducció del punt de vista modular del treball de Jordan al llenguatge del descens es llegeix en aquests caràcters de Galois. Recordem que si (A,ι) és una superfície abeliana amb QM definida sobre k, ja hem vist que l'elecció d'un isomorfisme de $C_p = \mathcal{O}_D/I(p)$ amb $\mathbb{F}_{p^2}$ defineix un caràcter $\alpha_{(A,\iota),p} : \mathrm{Gal}\,(\bar{k}/k) \to \mathbb{F}_{p^2}^{\times}$ provinent de l'acció de Galois en el subgrup canònic de torsió C_p, és a dir, el caràcter d'isogènia. La relació entre els caràcters d'isogènia i els caràcters obtinguts per especialització del torsor $f_p : Y_{D,p} \to X_D$ és la següent:

Lema 3.22. *Sigui k un cos de característica zero que escindeix B_D, i sigui $Q \in X_D(k)$. Si (A,ι) és una superfície abeliana amb QM definida sobre k i parametritzada per Q, aleshores $\alpha_{(A,\iota),p}^{12} = \phi_Q$.*

Demostració. Vegeu [**Sko05**, Lemma 2.1]. □

Suposem ara que K és un cos quadràtic imaginari. Usant el llenguatge i les eines de la teoria del descens, Skorobogatov porta alguns dels resultats de Jordan en [**Jor86**] un pas més enllà, en el sentit que amb les mateixes hipòtesis que usa Jordan en els seus resultats, aconsegueix provar que no tan sols $X_D(K)$ és buit, sinó que de fet $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$. Aquesta diferència implica, com ja hem dit, que els contraexemples al principi de Hasse que sorgeixen del treball de Jordan queden explicats per l'obstrucció de Brauer-Manin.

Així doncs, per exemple, adaptant el Teorema 6.1 de [**Jor86**] Skorobogatov prova el següent:

Teorema 3.23 (Skorobogatov)**.** *Sigui B_D una àlgebra de quaternions racional i indefinida, ramificada en un primer $p \geq 11$, $p \equiv 3 \mod 4$, i sigui X_D la corba de Shimura definida per B_D. Suposem que B_D és escindida per un cos quadràtic imaginari K en el qual p és inert, i sigui $\mathfrak{p}$ l'únic primer de K sobre p. Suposem també que no existeix cap homomorfisme exhaustiu del grup de classes generalitzat de K respecte al mòdul $\mathfrak{p}$ en el producte del grup de classes Cl_K de K amb $\mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$. Aleshores $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

L'argument principal darrera de les demostracions en [**Sko05**] que s'afegeix a les idees de Jordan es pot descriure com segueix. Suposem que K és un cos de nombres i que $Q \in X_D(K)$ és un punt K-racional en la corba de Shimura X_D. El torsor $f_p : Y_{D,p} \to X_D$ per al grup $G = \mathbb{F}_{p^2}^{\times 12}$ és un torsor per a un grup de tipus multiplicatiu. L'aplicació d'avaluació induïda per aquest torsor associa al punt Q la classe $\phi_Q \in \mathrm{H}^1(K, G)$ del K-torsor per G corresponent a la seva fibra. Anàlogament, donada una successió de punts K_v-racionals $\{Q_v\}_v$ en X_D (on v recorre les places de K), obtenim de la mateixa manera elements $\phi_{Q_v} \in \mathrm{H}^1(K_v, G)$. Els caràcters ϕ_{Q_v} són de fet caràcters de $\mathrm{Gal}\,(\bar{K}_v/K_v)$ en G. Aleshores, es considera el següent diagrama commutatiu donat pel torsor f_p:

$$\begin{array}{ccc} X_D(K) & \hookrightarrow & X_D(\mathbb{A}_K) \\ \downarrow & & \downarrow \\ \mathrm{H}^1(K, G) & \longrightarrow & \prod_v \mathrm{H}^1(K_v, G) \end{array}$$

En altres paraules, si existeix un punt racional global $Q \in X_D(K)$, aleshores la família de caràcters locals $\{\phi_{Q_v}\}_v \in \prod_v \mathrm{H}^1(K_v, G)$ determinada per Q consisteix en les restriccions d'un caràcter global en $\mathrm{H}^1(K, G)$ a cadascun dels subgrups $\mathrm{Gal}\,(\bar{K}_v/K_v) \subseteq \mathrm{Gal}\,(\bar{K}/K)$.

Així, per tal de provar que hi ha una obstrucció de Brauer-Manin a l'existència de punts racionals en X_D, l'argument clau es redueix al següent: cal provar que no existeix cap família de caràcters locals $\{\phi_{Q_v}\}_v$ definida per una successió de punts locals $Q_v \in X_D(K_v)$ que prové de la restricció d'un caràcter global de $\mathrm{Gal}\,(\bar{K}/K)$. Si s'aconsegueix provar aquest fet, aleshores el subconjunt de descens $X_D(\mathbb{A}_K)^{f_p} \subseteq X_D(\mathbb{A}_K)$ associat al torsor f_p és buit. Finalment, aplicant el teorema principal de la teoria del descens de Colliot-Thélène i Sansuc (vegeu [**Sko01**, Theorem 6.1.2]) se segueix que de fet $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

Exemple 3.24. Un dels exemples tractats per Skorobogatov en [**Sko05**] és el de la corba de Shimura $X_{23\cdot 107}$ definida per l'àlgebra de quaternions $B_{23\cdot 107}$ de discriminant $23 \cdot 107$, considerada també en [**RSY05**]. La corba $X_{23\cdot 107}$ té gènere 193, i càlculs basats en els resultats en [**JL85**] mostren que $X_{23\cdot 107}$ té punts racionals sobre totes les complecions de $\mathbb{Q}(\sqrt{-23})$, però resulta que $X_{23\cdot 107}(\mathbb{Q}(\sqrt{-23})) = \emptyset$, de manera que $X_{23\cdot 107}$ és un contraexemple al principi de Hasse sobre $\mathbb{Q}(\sqrt{-23})$.

Per tal d'aplicar el Teorema anterior per a $p = 107$, es té que

$$\mathrm{Cl}^{(107)}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$$

i $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/3\mathbb{Z}$, de manera que

$$\mathbb{Z}/\frac{107^2-1}{12}\mathbb{Z} \times \mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Aleshores, és senzill comprovar que les hipòtesis del teorema se satisfan, de manera que el conjunt de Brauer $X_{23\cdot 107}(\mathbb{A}_{\mathbb{Q}(\sqrt{-23})})^{\mathrm{Br}}$ és buit i aquest contraexemple al principi de Hasse queda explicat per l'obstrucció de Brauer-Manin.

L'altre resultat principal presentat en [**Sko05**] (vegeu [**Sko05**, Theorem 3.1]) porta el Teorema 3.5 un pas més enllà, en la mateixa direcció que l'anterior resultat. Amb les notacions prèvies al Teorema 3.5:

Teorema 3.25 (Skorobogatov)**.** *Sigui q un nombre primer. Si K un cos quadràtic imaginari en el qual q ramifica i $B_D \in \mathcal{C}(q)$ és escindida per K, aleshores $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

Exemple 3.26. Com a aplicació d'aquest teorema, Skorobogatov recupera l'exemple donat per l'algebra B_{39} i el cos quadràtic imaginari $\mathbb{Q}(\sqrt{-13})$ de l'Exemple 3.6. La corba de Shimura corresponent X_{39} té punts localment arreu sobre $\mathbb{Q}(\sqrt{-13})$, i per a aquest cas particular es va comprovar a [**SS03**] que $X_{39}(\mathbb{A}_{\mathbb{Q}(\sqrt{-13})})^{\mathrm{Br}} = \emptyset$, però usant una equació conjectural per a X_{39} deguda a Kurihara. Aplicant el teorema anterior amb $q = 2$ s'obté aquest fet de manera incondicional.

Tanmateix, val la pena esmentar que la corba definida per l'equació conjecturada per Kurihara per a X_{39} és realment isomorfa a la corba de Shimura X_{39}, gràcies al treball de Molina en [**Mol10**].

CAPíTOL 4

Representacions de Galois sobre el cos de mòduli

Com hem vist en l'exposició dels treballs de Jordan i Skorobogatov, l'estudi dels punts K-racionals d'una corba de Shimura X_D, amb K un cos quadràtic imaginari se simplifica notablement sota la hipòtesi que K escindeix l'àlgebra de quaternions B_D. Sense aquesta hipòtesi, les superfícies abelianes parametritzades per punts en $X_D(K)$ poden no admetre un model racional sobre K. Per superar aquesta dificultat, en aquest capítol proposem considerar certes representacions de $\mathrm{Gal}\,(\bar{K}/K)$ associades a punts K-racionals de X_D, independentment de si les superfícies abelianes parametritzades per aquests punts admeten un model racional sobre K o no.

Cal remarcar que en aquest capítol ens emmarquem primer en un context força general, doncs les idees s'hi apliquen sense gaire dificultat afegida. Tanmateix, al final del capítol particularitzarem per al cas que ens ocupa, el de les corbes de Shimura, i veurem algunes propietats de les representacions que introduïm, que ens permetran provar el Teorema 5.1.

1. Representacions de Galois associades a varietats abelianes

Sigui k un cos de característica zero, fixem una clausura algebraica $\bar{k}$ de k, i sigui $G_k = \mathrm{Gal}\,(\bar{k}/k)$ el grup de Galois absolut de k. Per una extensió de cossos K/k entendrem sempre un subcós K de $\bar{k}$ contenint k.

Sigui A una varietat abeliana polaritzada de dimensió g definida sobre un cos K/k. Si no és rellevant, no farem explícita la polarització de A. Sigui p un nombre primer, i considerem l'acció del grup de Galois $G_K = \mathrm{Gal}\,(\bar{k}/K)$ en $A(\bar{k})$. Aquesta acció indueix al seu torn una acció de $G_K = \mathrm{Gal}\,(\bar{k}/K)$ en el mòdul de Tate p-àdic $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ de A, que dóna lloc a la representació de Galois usual

$$\varrho_A = \varrho_{A,p} : G_K \longrightarrow \mathrm{Aut}(V_p(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Q}_p).$$

Ometrem el primer p en la notació quan aquest sigui clar pel context.

