Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura

Montserrat Alsina i Aubach

UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques
Departament d'Àlgebra i Geometria

ARITMÈTICA D'ORDRES QUATERNIÒNICS I UNIFORMITZACIÓ HIPERBÒLICA DE CORBES DE SHIMURA

Montserrat Alsina i Aubach

ARITMÈTICA D'ORDRES QUATERNIÒNICS I UNIFORMITZACIÓ HIPERBÒLICA DE CORBES DE SHIMURA

Memòria presentada per a optar al grau de
doctora en Matemàtiques per

Montserrat Alsina i Aubach

Universitat de Barcelona, 1999

Departament d'Àlgebra i Geometria

Programa de Doctorat d'Àlgebra i Geometria, bienni 1989-1991

Doctorant: Montserrat Alsina i Aubach

Tutora i directora de tesi: Dra. Pilar Bayer i Isant

Pilar Bayer i Isant, catedràtica d'Àlgebra

de la Facultat de Matemàtiques de la Universitat de Barcelona,

FAIG CONSTAR

que la senyora Montserrat Alsina i Aubach ha realitzat aquesta memòria per a optar al grau de doctora en Matemàtiques sota la meva direcció.

Barcelona, desembre de 1999

P. Bayer

Signat: Pilar Bayer i Isant

Als meus fills, Mireia, Pau i ...

Introducció

> *Envisageons une forme quadratique indéfinie F à coefficients entiers* [...]. *Considérons le groupe principal de F formé de toutes les substitutions à coefficients entiers qui n'altèrent pas cette forme.* [...] *au groupe principal de F correspondra un groupe fuchsien G, qui sera le groupe fuchsien principal de F.*
>
> *H. Poincaré* [Poi1887]

L'estudi dels grups fuchsians i les funcions automorfes associades s'inicià en el segle XIX, principalment en els treballs de H. Poincaré, R. Fricke i F. Klein. Un grup fuchsià $\Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$ actua en el semiplà superior complex $\mathcal{H}$ i el quocient $\Gamma\backslash\mathcal{H}$ s'identifica amb una superfície de Riemann. Poincaré emprà també les formes quadràtiques ternàries indefinides en l'estudi dels grups fuchsians. Posteriorment, Fricke i Klein [Fri1893] [FK1897] prosseguiren aquest estudi.

En el cas dels grups fuchsians commensurables amb subgrups de $\mathrm{SL}(2,\mathbb{Z})$, la superfície de Riemann associada no és compacta. Aquest fet permeté la creació d'una teoria aritmètica de funcions automorfes desenvolupables en sèrie de Fourier a l'entorn de les puntes. Ara bé, quan la superfície de Riemann és compacta això no és possible, la qual cosa féu que durant dècades no s'estudiés aquest cas.

A partir dels anys seixanta, al llarg de nombrosos treballs, G. Shimura considerà l'acció de grups fuchsians donats per subgrups d'unitats d'àlgebres de quaternions en el semiplà de Poincaré, i inclogué el cas compacte i no compacte. En un dels seus treballs esmenta el punt de vista de Poincaré:

> [...] *part of the paper is devoted to the theory of a certain type of automorphic functions of one variable known in the literature as functions belonging to indefinite ternary quadratic forms* [Poi1887], [FK1897]. *They occur as moduli of abelian varieties of dimension* 2 *whose endo-*

> *morphismrings are isomorphic to an order of an indefinite quaternion algebra.*
>
> *G. Shimura* [Shi59]

Posteriorment, Shimura estengué la teoria al cas de diverses variables.

Denotem per $\mathbb{H}$ el cos dels quaternions de Hamilton. Sigui K un cos de nombres totalment real de grau d i considerem una àlgebra de quaternions H sobre K. Suposem que $H \otimes_{\mathbb{Q}} \mathbb{R} = \mathrm{M}(2,\mathbb{R})^r \times \mathbb{H}^{d-r}$ amb $0 < r \leq d$ i fixem un ordre $\mathcal{O} \subseteq H$. El grup d'unitats de $\mathcal{O}$ de norma positiva $\Gamma \subseteq \mathrm{SL}(2,\mathbb{R})^r$ actua de forma pròpia i discontínua en $\mathcal{H}^r$. El quocient $\Gamma\backslash\mathcal{H}^r$ s'identifica amb els punts complexos d'una varietat algebraica de dimensió r.

Shimura perfilà una teoria, cada cop més àmplia, al voltant d'aquests grups i les varietats associades. Pels seus resultats, en especial per la construcció de models canònics, les varietats reberen el nom de varietats de Shimura.

Els treballs de Shimura despertaren l'interès d'altres autors donant com a fruit diversos treballs, distribuïts de forma irregular en el temps. Avui dia l'estudi de les corbes i, més generalment, de les varietats de Shimura ha mostrat ser un tema d'interès creixent en teoria de nombres, ja que intervenen en la demostració de resultats importants.

Aquesta memòria aporta una contribució a l'estudi de les corbes de Shimura des d'un punt de vista efectiu.

En aquesta introducció descrivim primerament alguns aspectes dels treballs de Shimura i d'altres autors, i esmentem algunes aplicacions centrades en el cas de les corbes de Shimura. Després d'unes consideracions generals on manifestem l'objectiu de la memòria, citem resultats d'altres autors que hem necessitat per al nostre treball. Finalment, detallem el contingut de la memòria, donant una descripció per capítols de les nostres aportacions.

Els models canònics de Shimura

Una de les aportacions principals de Shimura, en el tema que ens ocupa, és la demostració de l'existència d'un model canònic S_K per a les varietats algebraiques $\Gamma\backslash\mathcal{H}^r$, de dimensió r. A aquest efecte, Shimura utilitzà espais de moduli associats a sistemes de varietats abelianes amb multiplicació quaterniònica. Cal distingir dos casos extrems especialment significatius: $r = 1$ o bé $r = d$.

Si $K = \mathbb{Q}$, els dos casos coincideixen, ja que $r = d = 1$. Si l'àlgebra de quaternions és $H = \mathrm{M}(2, \mathbb{Q})$, les corbes que en resulten són les corbes modulars clàssiques. Si $K \neq \mathbb{Q}$, els casos $r = 1$ i $r = d$ són ben diferents. El cas $r = d$ correspon a una K-àlgebra de quaternions H totalment indefinida. En aquest cas, Shimura demostrà l'existència i la unicitat d'un model canònic utilitzant espais de moduli associats a una família de varietats abelianes amb estructures de nivell, cf. [Shi63] i [Shi66]. El cas $r = 1 \neq d$ és el més complicat. En aquest cas, Shimura aconseguí la prova sobre l'existència i la unicitat del model canònic en considerar un nombre infinit de varietats de moduli, cf. [Shi67]. Així, la corba S_K no té sempre una interpretació modular directa.

Shimura generalitzà els resultats anteriors al cas de grups reductius que actuen en dominis simètrics acotats, cf. [Shi70a] i [Shi70b]. Aquest punt de vista fou generalitzat i axiomatitzat per Deligne [Del71] [Del79] i reprès per altres autors.

Dels treballs posteriors de Shimura, destaquem [Shi75], on estudià les varietats S_K sobre el cos dels nombres reals i provà que aquestes tenen punts reals si, i només si, $H = \mathrm{M}(2, K)$.

Al final de la memòria donem una llista de més d'un centenar de treballs de Shimura relacionats amb el tema.

Aportacions d'altres autors

A continuació, donem una breu pinzellada sobre treballs d'altres autors, referents a corbes de Shimura S_K. D'una banda, bona part dels treballs es restringeixen al cas que H sigui una àlgebra de quaternions sobre $\mathbb{Q}$. D'altra banda, molts dels resultats es restringeixen al cas que l'ordre quaterniònic sigui maximal. La majoria d'autors incorporen les dues restriccions.

En primer lloc, esmentem resultats referents al model de la corba sobre cossos locals i l'estudi de la reducció.

Sigui R l'anell d'enters del cos K. Fixem una plaça v finita de K i sigui K_v el completat de K en v. Cerednik [Cer76] fa una aportació important en demostrar l'existència d'una uniformització v-àdica de la corba S_K mitjançant subgrups aritmètics discrets de $\mathrm{PGL}(2, K_v)$. La demostració de Cerednik de l'existència d'un model de S_K sobre l'anell d'enters local R_v és indirecta. En aquest sentit, és destacable el treball de Drinfeld [Dri76] que proporciona una prova més directa del resultat anterior en el cas $K = \mathbb{Q}$, utilitzant la interpretació modular de les corbes de Shimura. Aquests resultats són bàsics per

a molts dels treballs posteriors. Cal esmentar l'existència de treballs dedicats a l'exposició dels resultats de Cerednik i Drinfeld, com ara [vdP89] i [BC91].

Per a les corbes modulars $X_0(N)$ i $X_1(N)$, la teoria de la reducció està estudiada i documentada en els treballs de Deligne-Rapoport [DR73] i Katz-Mazur [KM85]. En aquest cas, els primers p de bona reducció són els $p \nmid N$.

Els resultats referents a la reducció de les corbes de Shimura no modulars són necessàriament més complicats, ja que entra en joc un nou paràmetre, el discriminant D de l'àlgebra de quaternions. Per a les corbes de Shimura $S_{\mathbb{Q}}$, associades a un ordre d'Eichler $\mathcal{O}$ de nivell N d'una àlgebra de quaternions H de discriminant D, els primers p de bona reducció són precisament els $p \nmid DN$. Notem que si $H = \mathrm{M}(2,\mathbb{Q})$, aleshores $D = 1$. Hi ha resultats sobre la reducció de $S_{\mathbb{Q}}$ de Morita [Mor81] i, per a la corba S_K amb $K \neq \mathbb{Q}$, de Carayol [Car83] [Car86]. En aquesta línia, destaquem també els treballs d'Ihara [Iha68] [Iha69], Ogg [Ogg85] i el treball recent de Buzzard [Buz97], basat en la seva tesi.

Els resultats de Shimura sobre els models canònics S_K no són explícits. La demostració de la seva existència no dóna indicacions de com trobar una equació de la corba. Kurihara [Kur79] calcula l'equació d'algunes corbes de Shimura concretes de gènere ≤ 1 associades a un ordre maximal ($N = 1$). A aquest efecte, combina resultats de Shimura ([Shi67],[Shi70a] i [Shi75]) i resultats d'uniformització v-àdica. Jordan i Livné [Jor81] i Michon [Mic81a] calculen tres equacions més de gènere ≤ 1. Posteriorment, Kurihara [Kur94] presenta resultats parcials vers un possible càlcul d'equacions de corbes $S_{\mathbb{Q}}$ de qualsevol gènere.

El problema de la determinació de les corbes de Shimura hiperel·líptiques està resolt quan $K = \mathbb{Q}$ i $\mathcal{O}$ és un ordre d'Eichler. Ishii [Ish75] determina les corbes hiperel·líptiques corresponents a ordres maximals amb certes hipòtesis restrictives. Michon [Mic81b] resol totalment el cas d'ordre maximal, utilitzant resultats d'Ogg [Ogg74] relatius al cas modular. Ogg [Ogg83] i [Ogg85] completa la llista de corbes de Shimura $S_{\mathbb{Q}}$ hiperel·líptiques; estudia les involucions w de $S_{\mathbb{Q}}$ en el cas d'un ordre d'Eichler de nivell N i descriu els components connexos del conjunt de punts reals de la corba $S_{\mathbb{Q}}/ < w >$, utilitzant [Shi75] i resultats d'Eichler d'aritmètica de les àlgebres de quaternions, cf. [Eic55b] i [Vig80].

Jordan i Livné [Jor84] [JL85] donen criteris necessaris i suficients per a l'existència de punts de les corbes $S_{\mathbb{Q}}$ en els cossos locals $\mathbb{Q}_p$, per al cas d'ordre maximal. Ogg [Ogg85] tracta el cas d'ordre d'Eichler i caracteritza l'existència de punts de les corbes $S_{\mathbb{Q}}$ i $S_{\mathbb{Q}}/ < w >$ en els cossos locals $\mathbb{Q}_p$.