Ara sigui R una $\mathbb{Z}$-àlgebra finita i suposem que A admet un monomorfisme de $\mathbb{Z}$-àlgebres $i : R \hookrightarrow \mathrm{End}(A)$. Aquí, com que A està definida sobre K, $\mathrm{End}(A) = \mathrm{End}_K(A)$. Aleshores, definim la $\mathbb{Q}$-àlgebra $C_R(A)$ com el commutador de $R \otimes_{\mathbb{Z}} \mathbb{Q}$ en $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ via i, és a dir,

$$C_R(A) := \{\varphi \in \mathrm{End}^0(A) : \varphi \circ i(r) = i(r) \circ \varphi \text{ per a tot } r \in R\}.$$

Similarment, com que els elements de R també actuen com endomorfismes en $T_p(A)$, definim la $\mathbb{Z}_p$-àlgebra $C_R(T_p(A))$ com el commutador de $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ en $\mathrm{End}(T_p(A))$, és a dir,

$$C_R(T_p(A)) := \{\varphi \in \mathrm{End}(T_p(A)) : \varphi \circ i(r) = i(r) \circ \varphi \text{ per a tot } r \in R\}.$$

Observem que $C_R(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ és una $\mathbb{Q}_p$-subàlgebra de $C_R(T_p(A)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Aleshores, definim

$$G_p := C_R(T_p(A))^\times \quad \text{i} \quad \bar{G}_p := (C_R(T_p(A))/pC_R(T_p(A)))^\times,$$

els grups d'elements invertibles en $C_R(T_p(A))$ i $C_R(T_p(A))/pC_R(T_p(A))$, respectivament.

Ara, com que l'acció de G_K en el mòdul de Tate $T_p(A)$ de A commuta amb l'acció de R via $i : R \hookrightarrow \mathrm{End}(A)$, tenim associada al parell (A, i) una representació de Galois

$$\varrho_{(A,i)} = \varrho_{(A,i),p} : G_K \longrightarrow G_p.$$

La reducció de $\varrho_{(A,i)}$ mòdul p es correspon a la representació de Galois donada per l'acció de G_K en el subgrup de p-torsió $A[p] = T_p(A)/pT_p(A)$ de A, que denotem per

$$\bar{\varrho}_{(A,i)} = \bar{\varrho}_{(A,i),p} : G_K \longrightarrow \bar{G}_p.$$

2. Representacions de Galois associades a punts en varietats de Shimura

Siguin k i $\bar{k}$ com abans, i sigui R una $\mathbb{Z}$-àlgebra finita. Sigui X una varietat de Shimura parametritzant classes d'isomorfisme de certs parells (A, i), on A és una varietat abeliana polaritzada i $i : R \hookrightarrow \mathrm{End}(A)$ és un monomorfisme de $\mathbb{Z}$-àlgebres, de manera que un punt $P \in X(\bar{k})$ es correspon a la classe de $\bar{k}$-isomorfisme

$$P = [(A, i)] = \{(A', i')/\bar{k} : \text{ existeix un isomorfisme de parells } (A', i') \simeq (A, i)\}$$

d'una varietat abeliana polaritzada $(A, i)/\bar{k}$ amb multiplicació per R.

Definició 4.1. *Diem que el parell $(A, i)/\bar{k}$ admet un* model racional *sobre un cos K/k si existeix un parell (A', i') definit sobre K i un isomorfisme de parells $(A' \times \bar{k}, i' \times \bar{k}) \simeq (A, i)$. En tal cas, es diu que K és un* cos de definició *de (A, i). D'altra banda, el* cos de mòduli $k_P = k_{(A,i)}$ *de (A, i) és la mínima extensió de cossos k'/k tal que per a tot $s \in G_{k'}$ existeix un isomorfisme $f_s : {}^s(A, i) \to (A, i)$.*

Clarament, el cos de mòduli de (A, i) és únic, i està contingut en tot cos de definició de (A, i). Aleshores, per a qualsevol extensió de cossos K/k, el conjunt $X(K)$ de punts K-racionals de X és

$$X(K) = \{P \in X(\bar{k}) : k_P \subseteq K\}.$$

En particular, notem que si (A, i) admet un model racional sobre K aleshores $P = [(A, i)]$ pertany a $X(K)$. Tanmateix, el recíproc és fals en general.

Sigui ara $P = [(A, i)]$, i suposem sense pèrdua de generalitat que $k_P = k$ (si $k_P \supsetneq k$, substituïm k per k_P). Al llarg de la secció, farem la següent hipòtesi:

Hipòtesi 4.2. *$C_R(A)$ és un cos, i les úniques arrels de la unitat que conté són ± 1.*

En el que segueix, denotarem per $\mathrm{Aut}(A, i)$ el grup d'automorfismes del parell (A, i), on recordem que A és una varietat abeliana polaritzada.

Lema 4.3. *Si se satisfà la Hipòtesi 4.2,* $\mathrm{Aut}(A,i) = \{\pm 1\}$.

DEMOSTRACIÓ. A partir de les definicions, $C_R(A) = \mathrm{End}^0(A,i)$, de manera que $\mathrm{Aut}(A,i)$ està contingut en el grup multiplicatiu $C_R(A)^\times$ d'elements invertibles en $C_R(A)$. Però, com que el grup d'automorfismes d'una varietat abeliana polaritzada és finit (vegeu [**Mil86**, Proposition 17.5]), se segueix que els elements de $\mathrm{Aut}(A,i)$ són arrels de la unitat en $C_R(A)$. Sota la Hipòtesi 4.2, deduïm que $\mathrm{Aut}(A,i) = \{\pm 1\}$. □

De la definició de cos de mòduli, podem associar al punt P un 2-cocicle $c_P : G_k \times G_k \to \{\pm 1\}$ com segueix: escollim una col·lecció d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A,i)) \to (A,i)\}_{s\in G_k}$ i definim

$$c_P(s,t) = f_s \cdot {}^s f_t \cdot f_{st}^{-1} \in \mathrm{Aut}(A,i) = \{\pm 1\}, \quad \text{per a tot } s,t \in G_k.$$

Lema 4.4. *La classe de cohomologia* $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ *definida pel 2-cocicle* c_P *no depèn de l'elecció de* $\mathbf{f}$.

DEMOSTRACIÓ. Suposem que $\mathbf{f} = \{f_s : {}^s(A,i) \to (A,i)\}_{s\in G_k}$ i $\mathbf{f}' = \{f'_s : {}^s(A,i) \to (A,i)\}_{s\in G_k}$ són dues col·leccions diferents d'isomorfismes, i siguin c_P i c'_P els respectius cocicles definits com abans. Llavors, per a cada $s \in G_k$, $\lambda_s := f'_s \cdot f_s^{-1}$ és un automorfisme de (A,i), d'on $\lambda_s = \pm 1$, i podem escriure $f'_s = \lambda_s \cdot f_s$. Aleshores:

$$c'_P(s,t) = (\lambda_s \cdot f_s) \cdot {}^s(\lambda_t \cdot f_t) \cdot (\lambda_{st} \cdot f_{st})^{-1} = \lambda_s \cdot \lambda_t \cdot \lambda_{st}^{-1} c_P(s,t),$$

de manera que c_P i c'_P difereixen per una covora, i per tant defineixem la mateixa classe de cohomologia en $\mathrm{H}^2(G_k, \{\pm 1\})$. □

El següent lema és conseqüència d'un resultat conegut degut a Weil (vegeu [**Wei56**, Theorem 3]):

Lema 4.5. *Un cos* K/k *és un cos de definició per a* (A,i) *si, i només si, la restricció* $c_{P,K}$ *de* c_P *a* G_K *esdevé trivial en* $\mathrm{H}^2(G_K, \{\pm 1\})$.

Sigui $\mathcal{Q}_k$ el conjunt de classes d'isomorfisme d'àlgebres de quaternions sobre k, i sigui $B_P \in \mathcal{Q}_k$ l'àlgebra de quaternions sobre k corresponent a $[c_P] \in \mathrm{H}^2(G_K, \{\pm 1\})$ per l'isomorfisme clàssic $\mathrm{H}^2(G_K, \{\pm 1\}) \simeq \mathcal{Q}_k$ donat per la teoria de cossos de classes. En termes de B_P, el lema anterior ens diu que un cos K és un cos de definició per a (A,i) si, i només si, $B_P \otimes_k K \simeq \mathrm{M}_2(K)$. És a dir, si i només si K *escindeix* B_P.

Corol·lari 4.6. *Existeixen infinites extensions quadràtiques* K/k *que són un cos de definició per a* (A,i). *Concretament, aquelles que escindeixen* B_P.

En general, és difícil calcular la classe del cocicle c_P i l'àlgebra de quaternions B_P. Tanmateix, això ha estat possible en alguns casos: vegeu el Teorema 4.9.

Finalment, estem en condicions de construir representacions de G_k associades al punt $P \in X(k)$. Primer, escollim una col·lecció arbitrària d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A,i)) \to (A,i)\}_{s\in G_k}$ i definim

$$\varrho_P = \varrho_{P,p} : G_k \longrightarrow G_p/\{\pm 1\}$$

mitjançant la regla

$$x \in T_p(A) \longmapsto \varrho_P(s)(x) := f_s({}^s x), \quad s \in G_k. \tag{4}$$

Similarment, definim

$$\bar{\varrho}_P = \bar{\varrho}_{P,p} : G_k \longrightarrow \bar{G}_p/\{\pm 1\}.$$

Degut al següent resultat, el paper de $\mathbf{f}$ és irrellevant:

Lema 4.7. *ϱ_P és un homomorfisme de grups independent de l'elecció de $\mathbf{f}$.*

Demostració. Observem primer que per a $s,t \in G_k$ i $x \in T_p(A)$ tenim

$$\varrho_P(st)(x) = f_{st}({}^{st}x) = c_P(s,t)^{-1}(f_s({}^s f_t({}^s({}^t x)))) = c_P(s,t)^{-1}(\varrho_P(s)(\varrho_P(t)(x))),$$

de manera que $\varrho_P(st) = \varrho_P(s)\cdot\varrho_P(t)$, ja que $c_P(s,t) = \pm 1$. En conseqüència, $\varrho_P : G_k \to G_p/\{\pm 1\}$ és un homomorfisme de grups.

Ara siguin $\mathbf{f} = \{f_s : {}^s(A,i) \to (A,i)\}_{s\in G_k}$ i $\mathbf{f}' = \{f'_s : {}^s(A,i) \to (A,i)\}_{s\in G_k}$ dues col·leccions diferents d'isomorfismes. Com abans, definim l'aplicació $\lambda : G_k \to \mathrm{Aut}(A,i) = \{\pm 1\}$ per $s \mapsto \lambda_s := f'_s \cdot f_s^{-1}$. Llavors,

$$\begin{aligned} \varrho_{P,\mathbf{f}'}(s) : x &\longmapsto f'_s({}^s x), \\ \lambda_s \cdot \varrho_{P,\mathbf{f}}(s) : x &\longmapsto f'_s \cdot f_s^{-1} \cdot f_s({}^s x) = f'_s({}^s x). \end{aligned}$$

Això prova que $\varrho_{P,\mathbf{f}'} = \varrho_{P,\mathbf{f}}$, ja que λ pren valors en $\{\pm 1\}$. De fet, per a qualsevol col·lecció $\mathbf{f}$ com abans i qualsevol aplicació $\lambda : G_k \to \{\pm 1\}$, $f'_s := \lambda_s \cdot f_s$ defineix una segona col·lecció $\mathbf{f}'$ d'isomorfismes satisfent la relació anterior. □

Remarca 4.8. En vistes del Lema 4.7, si (A,i) està definida sobre K/k, podem escollir $f_s = id$ per a tot $s \in G_K \subseteq G_k$. Aleshores, les restriccions de ϱ_P i $\bar{\varrho}_P$ a G_K clarament coincideixen amb la reducció mòdul ± 1 de $\varrho_{(A,i)}$ i $\bar{\varrho}_{(A,i)}$, respectivament.

2.1. El cas de les corbes de Shimura. Sigui ara B_D una àlgebra de quaternions racional i indefinida, de discriminant reduït $D > 1$, fixem un ordre maximal $\mathcal{O}_D$ en B_D i considerem la corba de Shimura X_D associada.

Sigui k un cos de característica zero, i sigui $P \in X_D(k)$ un punt k-racional en X_D. Per la interpretació de mòduli de X_D, P es correspon amb la classe d'isomorfisme d'un parell $(A,\iota)/\bar{k}$, on A és una superfície abeliana i $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ és un monomorfisme d'anells, i tal que el seu cos de mòduli és k. Per tant, existeix una col·lecció d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A,\iota) \to (A,\iota)\}_{s\in G_k}$,

és a dir, per a cada $s \in G_k$, tenim un isomorfisme $f_s : {}^sA \to A$ de superfícies abelianes tal que el diagrama

$$\begin{array}{ccc} {}^sA & \xrightarrow{f_s} & A \\ {\scriptstyle {}^s\iota(\beta)}\downarrow & & \downarrow{\scriptstyle \iota(\beta)} \\ {}^sA & \xrightarrow{f_s} & A \end{array} \tag{5}$$

commuta per a tot $\beta \in \mathcal{O}_D$. Aquest és el cas, per exemple, quan el parell (A, ι) admet un model (A_k, ι_k) racional sobre k.

L'obstrucció per a les superfícies abelianes parametritzades per X_D a admetre un model racional sobre el seu cos de mòduli va ser estudiada per Jordan en [**Jor86**], com hem citat en el Teorema 3.2. Amb el llenguatge que acabem d'introduir, podem reenunciar el resultat de Jordan com segueix:

Teorema 4.9 (Jordan)**.** *Sigui k un cos de característica zero. Per a qualsevol punt $P \in X_D(k)$, es té $B_P = B_D \otimes k$.*

Observem que la condició perquè un parell (A, i) representant $P \in X_D(k)$ admeti un model racional sobre k depèn només de l'aritmètica de l'àlgebra B_D, i no del punt P.

Ens centrem ara en el cas d'un cos quadràtic imaginari $K/\mathbb{Q}$. Sigui v una plaça de K sobre un primer racional ℓ, i sigui $P_v \in X_D(K_v)$ un punt K_v-racional. Escollim una extensió quadràtica $K'/\mathbb{Q}$ escindint B_D, i denotem per v' una plaça de K' sobre ℓ. En particular, $L_w := K_v \cdot K'_{v'}$ escindeix B_D (denotem per w l'única extensió de la valoració ℓ-àdica en $\mathbb{Q}_\ell$ a $K_v \cdot K'_{v'}$). Aleshores, pel Teorema 4.9, existeix un parell (A_v, ι_v) definit sobre L_w tal que $P_v = [(A_v, \iota_v)]$.

D'altra banda, fixem un primer p dividint D. Com abans, tenim associada al parell (A_v, ι_v) una representació de Galois

$$\varrho_{(A_v,\iota_v)} = \varrho_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \subseteq \mathrm{Aut}_{B_D}(T_p(A_v)) \simeq (B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times,$$

induïda per l'acció del grup de Galois G_{L_w} en el mòdul de Tate p-àdic $V_p(A_v) = T_p(A_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ de A_v, on l'isomorfisme $\mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ se segueix de [**Oht64**]. Notem que en la notació anterior, $\mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) = C_{\mathcal{O}_D}(T_p(A_v))^\times$. La reducció mòdul p d'aquesta representació és doncs la representació

$$\bar{\varrho}_{(A_v,\iota_v)} = \bar{\varrho}_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A_v[p]) \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times \subseteq \mathrm{Aut}_{\mathbb{F}_{p^2}}(A_v[p]) \simeq \mathrm{GL}_2(\mathbb{F}_{p^2})$$

que sorgeix de l'acció de Galois en el subgrup de p-torsió $A_v[p]$.

Finalment, considerem el subgrup canònic de torsió $C_p \subseteq A_v[p]$ de A_v en el primer p, considerat com a $\mathcal{O}_D$-mòdul, que fou introduït a [**Jor81**]. Recordem que $C_p = A_v[I(p)] \simeq \mathcal{O}_D/I(p) \simeq \mathbb{F}_{p^2}$, on $I(p)$ és l'únic $\mathcal{O}_D$-ideal bilateral de norma reduïda p ([**Vig80**, p. 86]). En particular, $\mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^\times$, i per la unicitat C_p és racional sobre L_w. Per tant, podem associar al parell (A_v, ι_v) la

representació de Galois induïda per l'acció de G_{L_w} en C_p, que denotem per

$$\alpha_{(A_v,\iota_v)} = \alpha_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}.$$

Aquest és l'anomenat *caràcter (canònic) d'isogènia en p*. Noti's que podem considerar $\alpha_{(A_v,\iota_v)}$ com a caràcter en $G_{L_w}^{ab} = \mathrm{Gal}\,(L_w^{ab}/L_w)$, on L_w^{ab} és la clausura abeliana de L_w en $\bar{L}_w$. Aquest caràcter està estretament relacionat amb la representació de Galois $\varrho_{(A_v,\iota_v)}$. De fet, tal i com ja hem vist al capítol anterior:

Proposició 4.10. *Amb les notacions anteriors:*

(a) *Existeix una $\mathbb{F}_{p^2}$-base de $A_v[p]$ respecte a la qual*

$$\bar{\varrho}_{(A_v,\iota_v)} = \begin{pmatrix} (\alpha_{(A_v,\iota_v)})^p & 0 \\ * & \alpha_{(A_v,\iota_v)} \end{pmatrix}.$$

I per a qualsevol $\sigma \in G_{L_w}$, el polinomi característic de $\varrho_{(A_v,\iota_v)}(\sigma) \in \mathrm{Aut}_{\mathbb{F}_p}(A_v[p])$ ve donat per

$$[(T - \alpha_{(A_v,\iota_v)}(\sigma))(T - \alpha_{(A_v,\iota_v)}(\sigma)^p)]^2.$$

(b) *Si $p \neq \ell$, aleshores $\varrho^{12}_{(A_v,\iota_v)}$ és no ramificada. En particular, $\alpha^{12}_{(A_v,\iota_v)}$ és no ramificat.*

Demostració. L'afirmació en (a) és [**Jor81**, Proposition 4.3.10], i (b) se segueix de [**Jor86**, §3]. □

A més, com en [**Jor86**, Proposition 4.6], tenim el següent:

Lema 4.11. *Sigui $\bar{\chi}_p : G_{K_v} \to \mathrm{Aut}(\mu_p) \simeq \mathbb{F}_p^{\times}$ la reducció mòdul p del caràcter p-ciclotòmic. Aleshores, $N_{\mathbb{F}_{p^2}/\mathbb{F}_p} \circ \alpha_{(A_v,\iota_v)} = \bar{\chi}_{p|G_{L_w}}$.*

De cara a poder treballar amb representacions de Galois associades al punt P_v, el següent lema és essencial:

Lema 4.12. *Si A_v no té multiplicació complexa per $\mathbb{Q}(\sqrt{-1})$ ni per $\mathbb{Q}(\sqrt{-3})$, aleshores se satisfà la Hipòtesi 4.2 per al parell (A_v, ι_v).*

Demostració. Suposem primer que A_v no té multiplicació complexa per cap cos quadràtic imaginari. Llavors, $\iota_v : \mathcal{O}_D \xrightarrow{\simeq} \mathrm{End}(A_v)$ és un isomorfisme, i el commutador $C_{\mathcal{O}_D}(A_v)$ de $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_D$ en $\mathrm{End}^0(A_v) \simeq B_D$ és $\mathbb{Q}$, ja que B_D és central. Per tant, en aquest cas se satisfà clarament la Hipòtesi 4.2.

D'altra banda, suposem que A_v té multiplicació complexa per un cos quadràtic imaginari $M/\mathbb{Q}$, de manera que $\mathrm{End}^0(A_v) \simeq \mathrm{M}_2(M)$. Aleshores, el commutador $C_{\mathcal{O}_D}(A_v)$ de $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_D$ en $\mathrm{End}^0(A_v) \simeq \mathrm{M}_2(M)$ conté clarament M, i per dimensions ha de ser exactament M (vegeu [**Pie82**, Theorem 12.7]). Com que els únics cossos quadràtics imaginaris amb arrels de la unitat no trivials són $\mathbb{Q}(\sqrt{-1})$ i $\mathbb{Q}(\sqrt{-3})$, se segueix que si $M \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ se satisfà la Hipòtesi 4.2, i el lema queda provat. □

D'ara en endavant, suposarem que A_v no té multiplicació complexa per $\mathbb{Q}(\sqrt{-1})$ ni per $\mathbb{Q}(\sqrt{-3})$. Per tant, associades al punt $P_v \in X_D(K_v)$ parametritzant el parell (A_v, ι_v) tenim representacions de Galois

$$\varrho_{P_v} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v))/\{\pm 1\} \subseteq \mathrm{GL}_4(\mathbb{Z}_p)/\{\pm 1\}$$

i

$$\bar{\varrho}_{P_v} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A_v[p])/\{\pm 1\} \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\}$$

que estenen l'acció de Galois en $T_p(A_v)$ i $A_v[p]$, respectivament. Pel mateix mètode, podem associar també a P_v una representació de Galois

$$\alpha_{P_v} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p)/\{\pm 1\} \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\}$$

a partir de l'acció de Galois en el subgrup canònic de torsió C_p. Per la Remarca 4.8, les restriccions d'aquestes representacions a $G_{L_v} \subseteq G_{K_v}$ coincideixen amb la reducció mòdul ± 1 de $\varrho_{(A_v,\iota_v)}$, $\bar{\varrho}_{(A_v,\iota_v)}$ i $\alpha_{(A_v,\iota_v)}$, respectivament.

Tenint en compte això, de la Proposició 4.10, se segueix de manera immedata el següent:

Corol·lari 4.13. *Si $p \neq \ell$, $\alpha_{P_v}^{12}$ és no ramificat.*

Escriurem $\tilde{\varrho}_{P_v} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v))$ i $\tilde{\alpha}_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^\times$ per als aixecaments de ϱ_{P_v} i α_{P_v} associats a la tria de $\mathbf{f}$ per (4). Aquests aixecaments no són homomorfismes en general, pero és fàcil comprovar que per a qualsevol $\sigma \in G_{K_v}$ es té $\tilde{\varrho}_{P_v}(\sigma^2) = \pm\tilde{\varrho}_{P_v}(\sigma)^2$, $\tilde{\alpha}_{P_v}(\sigma^2) = \pm\tilde{\alpha}_{P_v}(\sigma)^2$.