Per als primers de bona reducció, el problema es redueix a l'existència de punts de la corba reduïda sobre cossos finits, la qual es determina mitjançant la fórmula de les traces d'Eichler-Selberg; per als primers de mala reducció, cal utilitzar resultats d'uniformització de [Dri76] i [Kur79]. En [Jor86] hi ha resultats sobre $S_{\mathbb{Q}}(F)$, on F és un cos quadràtic imaginari. Jordan i Livné [JL87] tracten l'existència de divisors F-racionals i classes de divisors de grau d fixat, en el cas que F és una extensió finita de $\mathbb{Q}_p$. Kamienny [Kam90] obté resultats sobre la finitud del nombre de punts racionals d'algunes corbes de Shimura $S_{\mathbb{Q}}$ sobre cossos quadràtics. Molt recentment, Jordan i Livné [JL99] estudien propietats diofantines locals de quocients $S_{\mathbb{Q}}/ < w >$ per a certa família de corbes de Shimura $S_{\mathbb{Q}}$.

Els resultats anteriors sobre punts de corbes de Shimura són existencials i no donen cap informació explícita sobre els punts. En contraposició, destaquem el treball recent d'Elkies [Elk98], que calcula punts explícits en quocients $S_{\mathbb{Q}}/ < w >$ de corbes de Shimura de gènere ≤ 1 associades a un ordre maximal d'àlgebres de quaternions de discriminant $D = 6, 10, 14, 15$.

Dels treballs recents sobre corbes de Shimura destaquem també [Lin93], [Bes95], [HM95] i [Ji98].

Aplicacions de les corbes de Shimura

Les corbes de Shimura han esdevingut en els darrers anys una eina clau en l'estudi de problemes aritmètics i en la demostració de resultats importants.

L'article de K. Ribet [Rib80] marca l'entrada en joc de les corbes de Shimura en un nou escenari, en relacionar-les directament amb les corbes modulars. Partint de resultats d'Eichler [Eic58] i Shimizu [Shi65] sobre la fórmula de les traces, Ribet prova l'existència d'una isogènia entre la part nova de la jacobiana de la corba modular $X_0(N)$, amb N producte d'un nombre parell de primers diferents, i la jacobiana de la corba de Shimura associada a un ordre maximal d'una àlgebra de quaternions de discriminant N.

En la línia d'estudi de les representacions de Galois associades a formes modulars, les corbes de Shimura, i especialment les seves jacobianes, tenen, també de la mà de Ribet, un paper estratègic. Jordan i Livné [JL86] estudien la reducció del model de Néron de la jacobiana de la corba de Shimura $S_{\mathbb{Q}}$, en el cas d'ordre maximal, per als primers de mala reducció i determinen el grup de components connexos, utilitzant les descripcions del model regular de la corba sobre $\mathbb{Z}_p$, degudes a Drinfeld i Kurihara, i resultats de

Raynaud [Ray70] i Deligne-Rapoport [DR73]. Posteriorment, Ribet [Rib90] [Rib89], interrelaciona les reduccions del model de Néron de les jacobianes d'una corba de Shimura i d'una corba modular per a provar el cas particular de la conjectura (3.2.4?) de Serre [Ser87] conegut com a *conjectura epsilon*, amb la qual cosa queda demostrat que una part de la conjectura de Shimura-Taniyama-Weil implica l'últim teorema de Fermat. En [JL89] es demostren resultats sobre la cohomologia de certes corbes de Shimura, en la línia de generalitzar el resultat de Ribet a formes modulars de pes més gran que 2, i partint de resultats posteriors de Faltings i Jordan [FJ95]. En generalitzacions posteriors del treball de Ribet, cf. [Rib91], [BLR91] i [MR91], s'utilitzen i es puntualitzen altres resultats sobre corbes de Shimura. En [Rib94], el mateix autor en fa una descripció.

Entre els autors que segueixen la línia d'utilitzar corbes de Shimura per a aproximar-se a la conjectura de Serre, destaquem Diamond. Diamond i Taylor [DT94] donen resultats sobre corbes de Shimura anàlegs a resultats sobre corbes modulars. A aquest efecte, utilitzen la cohomologia dels models canònics, la reducció i la interpretació modular de les corbes de Shimura. En [Dia97a], amb vista a generalitzar resultats de [Rib90], Diamond utilitza corbes de Shimura anàlogues a les corbes modulars que provenen de grups de la forma $\Gamma_0(N) \cap \Gamma_1(N')$. Posteriorment tenim resultats de Ribet i Takahashi [RT97], Diamond [Dia97b], etc.

De resultes d'aquests treballs, les corbes de Shimura intervenen en la part de la conjectura de Shimura-Taniyama-Weil provada per Wiles [Wil95] i Taylor-Wiles [TW95]. En [DDT97] i [CSS97] es pot trobar una exposició del tema. Així doncs, les corbes de Shimura intervenen en la demostració del teorema de Fermat per partida doble.

Consideracions generals i objectiu de la memòria

Els comentaris anteriors mostren la necessitat i l'actualitat de l'estudi de les corbes de Shimura.

L'objectiu d'aquesta memòria és realitzar un apropament teoricopràctic a l'estudi de les corbes de Shimura, amb vista a l'obtenció de resultats numèrics que ens permetin una millor comprensió de les seves propietats.

Notem que la majoria de les aportacions descrites anteriorment no incideixen en aspectes efectius, la qual cosa, a més de dificultar-ne el seguiment, contrasta amb l'abundant experimentació numèrica duta a terme en el cas

modular. En aquest cas, comptàvem amb l'experiència adquirida en el Seminari de Teoria de Nombres (UB-UAB-UPC) de 1990-91, exposat en [BT92].

Els tractaments algorítmics de les corbes de Shimura i de les corbes modulars són essencialment diferents.

D'una banda, les corbes de Shimura es defineixen com a espais de moduli de superfícies abelianes, de les quals no se'n té informació numèrica. De l'altra, l'absència d'elements parabòlics en el grup fuchsià no permet utilitzar desenvolupaments de Fourier a l'entorn de puntes per a representar les funcions automorfes associades.

Les dificultats exposades ens han obligat a un canvi de paradigma. Tot semblà indicar que, per a desenvolupar un estudi algorítmic de les corbes de Shimura calia situar-les en un context més proper a l'àlgebra no commutativa, que fes paleses les propietats aritmètiques dels ordres. En aquest context, la relació inicial de Poincaré dels grups fuchsians i les formes quadràtiques ternàries indefinides és totalment natural i ens ha estat especialment valuosa.

Això ha motivat un canvi de llenguatge i la utilització d'eines d'àlgebra no commutativa per tal d'aconseguir efectivitat.

Grups fuchsians i formes quadràtiques

L'inici de l'estudi dels grups fuchsians en els treballs de Poincaré està lligat a la teoria de les formes quadràtiques. Shimura substituí el llenguatge algebraic de formes quadràtiques pel llenguatge geomètric de varietats abelianes.

De manera anàloga a la relació entre formes quadràtiques binàries i ordres dels cossos quadràtics, tenim una relació entre formes quadràtiques ternàries i ordres quaterniònics. Aquesta relació ens permet traslladar a un àmbit d'àlgebra no commutativa les necessitats de càlcul en corbes de Shimura. Així, com a eines algebraiques per a poder calcular hem considerat tant els ordres de les àlgebres de quaternions com les formes quadràtiques. En particular, això ha requerit l'estudi de treballs anteriors i posteriors a Shimura referents a àlgebres de quaternions i formes quadràtiques.

Com a resultats clàssics sobre les àlgebres de quaternions, citem els treballs d'Albert sobre la classificació de les àlgebres de divisió ([Alb34], [Alb35]). En aritmètica dels ordres quaterniònics, destaquen, evidentment, els treballs d'Eichler ([Eic37], [Eic38], [Eic55b], [Eic55a]), que donen nom als ordres que intervenen en aquesta memòria i n'estudien les classes d'ideals. Una re-

formulació d'aquests resultats clàssics es troba a Vigneras [Vig80]. Com a textos bàsics per a resultats generals sobre ordres de K-àlgebres, assenyalem Deuring [Deu68] i Reiner [Rei75]. En la dècada dels setanta, destaquem els treballs de Hijikata [Hij74], en els que intervenen ordres d'Eichler locals. Citem també els treballs de Pizer ([Piz73], [Piz76a], [Piz76b], [Piz80]), si bé són relatius a àlgebres de quaternions definides; en canvi, les àlgebres que intervenen en la construcció de les corbes de Shimura són indefinides. Takeuchi [Tak75] [Tak77a] [Tak77b] caracteritza els grups fuchsians que provenen d'àlgebres de quaternions i n'estudia els grups triangulars i les seves classes de commensurabilitat. En general, els resultats sobre ordres són poc explícits, sobretot per als ordres de $\mathbb{Q}$-àlgebres de divisió indefinides, amb diferències importants en les notacions i les definicions dels diferents treballs.

Per a l'estudi de les formes quadràtiques hem utilitzat des de treballs clàssics, com ara les *Disquisitiones Arithmeticae* de Gauss [Gau1801], fins a treballs més propers, com ara Ogg [Ogg69], Jones [Jon67], Serre [Ser73] i Lehman [Leh92]. Molts dels resultats es restringeixen a l'aritmètica de formes binàries de coeficients enters o de formes definides. Així mateix, notem també que les comandes sobre formes quadràtiques de programes d'ordinador habituals es redueixen pràcticament a formes binàries enteres.

Sobre correspondències entre formes quadràtiques i àlgebres de quaternions, destaquem els treballs clàssics de Latimer [Lat37], que establí una correspondència parcial, i els de Brandt ([Bra24], [Bra28], [Bra43]), on presentà una correspondència completa i introduí el concepte de K-forma. Els treballs de Brzezinski ([Brz80], [Brz82], [Brz83], [Brz90], [Brz95]), si bé fan ús de la relació entre formes quadràtiques i ordres d'una àlgebra de quaternions, se situen en l'estudi algebraic dels ordres de les àlgebres de quaternions. Per a les àlgebres definides, generalitza a ordres arbitraris certs resultats coneguts per als ordres d'Eichler, utilitzant descripcions dels grups d'automorfismes dels ordres. La correspondència completa entre formes ternàries i ordres quaterniònics ha estat recentment redemostrada, en termes d'àlgebres de Clifford, per Llorente [Llo]. La demostració és constructiva i permet el càlcul efectiu.

Destaquem també els treballs següents de Bayer-Travesa i Arenas-Bayer, que relacionen ordres quaterniònics, formes quadràtiques i punts de multiplicació complexa en el cas modular. En [BTc], els autors desenvolupen material bàsic per a un estudi aritmètic dels ordres de l'àlgebra de quaternions $\mathrm{M}(2,\mathbb{Q})$, que s'utiliza en [BTa] i [BTb]. En aquests dos treballs, relacionen la teoria de formes quadràtiques binàries enteres amb la teoria d'ordres de cossos quadràtics immersos en ordres de $\mathrm{M}(2,\mathbb{Q})$. Consideren diferents tipus d'immersions i

proven que l'estudi de les Γ-classes d'equivalència d'immersions és equivalent a l'estudi de les Γ-classes de certes formes quadràtiques binàries enteres. També determinen els nombres de classes corresponents mitjançant el control d'invariants numèrics adequats. En [ABb] consideren punts de multiplicació complexa de la corba modular $X_0(N)$ per a qualsevol discriminant quadràtic $d \neq 0$ i redueixen el seu estudi i l'avaluació del seu nombre al de certes formes quadràtiques binàries de coeficients enters de discriminant d. En [ABa] s'estudia un tipus especial d'aquests punts, que es presenten en nombre finit.

L'estudi numèric de l'acció dels grups fuchsians en el semiplà de Poincaré ha requerit també un estudi específic de geometria hiperbòlica i d'eines que s'hi utilitzen. En aquest sentit, destaquem el treballs de Ford [For51], Lehner [Leh64] i Siegel [Sie71], on es troben resultats sobre cercles d'isometria i la seva relació amb la construcció de dominis fonamentals.

Contingut de la memòria

Els principals resultats de la memòria fan referència a l'existència i propietats d'uniformitzacions hiperbòliques de corbes de Shimura, que s'obtenen per mitjà d'un estudi previ de l'aritmètica d'ordres de les àlgebres de quaternions.