Tot i que podem considerar α_{P_v} com a caràcter en $G_{K_v}^{ab}$, això no és cert per a l'aixecament $\tilde{\alpha}_{P_v}$, que no és ni tan sols homomorfisme. Tanmateix, observem que per a qualsevol $\sigma \in G_{K_v}$, $\tilde{\alpha}_{P_v}(\sigma)^2$ depèn només de la imatge $\sigma' \in G_{K_v}^{ab}$ de σ per l'aplicació natural de pas al quocient. En efecte, sigui $a \in \mathbb{F}_{p^2}^\times$ tal que $\alpha_{P_v}(\sigma) = \alpha_{P_v}(\sigma') = a \bmod \pm 1 \in \mathbb{F}_{p^2}^\times/\{\pm 1\}$. Llavors $\tilde{\alpha}_{P_v}(\sigma) = \pm a \in \mathbb{F}_{p^2}^\times$, i $\tilde{\alpha}_{P_v}(\sigma)^2 = a^2 \in \mathbb{F}_{p^2}^\times$ depèn només de σ'. Clarament, el mateix és cert si canviem 2 per un enter parell qualsevol.

Usant el fet que $\tilde{\alpha}_{P_v|G_{L_w}}$ coincideix amb $\alpha_{(A_v,\iota_v)}$, el Lema 4.11 implica que

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_v|G_{L_w}}(\sigma)) = \chi_{p|G_{L_w}}(\sigma), \quad \text{per a tot } \sigma \in G_{L_w}.$$

Com que L_w té com a molt grau 2 sobre K_v, podem escriure

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_v|G_{L_w}}(\sigma^2)) = \chi_{p|G_{L_w}}(\sigma^2) = \chi_p(\sigma)^2, \quad \text{per a tot } \sigma \in G_{K_v}.$$

I, usant que $\tilde{\alpha}_{P_v|G_{L_w}}(\sigma^2) = \pm\tilde{\alpha}_{P_v}(\sigma)^2$ per a tot $\sigma \in G_{K_v}$, obtenim

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_v}(\sigma)^2) = \chi_p(\sigma)^2, \quad \text{per a tot } \sigma \in G_{K_v}. \tag{6}$$

Finalment, com en el treball d'Skorobogatov, el caràcter $\alpha_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ també està estretament relacionat amb el caràcter $\phi_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$ obtingut per especialització del torsor $f_p : Y_{D,p} \to X_D$ en el punt P_v. Com en el Lema 3.22, per la interpretació modular del torsor f_p

tenim ara que $\phi_{P_v|G_{L_v}} = \alpha^{12}_{(A_v,\iota_v)}$. I aquesta relació es pot traduir fàcilment a una relació entre ϕ_{P_v} i α_{P_v}:

Lema 4.14. *Per a qualsevol $\sigma \in G_{K_v}$, $\tilde{\alpha}_{P_v}(\sigma)^{24} = \phi_{P_v}(\sigma)^2$. En termes de α_{P_v}, tenim*

$$\alpha_{P_v}(\sigma)^{12} = \phi_{P_v}(\sigma) \mod \pm 1, \quad \forall \sigma \in G_{K_v}.$$

Demostració. Com que la restricció de $\tilde{\alpha}_{P_v}$ a G_{L_v} coincideix amb $\alpha_{(A_v,\iota_v)}$, tenim que $(\tilde{\alpha}_{P_v|G_{L_v}})^{12} = \phi_{P_v|G_{L_v}}$. Per tant, si $\sigma \in G_{K_v}$ aleshores

$$\tilde{\alpha}_{P_v}(\sigma)^{24} = (\pm\tilde{\alpha}_{P_v}(\sigma^2))^{12} = (\tilde{\alpha}_{P_v|G_{L_v}}(\sigma))^{12} = \phi_{P_v|G_{L_v}}(\sigma^2) = \phi_{P_v}(\sigma)^2,$$

d'on se segueix l'enunciat. □

Per últim, usant també el Corol·lari 4.13 es dedueix que:

Corol·lari 4.15. *Si $p \neq \ell$, aleshores $\phi^2_{P_v}$ és no ramificat.*

CAPíTOL 5

Punts en corbes de Shimura racionals sobre cossos quadràtics imaginaris

Finalment, en aquest capítol presentem el resultat principal d'aquest treball, el Teorema 5.1, a la prova del qual dediquem la primera secció. Els arguments en la demostració d'aquest resultat són similars als emprats en [**Sko05**], però fent servir les representacions de Galois introduïdes en el capítol anterior.

En la segona secció del capítol exposem algunes conseqüències del Teorema 5.1 que permeten produir exemples de parells excepcionals (B_D, K) tals que X_D és un contraexemple al principi de Hasse sobre K. La Taula 5.1 recull alguns d'aquests exemples.

1. El resultat principal

En aquesta secció presentem i provem el resultat principal d'aquest treball, que dóna condicions suficients explícites per tal que el conjunt de punts K-racionals $X_D(K)$, per a K un cos quadràtic imaginari, sigui buit. De fet, el Teorema 5.1 que provem a continuació prova un fet lleugerament més feble, ja que dóna condicions suficients perquè $X_D(K)$ contingui només punts CM. Es diu que un punt $P \in X_D(K)$ és un *punt CM* si les superfícies abelianes (A, ι) parametritzades per P admeten CM per algun cos quadràtic imaginari (cf. Teorema 1.9). Tanmateix, en el Corol·lari 5.2 veiem que afegint petites hipòtesis es pot afirmar que realment $X_D(K)$ és buit.

De manera similar al Teorema 3.5, necessitem definir un conjunt de *primers excepcionals* associat a un nombre primer donat. Així, si q és un nombre primer, definim $P_1(q)$ com el conjunt (finit) de tots els factors primers dels enters no nuls en el conjunt

$$\bigcup_{s,a} \{a^2 - sq, a^4 - 4a^2q + q^2\},$$

on la unió és sobre $s = 0, 1, 2, 3, 4$ i els enters a tals que $|a| \leq 2q$. Per a $q \neq 2$, definim també $\mathcal{B}_1(q)$ com el conjunt d'àlgebres de quaternions racionals i indefinides que no són escindides per $\mathbb{Q}(\sqrt{-q})$. D'altra banda, definim $\mathcal{B}_1(2)$ com el conjunt d'àlgebres de quaternions racionals i indefinides que no són escindides ni per $\mathbb{Q}(\sqrt{-2})$ ni per $\mathbb{Q}(\sqrt{-1})$. Aleshores, el resultat principal d'aquest treball és el següent:

Teorema 5.1. *Sigui K un cos quadràtic imaginari en el qual un primer q ramifica. Si $B_D \in \mathcal{B}_1(q)$ és tal que D és divisible per un primer $p \notin P_1(q)$, $p \geq 5$, i p no descomposa en K, aleshores $X_D(K)$ conté només punts CM.*

DEMOSTRACIÓ. Sigui $p \notin P(q)$, $p \geq 5$, un factor primer de D tal que p no descomposa en K, i sigui $\mathfrak{p}$ l'únic primer de K sobre p. Sigui també $K'/\mathbb{Q}$ una extensió quadràtica escindint l'àlgebra de quaternions B_D, i tal que el primer q no és inert en K'. Si $D = p_1 \cdots p_{2r}$, l'existència d'una tal extensió K' es redueix a l'existència d'un discriminant quadràtic d tal que $(\frac{d}{p_i}) \neq 1$, $i = 1, \ldots, 2r$ i $(\frac{d}{q}) \neq -1$. Pel Teorema de Čebotarev, entre els d primers hi ha infinites possibles tries.

Suposem que $P \in X_D(K)$ és un punt sense multiplicació complexa per $\mathbb{Q}(\sqrt{-1})$ ni per $\mathbb{Q}(\sqrt{-3})$. Per la interpretació modular de X_D, podem escollir una superfície abeliana $(A, \iota)/\bar{K}$ amb multiplicació quaterniònica per $\mathcal{O}_D$ i amb cos de mòduli K parametritzada per P. Mitjançant l'embedding diagonal $X_D(K) \hookrightarrow X_D(\mathbb{A}_K)$, el punt P defineix una successió de punts locals $\{P_v\}_v \in X_D(\mathbb{A}_K)$. Per a cadascun d'aquests punts, diguem $P_v \in X_D(K_v)$, podem escollir la mateixa superfície abeliana (A, ι) representant P_v. Per claredat, però, la denotarem per (A_v, ι_v). Notem que (A_v, ι_v) no té multiplicació complexa per $\mathbb{Q}(\sqrt{-1})$ ni per $\mathbb{Q}(\sqrt{-3})$.

El caràcter global $\phi : G_K \to \mathbb{F}_{p^2}^{\times 12}$ obtingut per especialització del torsor f_p en el punt P restringeix a cadascun dels caràcters locals ϕ_{P_v} associats a cada punt P_v en G_{K_v}. Per tant, pel Corol·lari 4.15 tenim que ϕ^2 és no ramificat fora de $\mathfrak{p}$. Per a cada plaça no arquimediana v de K, sobre algun primer racional ℓ, escollim una plaça v' de K' sobre ℓ, de manera que (A_v, ι_v) admet un model racional sobre $L_w := K_v \cdot K'_{v'}$ (denotem per w l'única extensió de v a $K_v \cdot K'_{v'}$), així que suposarem que està definida sobre L_w. Aleshores, la restricció de ϕ_{P_v} a G_{L_w} coincideix amb la representació de Galois $\alpha^{12}_{(A_v, \iota_v)}$.

D'altra banda, sigui $\mathfrak{q}$ l'únic primer de K sobre q, i sigui $\sigma_\mathfrak{q} \in G_{K_\mathfrak{q}}$ un element de Frobenius en $\mathfrak{q}$, i.e. un element induint l'automorfisme de Frobenius $\mathrm{Fr}_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ per reducció. Afirmem primer que $\tilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2)^{24} = q^{24}$, i comencem provant aquest fet.

La teoria de cossos de classes global ens dóna una successió exacta

$$\prod_v U_v \longrightarrow G_K^{ab} \longrightarrow \mathrm{Cl}_K \longrightarrow 0,$$

on U_v és el grup d'unitats de l'anell d'enters de K_v i $U_v \to G_K^{ab}$ ve definida per l'aplicació local d'Artin w_v. L'idèle en $\prod_v U_v$ que té per components $1/q$, excepte la posició $\mathfrak{q}$, on posem π^2/q, amb π un uniformitzador en $\mathfrak{q}$, té per imatge $\mathrm{Frob}_\mathfrak{q}^2$, el quadrat d'un element de Frobenius $\mathrm{Frob}_\mathfrak{q} \in G_K^{ab}$ en $\mathfrak{q}$. Llavors, $\sigma_\mathfrak{q}^2 \cdot \mathrm{Frob}_\mathfrak{q}^{-2}$ pertany al subgrup d'inèrcia $I_{K_\mathfrak{q}} \subseteq G_{K_\mathfrak{q}}$ i, com que ϕ^2 és no ramificat fora de $\mathfrak{p}$, obtenim que $\phi^2(\sigma_\mathfrak{q}^2) = \phi^2(\mathrm{Frob}_\mathfrak{q}^2)$. Però ara observem que

$$\phi^2(\sigma_\mathfrak{q}^2) = \phi^2_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2) = \tilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2)^{24}$$

i

$$\phi^2(\mathrm{Frob}_\mathfrak{q}^2) = \phi^2_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1})) = \tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1}))^{24},$$

de manera que per provar la nostra afirmació hem de provar que $\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1}))^{24} = q^{24}$. Tenim dos casos per tractar:

(a) p és inert en K. En aquest cas, el grup d'unitats $U_{\mathfrak{p}}$ és una extensió de $\mathbb{F}_{p^2}^\times$ per un grup pro-p. Aleshores, l'homomorfisme $\alpha_{P_{\mathfrak{p}}} \circ w_{\mathfrak{p}} : U_{\mathfrak{p}} \to I_{\mathfrak{p}}^{ab} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ ha de ser trivial en la pro-p-part, de manera que $\alpha_{P_{\mathfrak{p}}} \circ w_{\mathfrak{p}}$ factoritza per un homomorfisme $\mu : \mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$. Si $a \in \mathbb{F}_{p^2}^\times$ és un generador del grup cíclic $\mathbb{F}_{p^2}^\times$, aleshores la classe $[a]$ de a en $\mathbb{F}_{p^2}^\times/\{\pm 1\}$ és un generador de $\mathbb{F}_{p^2}^\times/\{\pm 1\}$, i per tant l'homomorfisme μ ve determinat per un enter c (unívocament determinat mòdul $(p^2-1)/2$) tal que $\mu(a) = [a]^{-c}$.

Llavors, si denotem per $\tilde{u} \in \mathbb{F}_{p^2}^\times$ la reducció mòdul $\mathfrak{p}$ de $u \in U_{\mathfrak{p}}$, tenim $\alpha_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u)) = \mu(\tilde{u}) = [\tilde{u}]^{-c}$. En particular, $\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u)) = \pm\tilde{u}^{-c}$. D'altra banda, aplicant [**Ser72**, Prop. 3, 8] tenim que $\chi_p(w_{\mathfrak{p}}(u)) = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u})^{-1}$ per a tot $u \in U_{\mathfrak{p}}$. Per tant, usant (6),

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2) = \chi_p(w_{\mathfrak{p}}(u))^2 = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u})^{-2} = \tilde{u}^{-2(p+1)} \in \mathbb{F}_p^\times,$$

i també tenim

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2) = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u}^{-2c}) = \tilde{u}^{-2c(p+1)} \in \mathbb{F}_p^\times.$$

D'aquí es dedueix que $2c \equiv 2 \bmod p-1$. En conseqüència, $\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1}))^{24} = q^{24}$ com volíem.

(b) p ramifica en K. Ara, $U_{\mathfrak{p}}$ és una extensió de $\mathbb{F}_p^\times$ per un grup pro-p, i per tant tenim que l'homomorfisme $\alpha_{P_{\mathfrak{p}}} \circ w_{\mathfrak{p}} : U_{\mathfrak{p}} \to I_{\mathfrak{p}}^{ab} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ factoritza per un homomorfisme $\mu : \mathbb{F}_p^\times \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$. Llavors, la imatge $\alpha_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(U_{\mathfrak{p}}))$ ha d'estar continguda en l'únic subgrup cíclic d'ordre $p-1$ de $\mathbb{F}_{p^2}^\times/\{\pm 1\}$. En particular, per a tot $u \in U_{\mathfrak{p}}$, $\alpha_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2$ pertany a $\mathbb{F}_p^\times/\{\pm 1\} \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, que és l'únic subgrup d'ordre $(p-1)/2$ de $\mathbb{F}_{p^2}^\times/\{\pm 1\}$.

Així, si denotem de nou per $\tilde{u} \in \mathbb{F}_p^\times$ la reducció de u mòdul $\mathfrak{p}$, existeix un enter c, unívocament determinat mòdul $(p-1)/2$ tal que $\alpha_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2 = [\tilde{u}]^{-c}$, on $[\tilde{u}]$ denota la classe de $\tilde{u}$ en $\mathbb{F}_p^\times/\{\pm 1\}$. En particular, $\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2 = \pm\tilde{u}^{-c}$.

Ara, [**Ser72**, Prop. 3, 8] implica que $\chi_p(w_{\mathfrak{p}}(u)) = N_{\mathbb{F}_p/\mathbb{F}_p}(\tilde{u})^{-2} = \tilde{u}^{-1}$, de manera que aplicant (6) s'obté

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2) = \chi_p(w_{\mathfrak{p}}(u))^2 = \tilde{u}^{-4}.$$

Però observem ara que

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2) = (\pm\tilde{u}^{-c})^2 = \tilde{u}^{2c},$$

ja que $\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2 \in \mathbb{F}_p^\times$. Per tant, $c \equiv 2 \bmod p-1$, es dedueix que

$$\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1}))^{24} = (\tilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1}))^2)^{12} = q^{24} \in \mathbb{F}_p^\times,$$

i l'afirmació queda provada també en aquest cas.

Ara, com que q no és inert en K', si $\mathfrak{q}'$ és un primer de K' sobre q, el cos residual de $K'_{\mathfrak{q}'}$ és $\mathbb{F}_q$. En conseqüència, també el cos residual de $L_{\mathfrak{Q}} = K_{\mathfrak{q}} \cdot K'_{\mathfrak{q}'}$ és $\mathbb{F}_q$. Llavors, com que $A_{\mathfrak{q}}/L_{\mathfrak{q}}$ té bona reducció potencial, seguint la construcció de Serre i Tate en [**ST68**, p. 498] s'obté una superfície abeliana $\tilde{A}_{\mathfrak{q}}$ definida sobre $\mathbb{F}_q$ i tal que l'àlgebra de quaternions $B_D \subseteq \mathrm{End}^0_{L_{\mathfrak{q}}}(A_{\mathfrak{q}})$ admet

un embedding en $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_\mathfrak{q})$. A més, $\sigma_\mathfrak{q} \in G_{L_\Omega}$, i la seva acció en els mòduls de Tate $T_p(A_\mathfrak{q})$ i $T_p(\tilde{A}_\mathfrak{q})$ coincideix.

Com en [**Jor86**, §5], la traça de $\bar{\varrho}_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)$ és la reducció mòdul p d'un enter $a_{\mathfrak{q},n}$, $|a_{\mathfrak{q},n}| \leq 2q^{n/2}$, tal que

$$a_{\mathfrak{q},n} \bmod p = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)) = \alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n) + q^n\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)^{-1}.$$

En particular,

$$a_\mathfrak{q} \bmod p = a_{\mathfrak{q},2} \bmod p = \alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^2) + q^2\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^2)^{-1}.$$

Com que $\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})} = \tilde{\alpha}_{P_\mathfrak{q}|G_{L_\Omega}}$ i $\sigma_\mathfrak{q} \in G_{L_\Omega}$, usant l'afirmació que hem provat abans podem escriure

$$a_\mathfrak{q} \bmod p = \tilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2) + q^2\tilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2)^{-1} = q(\zeta + \zeta^{-1}),$$

on $\zeta = \frac{\tilde{\alpha}_{P_\mathfrak{p}}(\sigma_\mathfrak{q}^2)}{q}$ és una arrel 24-ena de la unitat. Calculant els possibles valors de $q(\zeta+\zeta^{-1})$ obtenim que o bé $a_\mathfrak{q} \mod p = 0$ o bé p divideix

$$a_\mathfrak{q} \pm q, a_\mathfrak{q}^2 - 2q^2, a_\mathfrak{q}^2 - 3q^2, a_\mathfrak{q} \pm 2q, \text{ o } a_\mathfrak{q}^4 - 4a_\mathfrak{q}^2q + q^2.$$

Com que $|a_\mathfrak{q}| \leq 2q$, la hipòtesi $p \notin P(q)$ implica que de fet

$$a_\mathfrak{q} = 0, \pm q, \pm\sqrt{2}q, \pm\sqrt{3}q, \pm 2q, \text{ o } \pm q\sqrt{2q \pm \sqrt{3}}.$$

Però, com que $a_\mathfrak{q}$ és un enter, les úniques possibilitats són $a_\mathfrak{q} = 0, \pm q$, o $\pm 2q$. Ara, si ξ és una arrel 48-ena de la unitat tal que $\xi^2 = \zeta$, la traça del polinomi característic de $\bar{\varrho}_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q})$ és la reducció mòdul p d'un enter $b_\mathfrak{q} = a_{\mathfrak{q},1}$ de valor absolut com a molt $2\sqrt{q}$ satisfent $b_\mathfrak{q} \bmod p = \sqrt{q}(\xi + \xi^{-1})$. Aplicant la teoria de Honda-Tate per a la classificació de l'àlgebra d'endomorfismes d'una superfície amb multiplicació quaterniònica definida sobre un cos finit (vegeu [**Jor86**, Theorem 2.1]), s'obté la següent llista de possibilitats:

$a_\mathfrak{q} = 0$, $q = 2$: llavors $\mathbb{Q}(\sqrt{-1})$ escindeix B_D;
$a_\mathfrak{q} = q = 3$: llavors $\mathbb{Q}(\sqrt{-3})$ escindeix B_D;
$a_\mathfrak{q} = -2q$: llavors $\mathbb{Q}(\sqrt{-q})$ escindeix B_D.

En tots els casos, obtenim una contradicció amb la hipòtesi $B_D \in \mathcal{B}_1(q)$, i per tant el resultat queda provat. □

De la mateixa prova, se segueix de fet que per a un parell (B_D, K) satisfent les hipòtesis del Teorema 5.1, $X_D(K)$ conté només punts amb CM per $\mathbb{Q}(\sqrt{-1})$ o per $\mathbb{Q}(\sqrt{-3})$. Així, per tal de donar condicions suficients perquè $X_D(K) = \emptyset$ basta estudiar els conjunts $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1}))$ i $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1}))$. Aquí, per a un cos quadràtic imaginari L, $\mathrm{CM}(L)$ denota la unió dels conjunts $\mathrm{CM}(R) \subset X_D(\bar{\mathbb{Q}})$, on R recorre els ordres quadràtics en L.

El problema sobre l'existència de punts amb CM en corbes de Shimura, així com la caracterització dels seus cossos de definició, ha estat resolt, i es té una caracterització explícita de quan una corba de Shimura té punts amb CM racionals sobre un cos de nombres donat. Usant els resultats de [**GR06**, §5], per exemple, és fàcil deduir el següent corol·lari al Teorema 5.1:

Corol·lari 5.2. *Suposem que el parell (B_D, K) satisfà les hipòtesis del Teorema 5.1.*

(i) *Si $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, aleshores $X_D(K) = \emptyset$.*

(ii) *Si $K = \mathbb{Q}(\sqrt{-1})$ i existeix un primer $\ell \equiv 1 \mod 4$ dividint D, aleshores $X_D(K) = \emptyset$.*

(iii) *Si $K = \mathbb{Q}(\sqrt{-3})$ i existeix un primer $\ell \equiv 1 \mod 3$ dividint D, aleshores $X_D(K) = \emptyset$.*

Notem que, si $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, les mateixes hipòtesis del Teorema 5.1 ja impliquen que $X_D(K) = \emptyset$. I en el cas en què $K = \mathbb{Q}(\sqrt{-1})$ o $K = \mathbb{Q}(\sqrt{-3})$, la hipòtesi que cal afegir per tal que $X_D(K) = \emptyset$ és una condició ben senzilla i explícita.