El model canònic de les corbes de Shimura està caracteritzat per uns certs punts, anomenats punts de multiplicació complexa. En la memòria hem determinat aquests punts de manera explícita, a partir d'un conjunt de bijeccions que establim entre: classes d'immersions optimals d'ordres quadràtics imaginaris en ordres quaterniònics; classes de representacions primitives d'enters per formes quadràtiques ternàries enteres; classes de formes quadràtiques binàries de coeficients semi-enters en cossos quadràtics, definides; i els punts de multiplicació complexa de la corba de Shimura.

Aquest plantejament ens ha portat, en particular, al desenvolupament d'una teoria de classificació de formes quadràtiques binàries per certs subgrups discrets de $\mathrm{SL}(2,\mathbb{R})$, diferents del grup modular $\mathrm{SL}(2,\mathbb{Z})$.

Paral·lelament hem elaborat el paquet informàtic `Poincare`, implementat en *MapleV*, que manipula els diferents objectes que intervenen al llarg de la memòria: ordres d'àlgebres de quaternions, formes quadràtiques, objectes de geometria hiperbòlica, immersions, punts de les corbes de Shimura, etc. El paquet conté la implementació dels algoritmes obtinguts i permet realitzar càlculs efectius. Notem que en els treballs de Poincaré apareixien ja, directament o indirectament, la majoria d'aquests objectes, la qual cosa ens ha

semblat una bona raó per a donar aquest nom al paquet. Per tal de facilitar l'ús i la comprensió del paquet, comentem a cada capítol les instruccions que fan referència als conceptes i resultats del propi capítol, i en presentem una descripció completa final en el capítol 10.

A continuació descrivim el contingut de la memòria.

El capítol 1 està dedicat a les àlgebres de quaternions $H = \left(\frac{a,b}{K}\right)$, per a K un cos commutatiu de $\mathrm{char}(K) \neq 2$, i els seus ordres, que anomenarem ordres quaterniònics. Revisem definicions i resultats coneguts i introduïm conceptes que necessitarem en els capítols posteriors. En particular, presentem unes famílies infinites de $\mathbb{Q}$-àlgebres de quaternions indefinides, per a les quals donarem resultats explícits al llarg de la memòria. En la secció 1.1, es descriu la teoria algebraica de les K-àlgebres de quaternions. Les $\mathbb{Q}$-àlgebres de quaternions H de discriminant $D = 1$ són les $\mathbb{Q}$-àlgebres no ramificades; definim com a $\mathbb{Q}$-àlgebres de quaternions poc ramificades les que tenen discriminant $D = pq$, amb p, q primers, i les classifiquem en el teorema 1.1.31. En particular, a partir de la classificació de les àlgebres $H = \left(\frac{p,q}{\mathbb{Q}}\right)$, que donem en el teorema 1.1.29, introduïm els conceptes d'àlgebres poc ramificades de tipus A i de tipus B, cf. 1.1.30. La secció 1.2 està dedicada a la teoria aritmètica dels ordres quaterniònics, especialment dels ordres d'Eichler de nivell N en una $\mathbb{Q}$-àlgebra de quaternions de discriminant D, que denotem per $\mathcal{O}(D, N)$. Conté resultats sobre ordres d'Eichler locals i globals. Completem la secció amb resultats explícits sobre ordres d'Eichler de les àlgebres poc ramificades de tipus A i B. La secció 1.3 conté comentaris sobre els algoritmes que hem implementat i taules amb resultats numèrics. D'una banda, hi ha instruccions per tal d'operar en l'àmbit no commutatiu de les àlgebres de quaternions i per al càlcul dels seus invariants; d'altra banda, s'hi troben instruccions que permeten la manipulació dels ordres i les seves bases, com ara càlcul de bases simplificades i intersecció d'ordres. Amb aquestes instruccions, hem obtingut taules de classificació d'àlgebres de quaternions i taules d'ordres d'Eichler, per a àlgebres poc ramificades de tipus A i B.

En el capítol 2 s'introdueixen formalment les corbes de Shimura $X(D, N)$, definides a partir d'un ordre d'Eichler $\mathcal{O}(D, N)$, i calculem explícitament les constants de les corbes corresponents a ordres d'algunes àlgebres poc ramificades de tipus A i B. Comencem amb una breu descripció de conceptes propis de la geometria hiperbòlica en el semiplà de Poincaré, en la secció 2.1. En la secció 2.2 donem les definicions habituals per a les homografies i explicitem alguns resultats auxiliars per als capítols següents; destaquem

la relació entre una homografia γ i la forma quadràtica binària f_γ associada. En la secció 2.3 s'introdueixen els grups d'homografies quaterniòniques $\Gamma(D,N)$ a partir de les unitats dels ordres $\mathcal{O}(D,N)$ i els explicitem per a les àlgebres poc ramificades de tipus A i B. La secció 2.4 està dedicada a la definició de les corbes de Shimura $X(D,N)$ com a quocient $\Gamma(D,N)\backslash\mathcal{H}$ i recull resultats sobre les constants associades a $X(D,N)$. Finalment, en la secció 2.5 llistem les instruccions implementades referents a: geometria hiperbòlica, homografies i invariants de les corbes de Shimura, com ara el nombre de cicles el·líptics, el gènere i el volum. Hi incloem també taules explícites de constants d'algunes corbes de Shimura i, per raons de completesa, incloem les equacions conegudes de corbes de Shimura i la llista de corbes de Shimura no modulars hiperel·líptiques.

En el capítol 3 donem una uniformització hiperbòlica implementable de les corbes de Shimura per al cas no ramificat, $X(1,N) = X_0(N)$, de nivell N primer. Així, construïm de forma sistemàtica dominis fonamentals en el semiplà de Poincaré de la corba $X(1,N)$ i reobtenim resultats sobre les constants associades. La secció 3.1 conté definicions i resultats majoritàriament coneguts relatius als cercles d'isometria i un mètode de construcció de dominis fonamentals, seguint [For51]. En particular, introduïm el concepte de cercle d'isometria maximal. En la secció 3.2 apliquem l'anterior als grups d'homografies quaterniòniques per al cas no ramificat de nivell primer, $\Gamma(1,N)$ amb N primer. En primer lloc, fixem un domini fonamental del subgrup d'homografies que fixa l'infinit. A continuació, obtenim resultats sobre els cercles d'isometria maximals, proposició 3.2.1, que ens permeten donar resultats explícits sobre les constants i propietats del domini fonamental construït i les constants associades al grup $\Gamma(1,N)$, cf. teoremes 3.2.4 i 3.2.11. En la secció 3.3 presentem els gràfics dels dominis, les taules de constants i la descripció de les instruccions implementades. Les comandes d'aquest capítol fan referència sobretot al càlcul de constants i dades associades al grup $\Gamma(1,N)$ i al domini fonamental construït. A títol d'exemple, donem les representacions gràfiques dels dominis fonamentals construïts per a les corbes $X(1,N)$, amb $N = 3, 11, 13, 23, 41$, de gènere 1, 2 o bé 3; incloem també taules que mostren explícitament els corresponents vèrtexs $\Gamma(1,N)$-equivalents i una presentació del grup $\Gamma(1,N)/\pm\mathrm{Id}$. Una versió reduïda dels resultats d'aquest capítol està publicada a [Als99b]; per a una versió completa i detallada, cf. [Als99a].

El capítol 4 està dedicat a les formes quadràtiques, amb especial èmfasi en les formes binàries, ternàries i quaternàries, amb l'objectiu d'unificar i generalitzar notacions i definicions que utilitzarem en els capítols posteriors. En la secció 4.1 fixem les definicions i les notacions, que en algun cas generalitzen

definicions conegudes. En la secció 4.2 es resumeixen les nocions relatives a la teoria de representació i equivalència de formes quadràtiques. La secció 4.3 recupera i generalitza definicions i resultats de Brandt relatius a les formes recíproques i la propietat de ser K-forma. En la secció 4.4 es presenten propietats generals de formes quadràtiques associades a àlgebres sobre un cos K. En la secció 4.5 apliquem la secció anterior als cossos quadràtics respecte de la forma quadràtica norma. Així, tractem les formes nòrmiques binàries associades als ordres quadràtics i precisem notacions i resultats que utilitzarem en els capítols posteriors. La secció 4.6 conté les instruccions programades referents a formes quadràtiques, en especial per al càlcul d'invariants de les formes quadràtiques i les formes recíproques associades, la condició de ser K-forma i les formes binàries associades als ordres quadràtics.

En el capítol 5 tractem les formes quadràtiques quaternàries i ternàries obtingudes en interpretar una $\mathbb{Q}$-àlgebra de quaternions H com a espai quadràtic i considerar el subespai dels quaternions purs. La interpretació es pot fer en funció de la norma o de la traça, definides en H, i considerem les formes nòrmiques $n_{H,4}$ i $n_{H,3}$, i les formes traça $t_{H,4}$ i $t_{H,3}$, respectivament. Obtenim relacions entre els invariants d'aquestes formes i els invariants de l'àlgebra H. Els resultats per a les formes nòrmiques són a la secció 5.1; en especial, $n_{H,4}$ i $n_{H,3}$ són K-formes, cf. teorema 5.1.18. Els resultats corresponents a la forma traça són a la secció 5.2; en aquest cas, generalitzant el concepte de K-forma, obtenim el teorema 5.2.13. Els resultats anteriors ens permeten construir bijeccions entre conjunts de formes quadràtiques i d'àlgebres de quaternions, que explicitem en la secció 5.3, teorema 5.3.3. Aquestes bijeccions són efectives i han estat implementades en els dos sentits. En la secció 5.4 presentem les instruccions sobre les formes nòrmiques i les formes traça associades a una àlgebra de quaternions, referents als invariants i les formes quadràtiques associades, on també donem taules amb les formes i els invariants calculats.

El capítol 6 està dedicat a l'estudi de les formes quadràtiques associades als ordres quaterniònics $\mathcal{O} \subseteq H$, especialment les formes nòrmiques quaternària i ternària, que denotem per $n_{\mathcal{O},4}$ i $n_{\mathcal{O},3}$, respectivament, i el conjunt de formes binàries $\mathcal{H}(\mathcal{O})$ associat a un ordre. Donem resultats sobre la relació entre els invariants de l'ordre i les formes quadràtiques associades. En la secció 6.1 tractem les formes nòrmiques quaternària i ternària associades a un ordre quaterniònic. A més de l'estudi dels seus invariants, l'aplicació dels conceptes introduïts per Brandt ens ha permès arribar a resultats sobre la caracterització de les formes nòrmiques que són K-formes en el teorema 6.1.13. En el cas d'ordres d'Eichler d'àlgebres de quaternions indefinides, el criteri és més explícit, proposició 6.1.20, i provem la relació entre conjugació

d'ordres i equivalència de formes associades als ordres, teorema 6.1.23. En la secció 6.2 estudiem breument la forma traça quaternària $t_{\mathcal{O},4}$ associada a un ordre quaterniònic. En la secció 6.3 descrivim les formes binàries associades als ordres quaterniònics i donem resultats explícits per a ordres de les àlgebres no ramificades i les poc ramificades de tipus A i de tipus B. La secció 6.4 conté comentaris breus sobre les instruccions implementades i taules de formes quadràtiques associades a alguns ordres, que mostren les formes nòrmiques i els seus invariants, la forma traça i l'expressió genèrica de les formes binàries associades a ordres d'Eichler d'àlgebres poc ramificades.

En el capítol 7 reformulem la teoria d'immersions optimals d'ordres de cossos quadràtics en ordres d'àlgebres de quaternions, a partir de l'estudi de les formes quadràtiques ternàries i binàries associades als ordres. D'una banda, això ens ha permès obtenir resultats sobre formes quadràtiques; d'altra banda, ens ha aportat efectivitat al càlcul d'immersions. En la secció 7.1 relacionem les immersions de cossos quadràtics en àlgebres de quaternions amb les representacions de formes quadràtiques binàries per formes quaternàries i les representacions de nombres per formes ternàries. La secció 7.2 recull les definicions sobre immersions i els resultats de classificació coneguts per a les immersions optimals d'ordres quadràtics en ordres quaterniònics. En la secció 7.3 mostrem lligams entre la classificació de les immersions i la de les representacions de nombres per formes ternàries, cf. 7.3.16. En la secció 7.4 donem resultats sobre famílies de formes binàries de coeficients semi-enters en un cos quadràtic amb determinant fixat associades als ordres quaterniònics i sobre la seva classificació per subgrups discrets de $\mathrm{SL}(2,\mathbb{R})$ en el teorema 7.4.7. En particular, explicitem les bijeccions i els conjunts de formes binàries corresponents en el cas no ramificat i els casos poc ramificats de tipus A i de tipus B.

En el capítol 8 estudiem la uniformització hiperbòlica de les corbes de Shimura corresponents a àlgebres de divisió i presentem polígons hiperbòlics explícits que són dominis fonamentals per a algunes corbes de Shimura poc ramificades. En la secció 8.1 caracteritzem les homografies quaterniòniques a partir dels resultats d'immersions i formes quadràtiques del capítol anterior, cf. 8.1.7. En particular, estudiem les homografies el·líptiques, cf. teorema 8.1.10 i les explicitem per a les àlgebres poc ramificades de tipus A i B. Estudiem també les homografies hiperbòliques que fixen l'infinit i certes simetries, anàlogues a les del cas modular. Així, posem de manifest l'existència d'una homotècia principal que substitueix la translació del cas no ramificat i introduïm les rectes hiperbòliques principals. En la secció 8.2 donem pautes per a l'aplicació del mètode dels cercles d'isometria en la construcció de domi-

nis fonamentals: estudiem els dominis fonamentals del subgrup d'homografies que fixen l'infinit i els cercles d'isometria associats a la resta d'homografies quaterniòniques. En la secció 8.3 fem efectiva la construcció de dominis fonamentals. Explicitem polígons hiperbòlics que són dominis fonamentals i en descrivim les característiques, mostrant que aquesta uniformització té propietats similars a la calculada en el capítol 3 per al cas de les corbes modulars, pel que fa a les transformacions que fixen l'infinit i les simetries. En la secció 8.4 mostrem les representacions gràfiques dels dominis fonamentals explicitats en la secció anterior, per a les corbes de Shimura $X(6,1)$, $X(10,1)$ i $X(15,1)$. Hi adjuntem taules amb els cicles i la presentació dels grups. Alguns resultats parcials relacionats amb els presentats en aquest capítol es troben a [Als97].

En el capítol 9 estudiem els punts de multiplicació complexa de les corbes de Shimura $X(D,N)$ utilitzant els resultats sobre la uniformització hiperbòlica i el tàndem immersions-formes quadràtiques dels capítols anteriors. Considerem un conjunt finit d'ordres quadràtics per als quals hi ha punts de multiplicació complexa especials. En particular, per a les corbes de Shimura no ramificades i poc ramificades explicitem els resultats anteriors i en donem representacions gràfiques. En la secció 9.1, donem les definicions i els resultats que relacionen aquests punts amb les representacions de formes ternàries i les formes binàries del capítol anterior, de manera que comptem el nombre de punts de multiplicació complexa per un ordre quadràtic en el teorema 9.1.17. En la secció 9.2 donem els resultats sobre el càlcul dels punts de multiplicació complexa en funció de formes quadràtiques, cf. 9.2.1. Deduïm resultats per al cas no ramificat, i els casos poc ramificats de tipus A i de tipus B. Els resultats gràfics els hem recollit en la secció 9.3, on també comentem les instruccions programades. Més concretament, representem tots els punts de multiplicació complexa especials en els dominis fonamentals de les corbes $X(1,N)$ presentats en el capítol 3 i en els dominis de les corbes $X(D,1)$ presentats en el capítol 8. Les comandes implementades permeten classificar els ordres per als quals una corba $X(D,N)$ té punts de multiplicació complexa especials, obtenir la llista d'ordres quadràtics de multiplicació complexa especial i calcular els punts de multiplicació complexa per un ordre quadràtic fixat.

Finalment, en el capítol 10 recollim les instruccions del paquet informàtic `Poincare`, que conté la implementació en *MapleV* dels algoritmes descrits en els capítols anteriors. En la secció 10.1 donem les característiques tècniques generals del paquet. En la secció 10.2 donem una descripció completa de les instruccions implementades, especificant els arguments d'entrada i les sorti-

des. La secció 10.3 conté una petita mostra de la sintaxi de les instruccions, per a il·lustrar com han estat implementades.

En general, en el començament de cada capítol o secció, donem referències per als resultats coneguts, dels quals ometem la demostració, llevat d'algun cas en què ens ha semblat millor explicitar-la per tal de clarificar idees o de mostrar una demostració directa.

Agraïments

En cloure la introducció a la memòria, voldria expressar el meu agraïment a les persones que, d'una manera o altra, hi han contribuït.

Per començar, vull donar les gràcies als professors del Departament de Matemàtiques de la UAB, especialment de l'àrea d'àlgebra, que em van desvetllar l'interès per l'àlgebra i la teoria de nombres; als membres del Departament d'Àlgebra i Geometria de la UB, amb qui vaig compartir docència i cursos de tercer cicle, i als companys del Departament de Matemàtica Aplicada III de la UPC, especialment als membres de la Delegació del Bages que han entès la importància que té per a mi la recerca.

Vull agrair també els ànims i el suport dels companys del Seminari de Teoria de Nombres (UB-UAB-UPC), amb els quals he compartit hores i més hores d'exposicions, discussions i reunions.

Molt especialment, vull manifestar un sincer agraïment a la Dra. Pilar Bayer, per la seva confiança en mi, per la seva orientació i estímul, i per haver-me conduït a l'estudi de les corbes de Shimura, que ens ha arribat a fascinar a mesura que avançàvem en la realització i la maduresa d'aquest treball.

També ha estat important per a mi l'entorn familiar i d'amics més propers, que ha viscut la dedicació que requereixen les matemàtiques; d'una manera especial, el Pau i la Mireia, que comencen a descobrir els nombres i les lletres, i l'Enric, amb qui comparteixo, des de fa temps, més que matemàtiques.

En la discussió inicial sobre la programació de les instruccions referents a la manipulació dels quaternions, cal esmentar els comentaris i la col·laboració de Rafal Ablamowicz (Tennessee Technological University).

Finalment, remarquem que aquest treball ha estat realitzat amb el suport econòmic parcial de DGES, PB96-0166.

Índex

Capítol 1

Àlgebres de quaternions i ordres quaterniònics

En aquest capítol tractem les àlgebres de quaternions i els seus ordres. En donem les definicions i els resultats principals. Introduïm conceptes i noves interpretacions i presentem les àlgebres poc ramificades.

1.1 Teoria algebraica d'àlgebres de quaternions

En aquesta primera secció, considerem les àlgebres de quaternions sobre un cos commutatiu K de $\mathrm{char}(K) \neq 2$, amb especial èmfasi en les $\mathbb{Q}$-àlgebres, que són bàsicament les que tractarem al llarg del treball. En particular, introduïm les àlgebres poc ramificades, de tipus A i de tipus B. Com a referències principals citem [Ger79], [Alb34], [Rei75] i [Vig80].

Una K-àlgebra A (associativa i amb unitat) és un K-espai vectorial dotat d'una estructura d'anell amb unitat, 1_A, de manera que el producte intern de l'anell i el producte per un escalar estan relacionats per

$$k(uv) = (ku)v = u(kv), \quad u, v \in A,\ k \in K.$$

Els elements $\{k \cdot 1_A : k \in K\}$, a través de la immersió de K dins de A, són centrals; és a dir, $K \subseteq Z(A)$, on $Z(A)$ denota el centre de A. Una K-àlgebra A es diu que és central si $Z(A) = K$, i es diu que és simple si no té ideals bilaterals no trivials.

Un homomorfisme de K-àlgebres $\varphi : A \longrightarrow B$ és un homomorfisme d'anells K-lineal (inclou $\varphi(1_A) = 1_B$). De fet, és suficient que φ sigui un homomorfisme de K-espais vectorials tal que $\varphi(1_A) = 1_B$ i que preservi el producte sobre una base de A.

De la forma habitual, denotem per $\mathrm{M}(n, R)$ l'anell de les matrius $n \times n$ d'entrades en R, per $\mathrm{GL}(n, R)$ el grup lineal format pels elements de $\mathrm{M}(n, R)$ invertibles, i per $\mathrm{SL}(n, R)$ el subgrup especial lineal dels elements de $\mathrm{GL}(n, R)$ de determinant igual a 1.

1.1.1 Definicions i resultats

1.1.1 Definició. Una K-àlgebra de quaternions H és una K-àlgebra central, simple i de dimensió 4 sobre el seu centre. Denotem per H^* el grup de les unitats de H. □

Sobre un cos K de característica diferent de 2, tota àlgebra de quaternions H té una K-base $\{1, i, j, ij\}$ que satisfà les relacions $i^2 = a$, $j^2 = b$ i $ij = -ji$, per a certs $a, b \in K^*$. Anomenem base canònica de H aquesta base. Recíprocament, una K-base i unes relacions com les anteriors, a més de la propietat associativa, defineixen una K-àlgebra de quaternions. En aquest cas, denotem per $\left(\frac{a,b}{K}\right)$ l'àlgebra de quaternions H. Observem que parelles diferents poden donar lloc a K-àlgebres de quaternions isomorfes (cf. 1.1.10).

1.1.2 Definició. Un quaternió $\omega = x + yi + zj + tij$ de H es diu que és un quaternió pur si $x = 0$. Denotem per H_0 el K-espai vectorial dels quaternions purs. □

La noció de puresa és independent de l'elecció de la base $\{1, i, j, ij\}$, com mostra el resultat següent.

1.1.3 Proposició. *Sigui H unà K-àlgebra de quaternions i considerem $\omega \in H$, $\omega \neq 0$. Aleshores $\omega \in H_0$ si, i només si, $\omega \notin K$ i $\omega^2 \in K$.* □

Recordem els resultats següents sobre els automorfismes d'una K-àlgebra de quaternions.

1.1.4 Teorema. *Sigui H una K-àlgebra de quaternions.*

(i) *Els K-automorfismes de H són els automorfismes interns (és a dir, les conjugacions $\omega \mapsto \sigma^{-1}\omega\sigma$, on $\sigma \in H^*$). El grup $Aut_K(H)$ de K-automorfismes de H és isomorf al grup quocient H^*/K^*.*

(ii) *Si L és una K-àlgebra separable de rang 2, continguda en H, el subgrup d'automorfismes de H que fixen tots els elements de L és isomorf a L^*/K^*.* □

1.1.5 Corol·lari. *Siguin H una K-àlgebra de quaternions i $L \subseteq H$ una K-àlgebra quadràtica separable. Denotem per $m \mapsto m'$ el K-automorfisme no trivial de L. Aleshores, existeixen elements $\theta \in K^*$ i $\omega \in H$ tals que $H = L + L\omega$, amb $\omega^2 = \theta$ i $\omega m = m'\omega$ per a tot $m \in L$.* □

Una K-àlgebra de quaternions és o bé un cos no commutatiu, o bé una àlgebra isomorfa a l'àlgebra de matrius $\mathrm{M}(2, K)$; en el primer cas es diu que és una K-àlgebra de divisió i en el segon, que és una K-àlgebra de matrius. Si K és algebraicament tancat, obtenim només les àlgebres de matrius. Si K és un cos local ($\neq \mathbb{C}$), existeix una única K-àlgebra de quaternions de divisió, llevat isomorfisme. Si $K = \mathbb{R}$, s'obté el cos $\mathbb{H}$ dels quaternions de Hamilton.

A partir d'ara, K denotarà un cos de nombres i K_v, el cos local corresponent, per a cada plaça v de K. Denotem per R i R_v els anells d'enters corresponents.

1.1.6 Definició. Sigui H una K-àlgebra de quaternions. Per a cada plaça v de K, $H_v := H \otimes K_v$ és una K_v-àlgebra de quaternions. Si H_v és una àlgebra de divisió, es diu que H és ramificada en v; en cas contrari, es diu que H és no ramificada en v.