D'aquesta manera, com que les hipòtesis d'aquest resultat són explícites i calculables, podem produir parells (B_D, K) tals que K és deficient per X_D, és a dir, tal que $X_D(K) = \emptyset$. De fet, usant el treball de Jordan i Livné en [**JL85**] podem donar condicions suficients explícites perquè X_D sigui un contraexemple al principi de Hasse sobre K. En la següent secció analitzem aquest fet.

2. El principi de Hasse i els parells excepcionals

El fet que diferencia el Teorema 5.1 del Teorema 3.5, i que fa que sigui rellevant i novedós, és que ens permet produir *parells excepcionals* (B_D, K). Seguint la terminologia de [**Jor86**], un parell (B_D, K) format per una àlgebra de quaternions racional i indefinida B_D i un cos quadràtic imaginari K és *excepcional* si $X_D(K_v) \neq \emptyset$ per a tota plaça v de K i K no escindeix B_D.

Per a aquests parells, la dificultat en l'estudi dels punts K-racionals en X_D rau en el fet que les superfícies abelianes (A, ι) amb QM per B_D parametritzades per punts en $X_D(K)$ no admeten un model racional sobre K. És per això que els resultats de Jordan no s'apliquen en aquests casos. En canvi, la nostra aproximació fent servir les representacions de Galois associades a punts en corbes de Shimura introduïdes en el capítol anterior ens permet estendre les idees de Jordan i Skorobogatov per donar condicions suficients per tal que $X_D(K)$ sigui buit.

Després dels resultats presentats en la secció anterior, si (B_D, K) és un parell excepcional satisfent les hipòtesis del Corol·lari 5.2, en particular s'obté que X_D és un contraexemple al principi de Hasse sobre K. En tal cas direm que el parell (excepcional) (B_D, K) *viola el principi de Hasse*.

Dit d'una altra manera, si (B_D, K) és un parell satisfent les hipòtesis del Corol·lari 5.2 per al qual K no escindeix B_D, aleshores comprovar que (B_D, K) és un parell excepcional violant el principi de Hasse es redueix a provar que $X_D(K_v)$ és no buit per a tota plaça v de K. Fent servir els resultats de Jordan i Livné [**JL85**] sobre punts locals en corbes de Shimura, aquesta darrera condició pot comprovar-se computacionalment. Recordem primer algunes notacions introduïdes a [**JL85**].

Per a un ordre R en un cos quadràtic imaginari K', escriurem

$$S(R) = \frac{h(R)}{[R^\times : \mathbb{Z}^\times]} \prod_{\substack{q \mid D \\ q \text{ primer}}} (1 - \{\frac{R}{q}\}),$$

on $h(R)$ és el nombre de classes de R, i per a un primer racional q,

$$\{\frac{R}{q}\} = \begin{cases} 1 & \text{si } q \mid \mathrm{cond}(R), \\ (\frac{K'}{q}) & \text{altrament.} \end{cases}$$

Notem que $S(R) \neq 0$ si, i només si, el conductor de R és primer amb D i K' escindeix B_D. Aleshores, definim

$$\Sigma_\ell(D) = \frac{1}{2} \sum_{\substack{s \in \mathbb{Z} \\ s^2 < 4\ell}} \sum_R S(R),$$

on R recorre el conjunt d'ordres en cossos quadràtics imaginaris K' tals que R conté les arrels de $x^2 + sx + \ell$.

El següent corol·lari simplement afegeix a les hipòtesis del Corol·lari 5.2 les condicions que se segueixen del treball de Jordan i Livné per tal que X_D tingui punts localment arreu sobre K:

Corol·lari 5.3. *Sigui $g = g(X_D)$ el gènere de X_D. Sota les hipòtesis del Corol·lari 5.2, suposem també que se satisfan les següents condicions:*

(i) *$\Sigma_\ell(D) \neq 0$ per a tot primer $\ell < 4g^2$, $\ell \nmid D$, ℓ no inert en K.*

(ii) *Per a tot primer $\ell \mid D$ ramificant en K, o bé $\mathbb{Q}(\sqrt{-\ell})$ escindeix B_D o bé $\ell = 2$ i $\mathbb{Q}(\sqrt{-1})$ escindeix B_D.*

(iii) *Per a tot primer $\ell \mid D$ que descomposi en K, o bé $D = 2\ell$ amb $\ell \equiv 1 \mod 4$, o bé $\ell = 2$ i $D = 2q_1 \cdots q_{2r-1}$ amb primers $q_i \equiv 3 \mod 4$ que no descomposen en K.*

Aleshores X_D és un contraexemple al principi de Hasse sobre K.

Demostració. L'enunciat se segueix directament del treball en [**JL85**], junt amb el fet que $X_D(\mathbb{Q}_\ell) \neq \emptyset$ per a tot primer $\ell > 4g^2$, per la fita de Weil. □

En la Taula 5.1 a la pàgina següent recollim alguns exemples de parells excepcionals (B_D, K) que violen el principi de Hasse, obtinguts mitjançant càlculs basats en el Corol·lari 5.3. En la primera columna trobem discriminants de la forma $D = 2p$, amb p primer, i en la segona columna alguns cossos quadràtics imaginaris K per a cada discriminant D tals que (B_D, K) és un parell excepcional violant el principi de Hasse. Així, per a cada parell (D, K) de la taula tenim que K no escindeix B_D, $X_D(K) = \emptyset$ i $X_D(K_v) \neq \emptyset$ per a tota plaça v de K.

Finalment, volem remarcar que, de la mateixa manera que en la interpretació de Skorobogatov dels resultats de Jordan, els contraexemples al principi de Hasse que sorgeixen del Corol·lari 5.3 estan explicats per la obstrucció de Brauer-Manin. De fet, aquest fet és gairebé immediat a partir de la prova del Teorema 5.1:

Proposició 5.4. *Sigui K un cos quadràtic imaginari en el qual un primer q és ramificat. Sigui $B_D \in \mathcal{B}_1(q)$ una àlgebra de quaternions racional i indefinida de discriminant D, amb D divisible per un primer $p \notin P_1(q)$, $p \geq 5$, tal que p no descomposa en K.*

(i) *Si $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, aleshores $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

(ii) *Si* $K = \mathbb{Q}(\sqrt{-1})$ *i existeix un primer* $\ell \equiv 1 \mod 4$ *dividint* D*, aleshores* $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

(iii) *Si* $K = \mathbb{Q}(\sqrt{-3})$ *i existeix un primer* $\ell \equiv 1 \mod 3$ *dividint* D*, aleshores* $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

Demostració. Com en el Corol·lari 5.2, les hipòtesis en qualsevol dels tres casos impliquen que $X_D(K) = \emptyset$.

Ara, suposem que $X_D(\mathbb{A}_K) \neq \emptyset$, doncs altrament no hi ha res a dir. Aleshores, enlloc de començar amb un punt global $P \in X_D(K)$, hauríem de procedir com segueix. Primer, suposem que existeix una successió de punts locals $P_v \in X_D(K_v)$, un per a cada plaça no arquimediana v de K, de manera que els caràcters locals corresponents $\phi_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$ donats per especialització del torsor f_p en P_v són la restricció d'un caràcter global $\phi : G_K \to \mathbb{F}_{p^2}^{\times 12}$. Per a cada punt P_v, podem escollir un parell $(A_v, \iota_v)/\bar{K}_v$ amb cos de mòduli K_v representant P_v, i llavors la prova del Teorema 5.1 s'aplica de pas per pas fins obtenir una contradicció, mostrant que una tal successió de punts locals no pot existir. Per tant, el conjunt de descens $X_D(\mathbb{A}_K)^{f_p}$ associat al torsor f_p és buit, i aplicant el teorema principal de la toeria del descens de Colliot-Thélène i Sansuc (vegeu [**Sko01**, Theorem 6.1.2]), se segueix el resultat. □

$D = 2 \cdot p$	K
$2 \cdot 23$	$\mathbb{Q}(\sqrt{-55})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-119})$
$2 \cdot 31$	$\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, $\mathbb{Q}(\sqrt{-183})$
$2 \cdot 43$	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-183})$
$2 \cdot 59$	$\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-119})$
$2 \cdot 67$	$\mathbb{Q}(\sqrt{-55})$
$2 \cdot 71$	$\mathbb{Q}(\sqrt{-119})$, $\mathbb{Q}(\sqrt{-143})$
$2 \cdot 79$	$\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, $\mathbb{Q}(\sqrt{-183})$
$2 \cdot 83$	$\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-119})$

Taula 5.1. Alguns parells (D, K) tals que (B_D, K) viola el principi de Hasse.

CAPíTOL 6

Apèndix: punts racionals en quocients d'Atkin-Lehner

Com abans, sigui B_D una àlgebra de quaternions racional i indefinida, $\mathcal{O}_D$ un ordre maximal en B_D i considerem la corba de Shimura X_D associada (la involució ϱ per a la tria d'una tripleta $(B_D, \mathcal{O}_D, \varrho)$ no serà rellevant).

Pel Teorema 3.1 degut a Shimura, sabem que $X_D(\mathbb{Q}) = \emptyset$. Tanmateix, si m és un divisor positiu de D i considerem el quocient $X_D^{(m)} := X_D/\langle\omega_m\rangle$ de la corba X_D per l'acció de la involució d'Atkin-Lehner ω_m, que és de nou una corba algebraica definida sobre $\mathbb{Q}$, és natural preguntar-nos si el conjunt $X_D^{(m)}(\mathbb{Q})$ de punts racionals és buit o no. En aquest apèndix, tractarem de respondre aquesta qüestió per a certs quocients d'Atkin-Lehner.

En el que segueix, denotarem per $\pi_m : X_D \to X_D^{(m)}$ la projecció natural de pas al quocient, que identifica un punt $P \in X_D(\bar{\mathbb{Q}})$ amb $\omega_m(P)$. L'aplicació π_m és genèricament 2-a-1, i el nombre de punts fixos de ω_m va ser calculat per Ogg a [**Ogg83**].

En [**RSY05**], Rotger, Skorobogatov i Yafaev van establir un criteri per a l'existència de punts locals en $X_D^{(m)}$ per a tota plaça de $\mathbb{Q}$, és a dir per tal que $X_D^{(m)}(\mathbb{A}_\mathbb{Q})$ sigui no buit. Això els va permetre provar que $X_{23\cdot127}^{(127)}$ és un contraexemple al principi de Hasse sobre $\mathbb{Q}$.