Siguin $H = \left(\frac{a,b}{K}\right)$ i v una plaça de K. Es defineix l'invariant (local) de Hasse per

$$\varepsilon\left(\frac{a,b}{K}\right)_v = \begin{cases} 1, & \text{si } v \text{ no ramifica en } H, \\ -1, & \text{si } v \text{ ramifica en } H. \end{cases}$$ □

1.1.7 Teorema. (i) *Per a qualsevol K-àlgebra de quaternions H, el conjunt de places de K on H és ramificada és finit i de cardinal parell.*

(ii) *Dues K-àlgebres de quaternions són isomorfes si, i només si, són ramificades en les mateixes places.*

(iii) *Donat un conjunt de places de K de cardinal parell, que no contingui cap plaça complexa, existeix una K-àlgebra de quaternions que és ramificada exactament en aquestes places.* □

Aquests fets es resumeixen en la successió exacta següent, on Br_2 denota la 2-component del grup de Brauer i $\varepsilon = \sum \varepsilon_v$ (cf. [Ser79]):

$$1 \to \mathrm{Br}_2(K) \to \bigoplus_v \mathrm{Br}_2(K_v) \xrightarrow{\varepsilon} \{\pm 1\} \to 1.$$

Notem que, si K és un cos global, existeixen infinites àlgebres de quaternions sobre K no isomorfes.

Si $K = \mathbb{Q}$, l'invariant local de Hasse de l'àlgebra de quaternions coincideix amb el símbol de Hilbert local $(a, b)_p$.

1.1.8 Definició. Es defineix el discriminant reduït D_H d'una K-àlgebra de quaternions H com l'ideal enter de R igual al producte de les places finites de K que ramifiquen en H. □

1.1.9 Corol·lari. *Dues K-àlgebres de quaternions són isomorfes si, i només si, tenen el mateix discriminant reduït. En particular, una K-àlgebra de quaternions H és una K-àlgebra de matrius si, i només si, $D_H = R$.* □

Si R és un domini d'ideals principals (DIP), podem identificar els ideals de R amb els seus generadors, llevat d'unitats. Així, en les $\mathbb{Q}$-àlgebres de quaternions posem $D_H \in \mathbb{Z}$. Les $\mathbb{Q}$-àlgebres de matrius, per exemple, es caracteritzen per $D_H = 1$.

1.1.10 Remarca. Sobre $\mathbb{Q}$, a partir de les propietats generals dels símbols de Hilbert locals, s'obtenen els isomorfismes següents, per a $a, b, c \in \mathbb{Q}$.

(i) $\mathrm{M}(2, \mathbb{Q}) \simeq \left(\frac{1,-1}{\mathbb{Q}}\right) \simeq \left(\frac{1,b}{\mathbb{Q}}\right) \simeq \left(\frac{a,-a}{\mathbb{Q}}\right) \simeq \left(\frac{a,1-a}{\mathbb{Q}}\right)$.

(ii) $\left(\frac{b,a}{\mathbb{Q}}\right) \simeq \left(\frac{a,b}{\mathbb{Q}}\right) \simeq \left(\frac{ac^2,bc^2}{\mathbb{Q}}\right)$.

(iii) $\left(\frac{a,ab}{\mathbb{Q}}\right) \simeq \left(\frac{a,-b}{\mathbb{Q}}\right)$.

Explicitem, com a exemple, un isomorfisme $\left(\frac{1,b}{\mathbb{Q}}\right) \simeq \mathrm{M}(2, \mathbb{Q})$. L'utilitzarem especialment quan $b = -1$.

$$\begin{array}{rccc} \psi: & \left(\frac{1,b}{\mathbb{Q}}\right) & \longrightarrow & \mathrm{M}(2,\mathbb{Q}) \\ & x + yi + zj + tij & \mapsto & \begin{pmatrix} x+y & z+t \\ b(z-t) & x-y \end{pmatrix}. \end{array}$$

L'isomorfisme invers ve donat per

$$\begin{array}{rccl} \psi^{-1}: & \mathrm{M}(2,\mathbb{Q}) & \longrightarrow & \left(\dfrac{1,b}{\mathbb{Q}}\right) \\ & \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \mapsto & \frac{1}{2}((\alpha+\delta)+(\alpha-\delta)i+(\beta+\frac{1}{b}\gamma)j+(\beta-\frac{1}{b}\gamma)ij). \ \square \end{array}$$

1.1.11 Remarca. La base canònica $\{1,i,j,ij\}$ de $\left(\dfrac{1,b}{\mathbb{Q}}\right)$, es transforma per l'isomorfisme ψ en la base de $\mathrm{M}(2,\mathbb{Q})$ següent:

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

En cert sentit, aquesta serà la base de $\mathrm{M}(2,\mathbb{Q})$ que farà el paper de base canònica. $\square$

1.1.12 Definicions. Tota K-àlgebra de quaternions està dotada d'un K-endomorfisme que és un antiautomorfisme involutiu i que anomenem conjugació; es denota per $\omega \mapsto \overline{\omega}$. Donat $\omega \in H$, es defineix la traça reduïda per $\mathrm{tr}(\omega) = \omega + \overline{\omega}$, i la norma reduïda, per $\mathrm{n}(\omega) = \omega \cdot \overline{\omega}$.

Sigui $H = \left(\dfrac{a,b}{K}\right)$. Si $\omega = x + yi + zj + tij$, amb $x,y,z,t \in K$, tenim que $\overline{\omega} = x - yi - zj - tij$, $\mathrm{tr}(\omega) = 2x$ i $\mathrm{n}(\omega) = x^2 - ay^2 - bz^2 + abt^2$. Observem que $\omega \in H_0$ si, i només si, $\overline{\omega} = -\omega$; de fet, H_0 és el conjunt de quaternions de traça reduïda nul·la. Els elements de H^* són els elements de norma reduïda no nul·la. $\square$

Sigui $H = \mathrm{M}(2,K)$ i identifiquem K amb la seva imatge a $\mathrm{M}(2,K)$, pel K-homomorfisme que envia l'element unitat de K a la matriu identitat. Aleshores, si $\omega = \begin{pmatrix} c & d \\ e & f \end{pmatrix}$, tenim que $\overline{\omega} = \begin{pmatrix} f & -d \\ -e & c \end{pmatrix}$. La traça i la norma reduïdes d'un element $\omega \in \mathrm{M}(2,K)$ coincideixen amb la traça i el determinant de ω com a matriu, respectivament.

1.1.13 Proposició. *Sigui H una K-àlgebra de quaternions. Aleshores, l'aplicació traça reduïda dóna lloc a una K-forma bilineal simètrica no degenerada $\tau : H \times H \to K$ en posar $\tau(\alpha,\beta) = \mathrm{tr}(\alpha\beta)$, per a $\alpha,\beta \in H$. A més, la forma τ és associativa; això és, $\tau(\alpha\beta,\gamma) = \tau(\alpha,\beta\gamma)$, per a $\alpha,\beta,\gamma \in H$.* $\square$

1.1.14 Teorema. *Sigui K_H el conjunt d'elements de K que són positius en les places infinites reals de K que ramifiquen en H. Aleshores, $K_H = \mathrm{n}(H)$.* $\square$

1.1.15 Teorema. *Sigui K un cos totalment real d'anell d'enters R. Sigui H una K-àlgebra de quaternions indefinida. Aleshores, per a tot $\delta \in R \cap H^*$, existeix $\omega \in H^*$ tal que $n(\omega) = \delta$ i $\mathrm{tr}(\omega) \in R$.* □

1.1.16 Proposició. *Sigui $\psi : H \longrightarrow H'$ un isomorfisme de K-àlgebres de quaternions. Sigui $H = \left(\frac{a,b}{K}\right)$, amb una base fixada $\{1, i, j, ij\}$. Es tenen les propietats següents:*

(i) $\psi(i)^2 = a, \quad \psi(j)^2 = b.$

(ii) $\psi(H_0) = H'_0.$

(iii) $\psi(\overline{\omega}) = \overline{\psi(\omega)}$, *per a* $\omega \in H.$

(iv) $\mathrm{n}(\psi(\omega)) = \mathrm{n}(\omega), \quad \mathrm{tr}(\psi(\omega)) = \mathrm{tr}(\omega)$, *per a* $\omega \in H.$

DEMOSTRACIÓ: La propietat (i) és trivial, ja que $\psi(i)^2 = \psi(i^2) = \psi(a) = a$; anàlogament es veu $\psi(i)^2 = b$.

Expressem $\psi(i), \psi(j), \psi(ij)$ en funció de la base de H'. L'apartat (i) implica que necessàriament pertanyen a H'_0. De fet, també és un corol·lari de la proposició 1.1.3, que caracteritza els quaternions purs de manera independent de la base. Com que ψ és un isomorfisme, obtenim la igualtat donada a (ii).

Per a provar (iii), sigui $\omega = k + u$, amb $k \in K$ i $u \in H_0$. Tenim que $\overline{\omega} = k - u$; per tant $\psi(\overline{\omega}) = k - \psi(u)$. Ara bé, si apliquem (ii) i les propietats de la conjugació, tenim que $k - \psi(u) = \overline{k + \psi(u)} = \overline{\psi(\omega)}$.

Per a veure (iv), només cal aplicar la definició d'homomorfisme de K-àlgebres. Explícitament, $\mathrm{n}(\psi(\omega)) = \psi(\omega)\overline{\psi(\omega)} = \psi(\omega)\psi(\overline{\omega}) = \psi(\omega\overline{\omega}) = \psi(\mathrm{n}(\omega)) = \mathrm{n}(\omega)$. Anàlogament, per a la traça, tenim que $\mathrm{tr}(\psi(\omega)) = \psi(\omega) + \overline{\psi(\omega)} = \psi(\omega) + \psi(\overline{\omega}) = \psi(\omega + \overline{\omega}) = \psi(\mathrm{tr}(\omega)) = \mathrm{tr}(\omega)$. □

1.1.17 Remarca. Notem que les aplicacions de H en H que transformen una K-base de H en una altra K-base de H són automorfismes de H com a K-espai vectorial, però no són necessàriament automorfismes de K-àlgebres. □

1.1.18 Definició. Siguin H una K-àlgebra de quaternions i F un cos extensió de K. Es diu que F escindeix H si $H_F := H \otimes_K F \simeq \mathrm{M}(2, F)$. □

Fixada una K-àlgebra de quaternions H, sempre existeix un cos $F \supseteq K$ que escindeix H. De fet, si $\overline{K}$ és una clausura algebraica de K, aleshores $\overline{K}$ escindeix H. És clar que si F escindeix H, aleshores qualsevol cos $L \supseteq F$ també escindeix H.

Sigui F un cos que escindeix H i fixem un isomorfisme $\varphi : H \otimes F \xrightarrow{\sim} \mathrm{M}(2, F)$. Aleshores, el determinant i la traça de la matriu $\varphi(\omega \otimes 1)$ coincideixen amb la norma i la traça reduïda de $\omega \in H$, respectivament. En particular, el determinant i la traça de la matriu $\varphi(\omega \otimes 1)$ no depenen ni de l'isomorfisme φ ni del cos F que escindeix H.

Vegem a continuació quines són les condicions que determinen que un cos quadràtic sobre K escindeixi una K-àlgebra de quaternions.

1.1.19 Proposició. *Siguin H una K-àlgebra de quaternions i F un cos quadràtic sobre K. Aleshores són equivalents:*

(a) *F escindeix H.*

(b) *F és K-isomorf a un subcos commutatiu maximal de H que conté K.*

(c) *Existeix una K-immersió $F \hookrightarrow H$.*

(d) *Tota plaça v de K que ramifica en H no descompon completament en F.* □

L'equivalència entre (b) i (c) és clara. L'equivalència de les condicions (a), (b) i (d) és un cas especial dels teoremes de Hasse per a àlgebres centrals simples sobre cossos de nombres. Se'n pot trobar una demostració senzilla i directa per al cas de $\mathbb{Q}$-àlgebres de quaternions a [Lat36]. Notem que la condició (d) es dedueix fàcilment de (c). Efectivament, si $v | D_H$, tenim que H_v és una K_v-àlgebra de divisió; per tant, per a què existeixi una immersió de F en H, cal que hi hagi una immersió de F_v en H_v, per la qual cosa F_v ha de ser un cos. Això implica que v no descompon en F.

1.1.20 Remarca. Per al cas de les K-àlgebres de quaternions que són àlgebres de matrius, és evident que tots els cossos quadràtics les escindeixen. Qualsevol cos quadràtic satisfà (d), ja que no hi ha cap plaça que ramifiqui en l'àlgebra. Si $F = K(\sqrt{\delta})$, amb $\delta \in K$, (b) i (c) clarament se satisfan en prendre la K-immersió següent:

$$\begin{array}{rccc} \psi : & K(\sqrt{\delta}) & \hookrightarrow & \mathrm{M}(2, K) \\ & x + y\sqrt{\delta} & \mapsto & \begin{pmatrix} x & y \\ \delta y & x \end{pmatrix}. \end{array}$$

Òbviament es conserven la norma i la traça. □

1.1.21 Proposició. *Una extensió finita $F|K$ escindeix una K-àlgebra de quaternions H si, i només si, F_w escindeix H_v per a tota plaça $w|v$ de F.* □

1.1.22 Remarca. A nivell local, per la remarca anterior ens podem centrar en els cossos que escindeixen les àlgebres de divisió H_v. En aquest cas, si K_v no és arquimedià, es té que tot cos quadràtic local F_w sobre K_v, amb $w|v$, escindeix H_v. En particular, aplicant 1.1.19, F_w és isomorf a un subcos de H_v. □

1.1.23 Remarca. Sigui $F = K(\alpha)$ un cos quadràtic que escindeix una K-àlgebra de quaternions H. Per la proposició 1.1.19 això equival a dir que existeix una immersió $\psi : F \hookrightarrow H$.

(i) Per ser ψ morfisme d'àlgebres, conserva la norma i la traça. Una immersió $\psi : F \hookrightarrow H$ queda determinada per un element $\psi(\alpha) \in H$ tal que $\mathrm{n}(\psi(\alpha)) = \mathrm{n}(\alpha)$ i $\mathrm{tr}(\psi(\alpha)) = \mathrm{tr}(\alpha)$.

(ii) Si $F \subset H$, aleshores el conjunt d'immersions de F en H està en bijecció amb la classe de conjugació de l'element $\psi(\alpha)$ en H^*, $\{\sigma^{-1}\psi(\alpha)\sigma \mid \sigma \in H^*\} = \{\omega \in H \mid \mathrm{n}(\omega) = \mathrm{n}(\alpha), \mathrm{tr}(\omega) = \mathrm{tr}(\alpha)\}$. □

1.1.24 Definició. Siguin K un cos de nombres totalment real, $[K : \mathbb{Q}] = m$, i H una K-àlgebra de quaternions. Fixem un isomorfisme $H \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}(2,\mathbb{R})^r \times \mathbb{H}^{m-r}$. Si $r = 0$, es diu que H és definida. Si $r \geq 1$, es diu que H és indefinida. □

En particular, en les $\mathbb{Q}$-àlgebres de quaternions, el caràcter definit o indefinit de l'àlgebra H es llegeix en el discriminant D_H: un nombre senar de factors de D_H correspon al cas definit i un nombre parell, al cas indefinit. Observem que $\mathbb{R}$ escindeix les $\mathbb{Q}$-àlgebres de quaternions indefinides. La proposició següent dóna una immersió explícita en aquest cas.

1.1.25 Proposició. *Sigui $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ una àlgebra de quaternions indefinida, amb $a > 0$. Aleshores, s'obté una immersió $\Phi : H \hookrightarrow \mathrm{M}(2,\mathbb{R})$ en posar:*

$$\Phi(x + yi + zj + tij) = \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}. \square$$

De fet, Φ és una immersió de H en les matrius $\mathrm{M}(2, \mathbb{Q}(\sqrt{a}))$. En aquest monomorfisme es comprova directament que el determinant i la traça de la matriu $\Phi(\omega)$ coincideixen amb la norma i la traça de l'element $\omega \in H$, respectivament.

1.1.2 $\mathbb{Q}$-àlgebres de quaternions no ramificades i poc ramificades

Considerem ara $\mathbb{Q}$-àlgebres de quaternions de la forma $H = \left(\frac{p,q}{\mathbb{Q}}\right)$, amb p i q nombres primers positius.

Denotem per $\left(\frac{\cdot}{\cdot}\right)$ el símbol multiplicatiu de residus quadràtics en sentit ampli; és a dir, per a un primer p senar és:

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{si } d \text{ és un quadrat no nul mòdul } p, \\ 0 & \text{si } p \mid d, \\ -1 & \text{si } d \text{ no és un quadrat mòdul } p, \end{cases}$$

i si $p = 2$ és:

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

1.1.26 Proposició. *Donada $H = \left(\frac{p,q}{\mathbb{Q}}\right)$, sempre existeix una immersió $H \hookrightarrow \mathrm{M}(2, \mathbb{R})$.*

DEMOSTRACIÓ: Si $H \simeq \mathrm{M}(2, \mathbb{Q})$, H és una subàlgebra de $\mathrm{M}(2, \mathbb{R})$ de forma natural. Si H és una àlgebra de divisió, aleshores és forçosament indefinida, atès que p i q són positius. En aquest cas, la proposició 1.1.25 ens dóna una immersió explícita. □

1.1.27 Proposició. *Sigui $H = \left(\frac{p,q}{\mathbb{Q}}\right)$. Aleshores H és una àlgebra de matrius si, i només si, estem en un dels casos que segueixen:*

(i) $p = q = 2$;

(ii) $p = q \equiv 1 \mod 4$;

(iii) $q = 2$ *i* $p \equiv \pm 1 \mod 8$;

(iv) $p \neq q$, $p \neq 2$, $q \neq 2$, $\left(\frac{q}{p}\right) = 1$, *i o bé* p *o bé* q *és 1 mòdul 4.*

DEMOSTRACIÓ: Les $\mathbb{Q}$-àlgebres de quaternions no ramificades es caracteritzen per tenir el discriminant igual a 1 (cf. 1.1.9). Aplicant el teorema 1.1.7 de classificació de les àlgebres de quaternions, només ens cal assegurar que $(p,q)_v = 1$ per a tota plaça v finita, ja que $(p,q)_\infty = 1$. Cal comprovar que això passa precisament en els casos indicats en la proposició. És clar que $(p,q)_v = 1$ per a tot $v \neq 2, p, q$.

Directament tenim que $(2,2)_v = 1$ per a tot v, que és el cas (i).

En el cas (ii), si $p = q$ és un primer senar, aleshores $(p,p)_p = (p,p)_2$, i aquest valor és 1 si, i només si, $p \equiv 1 \mod 4$.

Si $q = 2$ i p és senar, tenim que $(p,2)_2 = (p,2)_p$ i pren el valor 1 si, i només si, $p \equiv \pm 1 \mod 8$. Així obtenim (iii).

Suposem $p \neq q$, ambdós diferents de 2. Com que el nombre de places ramificades ha de ser parell, és suficient imposar que $(p,q)_p = (p,q)_q = 1$. La primera igualtat se satisfà si, i només si, un dels dos primers és $\equiv 1 \mod 4$. Si imposem que $(p,q)_p = \left(\frac{q}{p}\right)$ valgui 1, obtenim l'últim cas. □

En la proposició següent obtenim els discriminants, en funció de p i q, per als casos en què la $\mathbb{Q}$-àlgebra anterior és una àlgebra de divisió.

1.1.28 Proposició. *Sigui* $H = \left(\frac{p,q}{\mathbb{Q}}\right)$.

(i) *Si* $p \equiv q \equiv 3 \mod 4$ *i* $\left(\frac{q}{p}\right) \neq 1$, *aleshores* $D_H = 2p$.

(ii) *Si* $q = 2$, $p \equiv 3 \mod 8$, *aleshores* $D_H = pq = 2p$.

(iii) *Si* $p \neq q$, $p \equiv 1 \mod 4$ *i* $\left(\frac{p}{q}\right) = -1$, *aleshores* $D_H = pq$.

DEMOSTRACIÓ: Es tracta d'analitzar els símbols de Hilbert locals $(p,q)_v$, per a $v = 2, p, q$. De fet, cal anar resseguint, i ampliant, els casos revisats en la demostració de la proposició anterior. Anem a explicitar-ho.

En el cas (i) suposem que $p \equiv q \equiv 3 \mod 4$; per tant, $(p,q)_2 = -1$. Si $p \neq q$, tenim que $(p,q)_p = -(p,q)_q$, per la llei de reciprocitat quadràtica; a més, com abans, $(p,q)_p = \left(\frac{q}{p}\right) \neq 1$, per hipòtesi. Si $p = q$, llavors $(p,p)_p = -1$.

Per a veure (ii), només cal tenir en compte que $(p,2)_2 = (p,2)_p$; el seu valor és -1 si, i només si, $p \equiv \pm 5 \mod 8$. Afegim la restricció $p \equiv 3 \mod 4$, encara que no és necessària per tal que no hi hagi interseccions entre els diferents apartats.

Per a (iii), com que $p \equiv 1 \mod 4$, tenim que $(p,q)_p = (p,q)_q$, i el seu valor coincideix amb $\left(\frac{p}{q}\right)$, que per hipòtesi val -1. □

A partir de les dues proposicions anteriors arribem al teorema següent, que classifica les àlgebres donades per una parella de primers i proporciona un representant de cada classe.

1.1.29 Teorema. *Sigui* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions.*

(i) *Si* $D_H = 1$, *aleshores* $H \simeq \mathrm{M}(2,\mathbb{Q}) \simeq \left(\frac{1,-1}{\mathbb{Q}}\right)$.

(ii) *Si* $D_H = 2p$ *i* $p \equiv 3 \mod 4$, *aleshores* $H \simeq \left(\frac{p,-1}{\mathbb{Q}}\right)$.

(iii) *Si* $D_H = pq$, *amb* $q \equiv 1 \mod 4$ *i* $\left(\frac{p}{q}\right) = -1$, *aleshores* $H \simeq \left(\frac{p,q}{\mathbb{Q}}\right)$.

Si a i b són nombres primers, l'àlgebra H satisfà un, i només un, dels tres apartats anteriors. Denotarem per $H_A(p)$ *l'àlgebra de quaternions* $\left(\frac{p,-1}{\mathbb{Q}}\right)$, *amb* $p \equiv 3 \mod 4$; *i per* $H_B(p,q)$ *l'àlgebra de quaternions* $\left(\frac{p,q}{\mathbb{Q}}\right)$, *amb* $q \equiv 1 \mod 4$ *i* $\left(\frac{p}{q}\right) = -1$.

DEMOSTRACIÓ: Només cal comprovar que les àlgebres de quaternions donades com a representants de cada classe tenen el discriminant indicat.

El cas (i) és clar.

En el cas (ii), considerem l'àlgebra $H = \left(\frac{p,-1}{\mathbb{Q}}\right)$. Com que $p \equiv 3 \mod 4$, obtenim que $(p,-1)_p = (p,-1)_2 = -1$, la qual cosa prova (ii). Notem que l'apartat (ii) del teorema es correspon amb els apartats (i) i (ii) de la proposició anterior.

L'apartat (iii) reformula l'apartat (iii) de la proposició anterior.

Per a l'afirmació particular d'a i b primers, només cal comprovar que, efectivament, els casos descrits cobreixen totes les possibilitats, per a qualsevol parella de primers positius, distingint el cas $p = 2$ i si els primers són congruents amb 1 o bé -1 mòdul 4. □

1.1.30 Definició. D'acord amb la definició 1.1.6, anomenem $\mathbb{Q}$-àlgebres no ramificades les $\mathbb{Q}$-àlgebres de quaternions que tenen discriminant 1; és a dir, les àlgebres isomorfes a $\mathrm{M}(2,\mathbb{Q})$. Anomenem $\mathbb{Q}$-àlgebres ramificades les $\mathbb{Q}$-àlgebres de quaternions que tenen discriminant més gran que 1. Anomenem $\mathbb{Q}$-àlgebres poc ramificades les $\mathbb{Q}$-àlgebres de quaternions que tenen discriminant igual al producte de dos nombres primers. Diem que una $\mathbb{Q}$-àlgebra poc ramificada és de tipus A si és isomorfa a $H_A(p)$, per a algun primer p; diem que és de tipus B si és isomorfa a $H_B(p,q)$, per a alguns primers p, q. □

Completem el teorema 1.1.29 donant un representant per a totes les classes d'isomorfia de $\mathbb{Q}$-àlgebres poc ramificades.