D'altra banda, Parent i Yafaev [**PY07**] van proposar un mètode per a estudiar punts racionals globals en quocients d'Atkin-Lehner de corbes de Shimura de la forma $X_{pm}^{(m)}$ amb p i m primers, $p \equiv 1 \mod 4$, $m \equiv 3 \mod 4$. Aquests quocients són instàncies del cas "no ramificat" segons la terminologia de Ogg (vegeu [**Ogg85**]). En [**PY07**] es donen condicions per tal que aquests quocients nomes continguin punts CM. Recentment, aquest treball ha estat completat per Gillibert en [**Gil10**], on les condicions de Parent-Yafaev es fan explícites.

Des d'un punt de vista modular, el problema d'estudiar punts racionals en quocients d'Atkin-Lehner de corbes de Shimura ha estat estudiat a [**BFGR06**] i [**Rot08**], i està relacionat amb una conjectura atribuïda a Coleman sobre varietats abelianes de tipus GL_2 sobre $\mathbb{Q}$ (vegeu [**BFGR06**, §1]). Usant resultats d'aquests dos articles, en el Teorema 6.4 i el Corol·lari 6.5 donem condicions suficients explícites per tal que un quocient d'Atkin-Lehner de la forma $X_{pm}^{(m)}$, amb $p \equiv m \equiv 3 \mod 4$ no tingui punts racionals. Així doncs, els exemples que sorgeixen d'aquests resultats són complementaris als obtinguts per Parent i Yafaev, i se situen en el cas "ramificat" segons la terminologia de Ogg.

Comencem considerant un punt racional $Q \in X_D^{(m)}(\mathbb{Q})$, i sigui $K/\mathbb{Q}$ el cos quadràtic imaginari tal que $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$. De [**Jor86**, p. 93] se segueix la següent observació:

Lema 6.1. *Si $2 \nmid D$, aleshores $B_P = B_D \otimes K \simeq \mathrm{M}_2(K)$.*

En altres paraules, pel Teorema 4.9, podem escollir una superfície abeliana (A, ι) amb QM definida sobre K tal que $P = [(A, \iota)]$. Entendre bé el cos K serà fonamental en la prova del Teorema 6.4 que provem més endavant. En primer lloc, notem el següent:

Lema 6.2. *La involució ω_m no té punts fixos si, i només si, el cos quadràtic imaginari $\mathbb{Q}(\sqrt{-m})$ no escindeix B_D.*

Demostració. Aquest fet se segueix immediatament del criteri de Hasse (vegeu Corol·lari 1.27) junt amb la fórmula per al nombre de punts fixos d'una involució d'Atkin-Lehner deguda a Ogg ([**Ogg83**]). □

En segon lloc, provem mitjançant tècniques de descens el següent lema:

Lema 6.3. *Si $\mathbb{Q}(\sqrt{-m})$ no escindeix B_D, aleshores K és no ramificat fora de D.*

Demostració. Pel lema anterior, la projecció $\pi_m : X_D \to X_D^{(m)}$ és no ramificada, i per tant és un $X_D^{(m)}$-torsor pel grup $\mathbb{Z}/2\mathbb{Z}$. D'acord amb el treball de Morita sobre models integrals de X_D (vegeu [**Mor81**]), π_m s'estén a un morfisme llis d'esquemes projectius llisos sobre $\mathrm{Spec}(\mathbb{Z}[1/D])$, i dóna lloc a un torsor per al grup $\mathbb{Z}/2\mathbb{Z}$, ara considerat com a $\mathrm{Spec}(\mathbb{Z}[1/D])$-esquema.

Com és ben sabut, els punts $\mathbb{Q}$-racionals de $X_D^{(m)}$ es poden recuperar a partir dels punts $\mathbb{Q}$-racionals en els torsors *torçats* de $\pi_m : X_D \to X_D^{(m)}$. Concretament,

$$X_D^{(m)}(\mathbb{Q}) = \bigcup_{\tau \in H^1(\mathbb{Q}, \{\pm 1\})} {}^{\tau}X_D(\mathbb{Q}),$$

on ${}^{\tau}X_D(\mathbb{Q})$ és una abreviació per ${}^{\tau}\pi_m({}^{\tau}X_D(\mathbb{Q}))$. Aquí, les classes de cohomologia $\tau \in H^1(\mathbb{Q}, \{\pm 1\})$ es corresponen amb els caràcters quadràtics de Galois $\tau : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$, i per tant estan en bijecció amb les extensions quadràtiques de $\mathbb{Q}$. Com que X_D no té punts reals, ens podem restringir als cossos quadràtics imaginaris. A més, aplicant [**SY04**, Lemma 1.1] o bé [**Sko05**, p. 106], si $L/\mathbb{Q}$ és una extensió quadràtica ramificada en un primer que no divideix D, aleshores ${}^{\tau_L}X_D(\mathbb{Q}) = \emptyset$, on $\tau_L : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ és el caràcter quadràtic corresponent a L. En altres paraules, només els caràcters quadràtics no ramificats fora de D contribueixen en la descomposició anterior de $X_D^{(m)}(\mathbb{Q})$.

En particular, com que $P \in X_D(K)$ i $\pi_m(P) = Q \in X_D^{(m)}(\mathbb{Q})$, la classe $\zeta(Q) \in \mathrm{H}^1(\mathbb{Q}, \{\pm 1\})$ del $\mathbb{Q}$-torsor donat per la fibra $X_{D,Q} \to Q$ és el caràcter quadràtic τ_K corresponent a l'extensió quadràtica $K/\mathbb{Q}$. En conseqüència, el punt Q prové d'un punt $\mathbb{Q}$-racional en la corba *torçada* ${}^{\tau_K}X_D$. Per la discussió anterior, K ha de ser no ramificat fora de D. □

Observem que aquest lema respon a la Proposició 1.3 enunciada a [**Rot08**] en un context més general, i és clau per provar el següent resultat.

Donat un nombre primer q, definim el conjunt $P_0(q)$ com el conjunt (finit) de tots els factors primers dels enters no nuls en el conjunt

$$\bigcup_{s,a} \{a^2 - sq\},$$

on la unió és sobre $s = 0, 1, 2, 3, 4$ i els enters a tals que $|a| \leq 2\sqrt{q}$. Per exemple, tenim $P_0(3) = \{2, 3, 5, 11\}$ i $P_0(5) = \{2, 3, 5, 7, 11, 19\}$.

Teorema 6.4. *Siguin p, m dos primers diferents, amb $p \equiv m \equiv 3$ mod 4 i $(\frac{m}{p}) = -1$. Si existeix un primer senar q tal que $p \notin P_0(q)$, $(\frac{q}{p}) = 1$ i $(\frac{q}{m}) = -1$, aleshores $X_{pm}^{(m)}(\mathbb{Q})$ conté només punts CM.*

Demostració. Suposem que existeix un punt no-CM $Q \in X_{pm}^{(m)}(\mathbb{Q})$, i sigui K el cos quadràtic imaginari tal que $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_{pm}(K)$. Com que $(\frac{m}{p}) = -1$ i $p \equiv 3 \mod 4$, tenim que

$$(\frac{-m}{p}) = (\frac{-1}{p})(\frac{m}{p}) = 1,$$

la qual cosa implica que $\mathbb{Q}(\sqrt{-m})$ no escindeix B_D. Pel Lema 6.3, tenim que K és no ramificat en els primers no dividint pm. Per tant, les úniques possibilitats per K són $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{-m})$, $\mathbb{Q}(\sqrt{-pm})$.

Tanmateix, la darrera opció queda exclosa perquè 2 ramifica en $\mathbb{Q}(\sqrt{-pm})$. Però el cas $\mathbb{Q}(\sqrt{-m})$ també pot ser exclòs. De fet, com que $(\frac{-m}{p}) = 1$, tenim que $-m$ és un quadrat en $\mathbb{Q}_p$. Això implica que ${}^{-m}X_{pm} \times \mathbb{Q}_p \simeq X_{pm} \times \mathbb{Q}_p$, però $X_{pm}(\mathbb{Q}_p) = \emptyset$ pels resultats de Jordan i Livné a [**JL85**]. En conseqüència tenim que $K = \mathbb{Q}(\sqrt{-p})$.

Ara, observem que $B_{pm} \simeq (\frac{-p,m}{\mathbb{Q}})$. Per tant, usant el Lema 6.1 i [**BFGR06**, Theorem 4.5], el punt Q es correspon, en la terminologia de [**Rot08**], a una *tripleta modular* $(\mathcal{O}_{pm}, R_m, \mathbb{Q}(\sqrt{-p}))$. Finalment, aplicant [**Rot08**, Theorem 1.4], es dedueix que $(\frac{-q}{m}) = -1$, però les noestres hipòtesis impliquen que

$$(\frac{-q}{m}) = (\frac{-1}{m})(\frac{q}{m}) = 1,$$

i per tant obtenim una contradicció, que prové del fet de suposar l'existència d'un punt no-CM $Q \in X_{pm}^{(m)}(\mathbb{Q})$. Per tant, $X_{pm}^{(m)}(\mathbb{Q})$ conté només punts CM. □

Per tal d'estudiar quan $X_D^{(m)}(\mathbb{Q})$ és buit, cal veure sota quines condicions no pot existir un punt CM en X_D racional sobre $\mathbb{Q}$. L'existència de punts CM en els quocients d'Atkin-Lehner $X_D^{(m)}$, així com els seus cossos de racionalitat, va ser estudiada de manera satisfactòria en [**GR06**], on es dóna una descripció detallada d'aquests objectes. Aleshores, usant [**BFGR06**, Proposition 5.1], que se segueix del treball en [**GR06**, §5], es pot deduir fàcilment el següent corol·lari:

Corol·lari 6.5. *Sota les hipòtesis del Teorema 6.4, si $p \neq 3, 7, 11, 19, 43, 67, 163$, aleshores $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$.*

Aquest resultat aporta un progrés significant respecte a [**RSY05**, Theorem 5.1] i [**RSY05**, Corollary 5.2]. Fixat un primer q, el Corol·lari 6.5 ens diu que $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ sempre que m i p siguin primers diferents tals que $p \notin P_0(q)$, $p \neq 3, 7, 11, 19, 43, 67, 163$, $p \equiv m \equiv 3 \mod 4$, $(\frac{m}{p}) = -1$, $(\frac{q}{p}) = 1$ i $(\frac{q}{m}) = -1$. Pel Teorema de Densitat de Čebotarev, existeixen infinites tries possibles per a m i p.