1.1.31 Teorema. *Donats p i q dos nombres primers diferents, sigui H una $\mathbb{Q}$-àlgebra de quaternions poc ramificada de discriminant $D_H = pq$.*

(i) *Si* $p \equiv 3 \mod 4$ *i* $q = 2$, *aleshores* $H \simeq \left(\frac{p,-1}{\mathbb{Q}}\right)$.

(ii) *Si* $p \equiv 5 \mod 8$ *i* $q = 2$, *aleshores* $H \simeq \left(\frac{p,\,2}{\mathbb{Q}}\right)$.

(iii) *Si* $p \equiv 1 \mod 8$ *i* $q = 2$, *aleshores* $H \simeq \left(\frac{2p,-r}{\mathbb{Q}}\right)$, *on* r *és un nombre primer tal que* $\left(\frac{r}{p}\right) = \left(\frac{r}{2}\right) = -1$.

(iv) *Si* p *o bé* $q \equiv 1 \mod 4$ *i* $\left(\frac{q}{p}\right) \neq 1$, *aleshores* $H \simeq \left(\frac{p,q}{\mathbb{Q}}\right)$.

(v) *Si* p *o bé* $q \equiv 1 \mod 4$ *i* $\left(\frac{q}{p}\right) = 1$, *aleshores* $H \simeq \left(\frac{pq,-r}{\mathbb{Q}}\right)$, *on* r *és un nombre primer tal que* $\left(\frac{r}{s}\right) = \pm 1$ *depenent de si* $s \equiv \mp 1 \mod 4$, *respectivament, per a* $s = p, q$; *a més, si* p *o bé* $q \equiv 3 \mod 4$, *cal* $r \equiv 3 \mod 4$.

(vi) *Si* $p \equiv q \equiv 3 \mod 4$, *aleshores* $H \simeq \left(\frac{pq,-1}{\mathbb{Q}}\right)$.

DEMOSTRACIÓ: En primer lloc, observem que les condicions sobre els primers p i q cobreixen totes les parelles de primers diferents possibles. Així, només cal veure que les àlgebres escollides com a representants tenen, en cada cas, discriminant igual a pq.

Els apartats (i) i (iv) es corresponen amb els apartats (ii) i (iii) d'1.1.29, respectivament.

Per a veure (ii), notem que $(2,p)_p = (2,p)_2 = -1$ si, i només si, $p \equiv \pm 5 \mod 8$, però el cas $p \equiv 3 \mod 8$ ja està inclòs en (i).

Per a l'apartat (iii), vegem que sempre existeix almenys un primer r que compleix les condicions exigides. La condició $\left(\frac{r}{2}\right) = -1$ equival a $r \equiv \pm 5 \mod 8$; fixem, per exemple, el signe positiu. Per a complir l'altra condició, fixem $b \in \mathbb{Z}/p\mathbb{Z}$ que no sigui un quadrat i exigim que $r \equiv b \mod p$. Pel teorema xinès dels residus, com que $(8,p) = 1$, el sistema de congruències $x \equiv 5 \mod 8$, $x \equiv b \mod p$ té una solució (i només una): $x \equiv x_0 \mod 8p$. Considerem ara els elements d'aquesta classe que formen la progressió $\{x_0, x_0 + 8p, x_0 + 2 \cdot 8p, \dots\}$. Pel teorema de Dirichlet de la progressió aritmètica, suposant que $(x_0, 8p) = 1$, en aquesta progressió hi ha infinits primers r. Notem que, efectivament, tenim que $2 \nmid x_0$, ja que $x_0 \equiv 5 \mod 8$ i $p \nmid x_0$, ja que $x_0 \equiv b \mod p$, $b \neq 0$. Ara comprovem que el discriminant de l'àlgebra de quaternions de (iii) és, efectivament, $pq = 2p$. Tenim que $\varepsilon_v = (2p,-r)_v = (2,-1)_v(2,r)_v(p,-1)_v(p,r)_v = (2,r)_v(p,r)_v$. En particular, $\varepsilon_p = \left(\frac{r}{p}\right)$, $\varepsilon_2 = \left(\frac{r}{2}\right)$ i $\varepsilon_p = -\left(\frac{p}{r}\right)$. Així, les condicions imposades sobre r corresponen a demanar que $\varepsilon_p = \varepsilon_2 = -1$. La llei de reciprocitat quadràtica, automàticament, dóna $\varepsilon_r = 1$.

A l'apartat (v) es comprova que sempre existeix r, complint les condicions exigides, amb els mateixos arguments que a l'apartat (iii). Per a trobar el valor del discriminant de l'àlgebra, en aquest cas tenim que $\varepsilon_v = (pq,-r)_v = (p,-1)_v(p,r)_v(q,-1)_v(q,r)_v$. Suposem que $p \equiv 1 \mod 4$; en cas contrari,

intercanviem els papers de p i q. Aleshores, $\varepsilon_p = (p,-1)_p(p,r)_p = \left(\frac{r}{p}\right)$, que per hipòtesi val -1. Si $q \equiv 1 \mod 4$, tenim que $\left(\frac{r}{q}\right) = -1$; per tant, $\varepsilon_q = (q,-1)_q(q,r)_q = -1$ i $\varepsilon_r = (p,r)_r(q,r)_r = 1$; així el discriminant és pq. Si $q \equiv 3 \mod 4$, tenim que $\left(\frac{r}{q}\right) = 1$; per tant, $\varepsilon_q = (q,-1)_q(q,r)_q = -1$, i $\varepsilon_r = (p,r)_r(q,r)_r = 1$, gràcies a que $r \equiv 3 \mod 4$; així, el discriminant també és pq. La condició imposada sobre $\left(\frac{r}{q}\right)$ correspon a $\varepsilon_q = -1$. Perquè es compleixi $\varepsilon_q = -\varepsilon_r$, cal excloure el cas $q \equiv 3 \mod 4$, $r \equiv 1 \mod 4$.

Finalment, és immediat veure que l'àlgebra de quaternions de (vi) té discriminant pq. □

1.1.32 Remarca. Observem que les àlgebres de l'apartat (i) són les àlgebres poc ramificades de tipus A, i les dels apartats (ii) i (iv) són les poc ramificades de tipus B. De fet, notem que (ii) és un cas particular de (iv), i l'apartat (iii) també es pot incloure en (v), traient el requisit $q \neq 2$. □

1.2 Teoria aritmètica d'ordres quaterniònics

Dediquem aquesta secció a la teoria aritmètica relativa als ordres de les àlgebres de quaternions, en especial als ordres maximals i als ordres d'Eichler. En recordem els principals conceptes i resultats, unificant definicions i fixant la notació, i introduïm nous conceptes, com el de base normalitzada d'un ordre. Donem resultats explícits sobre ordres de les àlgebres poc ramificades de tipus A i de tipus B. Per a una teoria general per a K-àlgebres es pot consultar [Rei75]. Les referències dels treballs originals d'Eichler són principalment [Eic37] i [Eic38], però part dels seus resultats es troben també a altres treballs, com per exemple en [Vig80]. Per als ordres d'Eichler en les àlgebres de matrius locals, destaquem també [Hij74].

Sigui R l'anell d'enters de K, que és un anell de Dedekind. Sigui H una K-àlgebra de quaternions. Un element $\alpha \in H$ es diu que és enter sobre K si $\mathrm{n}(\alpha)$ i $\mathrm{tr}(\alpha)$ són de R. A diferència del cas d'extensions de cossos commutatius, el conjunt d'elements de H enters sobre K en general no és un anell.

1.2.1 Ordres i ideals

1.2.1 Definicions. Una R-xarxa Λ de H és un R-mòdul finitament generat contingut en H. Un R-ideal I de H és, per definició, una R-xarxa tal que $\Lambda \otimes_R K \simeq H$. L'invers d'un ideal I és $I^{-1} = \{h \in H \mid IhI \subset I\}$, que és també un R-ideal de H. Es diu que un R-ideal és enter si només conté elements enters. □

En una K-àlgebra de quaternions sempre hi ha ideals. Per exemple, si $\{v_1, v_2, v_3, v_4\}$ és una K-base de H, $I = R[v_1, v_2, v_3, v_4]$ és un R-ideal, i I_v és un R_v-ideal on v és una plaça de R.

1.2.2 Lema. *Siguin I i I' R-ideals de H. Aleshores existeix $\lambda \in R$, $\lambda \neq 0$, tal que $\lambda I \subset I'$.*

DEMOSTRACIÓ: Siguin $\{v_i\}$ i $\{v_i'\}$ R-bases de I i I', respectivament. Com que també són K-bases de H, tenim que $v_j = \sum_{i=1}^4 a_{ij} v_i'$, amb $a_{ij} \in K$. Sigui $0 \neq \lambda \in R$ tal que $\lambda a_{ij} \in R$ per a tot i, j. Així, $\lambda v_j \in I'$ per a $j = 1, 2, 3, 4$ i d'aquí, $\lambda I \subset I'$. □

1.2.3 Proposició. *Sigui $\mathcal{O} \subset H$. Les afirmacions següents són equivalents:*

(i) *$\mathcal{O}$ és un subanell de H i un R-mòdul lliure de rang 4.*

(ii) *$\mathcal{O}$ és un anell format per elements enters, que conté R tal que $\mathcal{O}K = H$.*

(iii) *$\mathcal{O}$ és un R-ideal que és un anell.*

Si $\mathcal{O}$ satisfà aquestes condicions, es diu que és un R-ordre de H. □

En particular, per a qualsevol ordre $\mathcal{O}$ quaterniònic tenim que $1_K \in \mathcal{O}$; així, sovint ens restringirem a bases de $\mathcal{O}$ del tipus $\{1, v_2, v_3, v_4\}$ cf. [God78].

A un ideal I d'una K-àlgebra de quaternions H, se li associen els ordres dret i esquerre de la forma següent:

$$\mathcal{O}_d(I) = \{h \in H \mid Ih \subset I\}, \quad \mathcal{O}_e(I) = \{h \in H \mid hI \subset I\}.$$

Els ideals enters són els que estan continguts en un dels seus ordres i els podem pensar com a ideals dret, esquerre o bilaterals en l'ordre, segons el cas. La norma reduïda $\mathrm{n}(I)$ d'un ideal I és, per definició, l'ideal fraccionari de R generat per les normes reduïdes dels seus elements.

Si $\mathcal{O}$ és un R-ordre, posem $\mathcal{O}_v := \mathcal{O} \otimes R_v$. Si v és una plaça finita, $\mathcal{O}_v$ és un R_v-ordre local; si v és una plaça infinita, s'escriu $R_v = K_v$ i es té que $\mathcal{O}_v = H_v$. Aleshores s'obté $\mathcal{O} = H \cap (\prod_v \mathcal{O}_v)$.