En la Taula 6.1, per a cada primer $p \equiv 3 \mod 4$, $3 \leq p < 200$, $p \neq 3, 7, 11, 19, 43, 67, 163$, recollim els primers $m \equiv 3 \mod 4$, amb $m < 200$, tals que p i m satisfan les hipòtesis del Corol·lari 6.5, de manera que $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ per a tot parell (p, m) que apareix en la taula.

p	m's tals que $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$
23	7, 11, 19, 43, 67, 79, 83, 103, 107, 199
31	3, 11, 23, 43, 79, 83, 127, 139, 151, 167, 179, 199
47	11, 19, 23, 31, 43, 67, 107, 127, 139, 151, 163, 179, 199
59	11, 23, 31, 43, 47, 67, 83, 103, 131, 151, 179, 191
71	7, 11, 23, 31, 47, 59, 67, 127, 139, 163
79	3, 7, 43, 47, 59, 71, 103, 107, 127, 139,191, 199
83	19, 43, 47, 67, 71, 79, 103, 107, 139, 163, 179
103	3, 11, 31, 43, 47, 67, 71, 127, 151, 191, 199
107	7, 31, 43, 59, 67, 71, 103, 127, 131, 139, 167, 179, 191
127	3, 7, 23,43, 59, 67, 83, 139, 151, 167
131	19, 23, 31, 47, 67, 71, 79, 83, 103, 127, 139, 163, 199
139	3, 19, 23, 43, 59, 103, 151, 179, 199
151	3, 7, 23, 67, 71, 79, 83, 107, 131, 163, 179, 199
167	23, 43, 59, 67, 71, 79, 83, 103, 131, 139, 151, 163
179	7, 11,23, 71, 79, 103, 127, 131, 163, 167
191	7, 11, 19, 31, 47, 71, 83, 127, 131, 139, 151, 167, 179
199	3, 11, 19, 59, 67, 71, 83, 107, 127, 163, 167, 179, 191

TAULA 6.1. Exemples que sorgeixen del Corol·lari 6.5.

Remarca 6.6. Aplicant el criteri per a l'existència de punts racionals localment arreu que es troba a [**RSY05**, Theorem 3.1], podem comprovar si un quocient d'Atkin-Lehner $X_{pm}^{(m)}$ satisfent les hipòtesis del Corol·lari 6.5 té punts racionals localment arreu. En tal cas, $X_{pm}^{(m)}$ serà un contraexemple al principi de Hasse sobre $\mathbb{Q}$.

Per exemple, escollint $p = 23$, $m = 107$, se segueix del Corol·lari 6.5 que $X_{23\cdot 107}^{(107)}(\mathbb{Q}) = \emptyset$. A més, es pot comprovar usant [**RSY05**, Theorem 3.1] que $X_{23\cdot 107}^{(107)}$ té punts racionals localment arreu, de manera que $X_{23\cdot 107}^{(107)}$ és un contraexemple al principi de Hasse. Aquest exemple ja va ser exposat a [**RSY05**], aplicant altres mètodes.

Conclusions

En aquest treball s'ha tractat el problema de l'existència de punts racionals sobre cossos quadràtics imaginaris en corbes de Shimura. Aquestes corbes admeten una interpretació en termes de mòduli per a superfícies abelianes amb multiplicació quaterniònica. Aleshores, l'estudi de les representacions de Galois en certs subgrups de torsió d'aquestes superfícies abelianes permet abordar el problema de manera prou satisfactòria.

Sota les hipòtesis de treball de [**Jor86**] i [**Sko05**], la no existència de superfícies abelianes amb multiplicació quaterniònica per una àlgebra de quaternions de divisió racional i indefinida B_D definides sobre un cos quadràtic imaginari K que escindeix B_D equival a la no existència de punts K-racionals en X_D. En canvi, en aquest treball hem presentat resultats anàlegs sense suposar que les superfícies abelianes parametritzades per X_D admeten un model racional sobre el seu cos de mòduli. Això ha estat possible gràcies a les representacions de Galois introduïdes en el Capítol 4, associades a punts en la corba de Shimura X_D.

Pel fet que les idees del Capítol 4 s'emmarquen en un context força general, aquest treball obre les portes a investigar nous problemes. Per exemple, sembla natural pensar que un resultat similar al Teorema 5.1 podria ser demostrat per al cas de varietats de Shimura de dimensió superior, sobre les quals hem fet un breu incís en el Capítol 2.

Un altre problema interessant és el d'estudiar l'existència de punts racionals en quocients d'Atkin-Lehner de corbes de Shimura. En el Capítol 6 hem vist un primer petit resultat, però fent servir els treballs en [**BFGR06**], [**Rot04**] i [**Rot08**], es pot demostrar un resultat similar al Teorema 5.1 per a quocients d'Atkin-Lehner de corbes de Shimura. És a dir, es poden trobar condicions suficients explícites sobre una àlgebra de quaternions racional i indefinida B_D, i sobre un divisor m de D, per tal de poder assegurar que $X_D^{(m)}(\mathbb{Q}) = \emptyset$. Per aconseguir-ho, d'una banda és fàcil veure que a partir del recobridor de Shimura $Z_{D,p} \to X_D$ associat a un factor primer de D es pot construir un recobridor $Z_{D,p}^{(m)} \to X_D^{(m)}$ amb les mateixes propietats. I d'altra banda, cal descriure la interpretació modular del quocient d'Atkin-Lehner $X_D^{(m)}$. Actualment, aquest problema ja s'està estudiant (els detalls apareixeran a [**dVR**]).

Per últim, es pot explorar també l'obstrucció de Brauer-Manin en corbes de Shimura i els seus quocients d'Atkin-Lehner, per tal d'investigar si aquesta és l'única obstrucció al principi de Hasse en aquestes corbes.

Bibliografia

[AB04] M. Alsina, P. Bayer, *Quaternion orders, quadratic forms and Shimura curves*, CRM Monograph Series, vol. 22, Amer. Math. Soc., Providence, RI, 2004.

[BB66] W. L. Baily, A. Borel, Compactification of arithmetic quotients of bounded symmetric domains, *Ann. of Math.* **84** (1966), 443-507.

[BFGR06] N. Bruin, V. Flynn, J. Gonzàlez, V. Rotger, On finiteness conjectures for endomorphism algebras of abelian surfaces, *Math. Proc. Camb. Phil. Soc.* **141:3** (2006), 383-408.

[BHC62] A. Borel, Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. of Math.* **75** (1962), 485-535.

[BL92] C. Birkenhake, H. Lange, *Complex Abelian Varieties*, Gundl. math. Wiss., vol. 302, Springer, 1992.

[dVR] C. de Vera-Piquero, V. Rotger, Rational points on Atkin-Lehner quotients of Shimura curves, en progrés.

[ES01] J. S. Ellenberg, C. Skinner, On the modularity of $\mathbb{Q}$-curves, *Duke Math. J.* **109** (2001), 97-122.

[GS06] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.

[Gil10] F. Gillibert, *Points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura de discriminant pq*, preprint 2010, `arXiv:1012.3414v1`.

[GR06] J. González, V. Rotger, Non elliptic Shimura curves of genus one, *J. Math. Soc. Japan* **58:4** (2006), 927-948.

[Har77] R. Hartshorne, *Algebraic Geometry*, GTM vol. 52, Springer, 1977.

[Jor81] B. W. Jordan, *On the Diophantine arithmetic of Shimura curves*, Harvard PhD. Thesis (1981).

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

[JL85] B. Jordan, J. Livné, Local diophantine properties of Shimura curves, *Math. Ann.* , **270** (1985), 235-248.

[Kat92] S. Katok, *Fuchsian Groups*, Chicago Lectures in Mathematics, The University of Chicago Press, 1992.

[Maz78] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129-162.

[Mil79] J. S. Milne, Points on Shimura varieties mod p, en *Proc. Sympos. Pure Math.*, **33**, *Amer. Math. Soc.*, Providence, 1979, 165-184.

[Mil86] J. S. Milne, Abelian varieties, en *Arithmetic geometry*, G. Cornell, J. H. Silverman (eds.), Springer-Verlag, 1986, 103-150.

[Mil08] J. S. Milne, Abelian Varieties (v2.00), disponible en `www.jmilne.org/math/`, 2008.

[Mol10] S. Molina, Equations of hyperelliptic Shimura curves, (2010), enviat per publicació.

[Mor81] Y. Morita, Reduction modulo $\mathfrak{P}$ of Shimura curves, *Hokkaido Math. J.* , **10** (1981), 209-238.

[Mum70] D. Mumford, *Abelian Varieties*, Oxford University Press, 1970.

[Ogg83] A. P. Ogg, Real points on Shimura curves, en *Arithmetic and geometry, Vol. I*, Progress in Math., vol. 35, Birkäuser, 1983, 277-307.

[Ogg85] A. P. Ogg, Mauvaise réduction des courbes de Shimura. In: Séminaire de théorie des nombres, Paris 1983-1984, pp. 199-217, Progr. Math., 59, Birkhäuser Boston, Boston, MA (1985).

[Oht64] M. Ohta, On ℓ-adic representations of Galois groups obtained from certain two dimensional abelian varieties, J. Fac. Sci. Univ. Tokyo, Sec IA, **21** (1974), 299-308.

[Pie82] R. S. Pierce, *Associative Algebras*, GTM vol. 88, Springer-Verlag, 1982.

[Poo06] B. Poonen, Heuristics for the Brauer-Manin obstruction for curves, *Experimental Math.* **15:4** (2006), 415-420.

[Poo] B. Poonen, Rational points on varieties, Course notes 2003/2008, disponible en `http://math.mit.edu/~poonen/`.

[PY07] P. Parent, A. Yafaev, Proving the triviality of rational points on Atkin-Lehner quotients of Shimura curves, *Math. Ann.* **339** (2007), 915-935.

[Rot03] V. Rotger, Quaternions, polarizations and class numbers *J. Reine Angew. Math.* **561** (2003).

[Rot04] V. Rotger, Modular Shimura varieties and forgetful maps, *Trans. Amer. Math. Soc.* **356** (2004), 1535-1550.

[Rot08] V. Rotger, Which quaternion algebras act on a modular abelian variety?, *Math. Res. Letters* **15** (2008), 251-263.

[RSY05] V. Rotger, A. Skorobogatov, A. Yafaev, Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\mathbb{Q}$, *Moscow Math. J.* , **5:2**, (2005) 463-476.

[Ser72] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* , **15** (1972), 259-331.

[Shi63] G. Shimura, On analyitic families of polarized abelian varieties and automorphic functions, *Ann. Math.* **78** (1963), 149-192.

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

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

[Shi75] G. Shimura, On the real points of an arithmetic quotient of a bounded symmetric domain, *Math. Ann.* **215** (1975), 135-164.

[Sij10] J. Sijsling, *Equations for arithmetic pointed tori*, PhD. Thesis (2010).

[Sil92] A. Silverberg, Fields of definition for homomorphisms of abelian varieties, *J. Pure Appl. Algebra* **77** (1992), 253-262.

[SS03] S. Siksek, A. Skorobogatov, On a Shimura curve that is a counterexample to the Hasse principle, *Bull. London Math.* **35** (2003), 409-414.

[Sko01] A.N. Skorobogatov, *Torsors and rational points*, Cambridge University Press, 2001.

[Sko05] A. Skorobogatov, Shimura coverings of Shimura curves and the Manin obstruction, *Math. Res. Lett.* **12** (2005), 779-788.

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

[Vig80] M. F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes Math. **800**, 1980.

[Wei56] A. Weil, The field of definition of a variety, *Amer. J. Math.* **78** (1956), 509-524.