1.2.4 Definicions. La diferent $\mathcal{D}(\mathcal{O})$ d'un R-ordre $\mathcal{O}$ és l'invers del dual de $\mathcal{O}$ per a la forma bilineal donada per la traça reduïda; és a dir, $\alpha \in \mathcal{D}(\mathcal{O})^{-1}$ si, i només si, $\mathrm{tr}(\alpha\mathcal{O}) \subseteq R$. La diferent de $\mathcal{O}$ és un ideal bilateral de $\mathcal{O}$. El discriminant reduït d'un R-ordre $\mathcal{O}$ és la norma reduïda de la diferent $\mathcal{D}(\mathcal{O})$. Denotem aquest ideal per $D_{\mathcal{O}}$. □

1.2.5 Proposició. *Sigui $\mathcal{O}$ un R-ordre d'una àlgebra de quaternions H. El discriminant reduït té les propietats següents:*

(i) *$D^2_{\mathcal{O}}$ és l'ideal de R generat per $\{\det(\mathrm{tr}(\omega_i\omega_j)) : 1 \leq i,j \leq 4, \omega_i, \omega_j \in \mathcal{O}\}$.*

(ii) *Si $\{v_i\}$ és una R-base de l'ordre $\mathcal{O}$, aleshores $D^2_{\mathcal{O}} = R\det(\mathrm{tr}(v_iv_j))$.*

(iii) *Siguin $\mathcal{O} \subseteq \mathcal{O}'$ R-ordres de H. Aleshores, $D_{\mathcal{O}'}$ divideix $D_{\mathcal{O}}$ i la igualtat de discriminants es dóna si, i només si, $\mathcal{O} = \mathcal{O}'$.*

(iv) *$(D_{\mathcal{O}})_v = D_{\mathcal{O}_v}$.* □

1.2.6 Corol·lari. *Siguin $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ i $\mathcal{O} \subseteq H$ un ordre quaterniònic. Sigui P la matriu que expressa una $\mathbb{Z}$-base $\mathcal{B}$ de $\mathcal{O}$ fixada respecte de la base $\{1,i,j,ij\}$ de H. Aleshores,*

$$D_{\mathcal{O}} = |4ab\det P|.$$

DEMOSTRACIÓ: Per la proposició anterior, $D^2_{\mathcal{O}} = |\det(\mathrm{tr}(v_iv_j))|$ per a $\mathcal{B} = \{v_i\}$. Prenem la base canònica $\{1,i,j,ij\}$ de H i posem M la matriu de l'aplicació bilineal definida per la traça respecte d'aquesta base. Per propietats del canvi de base en aplicacions bilineals, tenim que $D^2_{\mathcal{O}} = |\det M|(\det P)^2 = 16a^2b^2(\det P)^2$. □

1.2.7 Definició. Sigui $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ una K-base de H. Anomenem caràcter de la base $\mathcal{B}$ la matriu 1×4 de coeficients a K associada a la forma lineal traça en aquesta base: $(\mathrm{tr}(v_1), \mathrm{tr}(v_2), \mathrm{tr}(v_3), \mathrm{tr}(v_4))$. El caràcter de $\mathcal{B}$, el denotem per $\chi(\mathcal{B})$. □

Per a les $\mathbb{Q}$-àlgebres de quaternions, i els seus ordres, introduïm bases amb condicions sobre el seu caràcter.

1.2.8 Definició. Sigui H una $\mathbb{Q}$-àlgebra i $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ una $\mathbb{Q}$-base de H. Diem que $\mathcal{B}$ és una base normalitzada si $v_1 = 1$ i té caràcter $\chi(\mathcal{B}) = (2001)$ o bé (2000); és a dir, $v_1 = 1$, $v_2, v_3 \in H_0$ i $\mathrm{tr}(v_4) \in \{0, 1\}$. En el primer cas, diem que és una base normalitzada parella, i en el segon cas, que és senar. □

1.2.9 Lema. *Sigui $\mathcal{O}$ un $\mathbb{Z}$-ordre d'una $\mathbb{Q}$-àlgebra H. Aleshores tenim els fets següents:*

(i) *Existeixen $\mathbb{Z}$-bases de $\mathcal{O}$ normalitzades.*

(ii) *Dues $\mathbb{Z}$-bases de $\mathcal{O}$ normalitzades tenen el mateix caràcter; així, el caràcter és un invariant de l'ordre.*

(iii) *Donada $Q \in \mathrm{GL}(4, \mathbb{Z})$, Q és la matriu d'un canvi de base entre dues $\mathbb{Z}$-bases normalitzades de $\mathcal{O}$ si, i només si, $\chi(\mathcal{B})$ és un vector propi de valor propi 1 per l'esquerra de Q, per a $\mathcal{B}$ una $\mathbb{Z}$-base normalitzada de $\mathcal{O}$ qualsevol.*

DEMOSTRACIÓ: Anem a construir una $\mathbb{Z}$-base de $\mathcal{O}$ normalitzada. Sempre podem agafar una $\mathbb{Z}$-base de $\mathcal{O}$ de la forma $\{1, u_2, u_3, u_4\}$. Posem $u_i' = u_i - [\frac{\mathrm{tr}(u_i)}{2}]$, per a $i = 2, 3, 4$. Si $u_2', u_3' \in H_0$, ja tenim una base satisfent les condicions. En cas contrari, existeix $v_4 \in \{u_2', u_3', u_4'\}$ amb $\mathrm{tr}(v_4) = 1$, i aconseguirem $v_2, v_3 \in H_0$ a partir dels anteriors restant-los, si cal, v_4. És clar que aleshores $\{1, v_2, v_3, v_4\}$ és una $\mathbb{Z}$-base normalitzada de $\mathcal{O}$.

Per a veure (ii), observem que si $\mathrm{tr}(v_4) = 0$, aleshores tots els elements de l'ordre tenen traça parell. El recíproc també és cert. Així, $\mathrm{tr}(v_4) = 1$ si, i només si, existeix algun element de l'ordre amb traça senar. En aquest cas, és clar que en qualsevol base de $\mathcal{O}$ hi ha d'haver almenys un element de traça senar. Aquesta propietat depèn de l'ordre, i no de la base normalitzada.

La condició de l'apartat (iii) s'escriu $\chi(\mathcal{B}) = \chi(\mathcal{B})Q$. Això equival precisament a la relació de canvi de base, ja que per (ii) totes les bases d'un ordre tenen el mateix caràcter. □

Aquest resultat permet donar la definició següent.

1.2.10 Definició. Siguin $\mathcal{O}$ un $\mathbb{Z}$-ordre d'una $\mathbb{Q}$-àlgebra de quaternions i $\mathcal{B}$ una base normalitzada qualsevol de $\mathcal{O}$. El caràcter de l'ordre $\mathcal{O}$, denotat per $\chi(\mathcal{O})$, és el caràcter de la base $\mathcal{B}$. Així, diem que un ordre és senar si $\chi(\mathcal{O}) = (2001)$ o, equivalentment, si existeix $\omega \in \mathcal{O}$ amb $\mathrm{tr}(\omega) = 1$. Anàlogament,

diem que un ordre és parell si $\chi(\mathcal{O}) = (2000)$ o, equivalentment, si no existeix cap $\omega \in \mathcal{O}$ amb $\mathrm{tr}(\omega) = 1$; és a dir, tots els elements tenen traça parella. □

1.2.11 Remarca. Sigui $\mathcal{O}$ un $\mathbb{Z}$-ordre quaterniònic. Posem $k = 0$, respectivament $k = 1$, segons que $\mathcal{O}$ sigui parell, respectivament senar. Les condicions perquè una matriu $Q = (q_{ij}) \in \mathrm{GL}(4, \mathbb{Z})$ sigui una matriu de canvi de base entre dues bases normalitzades del $\mathbb{Z}$-ordre quaterniònic $\mathcal{O}$ són:

(i) $q_{11} = 1$ i $q_{i1} = 0$, per a $i = 2, 3, 4$;

(ii) $2q_{1i} = -kq_{4i}$, per a $i = 2, 3$, i $2q_{14} = k(1 - q_{44})$. □

1.2.12 Lema. *Sigui $\mathcal{O}$ un $\mathbb{Z}$-ordre d'una $\mathbb{Q}$-àlgebra de quaternions. Aleshores, per a tot $\sigma \in H^*$, l'ordre conjugat $\sigma^{-1}\mathcal{O}\sigma$ té el mateix caràcter que $\mathcal{O}$. En particular, si $\mathcal{B}$ és una base normalitzada de $\mathcal{O}$, aleshores $\sigma^{-1}\mathcal{B}\sigma$ és una base normalitzada de $\sigma^{-1}\mathcal{O}\sigma$.*

DEMOSTRACIÓ: Sigui $\{1, v_2, v_3, v_4\}$ una $\mathbb{Z}$-base normalitzada de $\mathcal{O}$. Aleshores $\{1, \sigma^{-1}v_2\sigma, \sigma^{-1}v_3\sigma, \sigma^{-1}v_4\sigma\}$ és una $\mathbb{Z}$-base normalitzada de $\sigma^{-1}\mathcal{O}\sigma$, ja que la traça es conserva per conjugació; és a dir, $\mathrm{tr}(\sigma^{-1}v_i\sigma) = \mathrm{tr}(v_i)$, la qual cosa implica, també, que les dues bases tenen el mateix caràcter. □

A continuació, introduïm el concepte de denominador de l'ordre, restringintnos també a $\mathbb{Q}$-àlgebres.

1.2.13 Definició. Sigui H una $\mathbb{Q}$-àlgebra de quaternions. Per a cada $\mathbb{Z}$-ordre $\mathcal{O}$, definim el denominador de l'ordre $m_{\mathcal{O}} \in \mathbb{Z}$ com el mínim enter positiu tal que $m_{\mathcal{O}} \cdot \mathcal{O} \subseteq \mathbb{Z}[1, i, j, ij]$. □

1.2.14 Lema. *Siguin H una $\mathbb{Q}$-àlgebra de quaternions i $\mathcal{O} \subseteq H$ un $\mathbb{Z}$-ordre quaterniònic, amb una base fixada. Sigui P la matriu de canvi de la base de $\mathcal{O}$ a la base canònica de H.*

(i) *$m_{\mathcal{O}}$ és l'enter positiu més petit tal que la matriu $m_{\mathcal{O}}P$ té els coeficients en $\mathbb{Z}$.*

(ii) *Si $\mathcal{O} \subseteq \mathcal{O}'$, aleshores $m_{\mathcal{O}} | m'_{\mathcal{O}}$.* □

1.2.15 Remarca. Per a l'àlgebra $H = \mathrm{M}(2, \mathbb{Q})$, també tenen sentit les definicions anteriors. Considerem el $\mathbb{Z}$-ordre $\mathcal{O} = \mathrm{M}(2, \mathbb{Z})$, de discriminant $D_{\mathcal{O}} = 1$.

Per exemple tenim les bases de H següents:

$$\mathcal{B} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$
$$\mathcal{B}' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$
$$\mathcal{B}'' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

La base $\mathcal{B}'$, donada per l'isomorfisme ψ de 1.1.10, tot i que té totes les entrades de les matrius enteres, no és una base de l'ordre $\mathcal{O}$. La base habitual de $\mathcal{O}$ és $\mathcal{B}$, però no és una base normalitzada. En canvi, $\mathcal{B}''$ és una base de $\mathcal{O}$ normalitzada.

El denominador de l'ordre $\mathcal{O}$ és $m_{\mathcal{O}} = 2$. Això es comprova expressant una base qualsevol de $\mathcal{O}$ respecte de la base $\mathcal{B}'$ de H, que és la que correspon a la base $\{1, i, j, ij\}$ en la definició de $m_{\mathcal{O}}$. □

En una K-àlgebra de quaternions cada R-ordre està contingut en un R-ordre maximal i sempre hi ha, almenys, un ordre maximal. A continuació s'introdueixen uns altres ordres, definits a partir dels ordres maximals, que tenen un paper especial en la construcció de les corbes de Shimura.

1.2.16 Definició. Un R-ordre d'Eichler d'una K-àlgebra de quaternions H és la intersecció de dos R-ordres maximals de H. □

1.2.17 Proposició. *Sigui $\psi : H \longrightarrow H'$ un K-isomorfisme entre dues K-àlgebres de quaternions. Es tenen les propietats següents:*

(i) *$\alpha \in H$ és un element enter si, i només si, $\psi(\alpha)$ és un element enter de H'.*

(ii) *$\mathcal{O} \subseteq H$ és un R-ordre si, i només si, $\psi(\mathcal{O})$ és un R-ordre de H'. En particular, $\mathcal{O}$ és un ordre maximal de H si, i només si, $\psi(\mathcal{O})$ és un ordre maximal de H'.*

(iii) *$\mathcal{O}$ és un R-ordre d'Eichler de H si, i només si, $\psi(\mathcal{O})$ és un R-ordre d'Eichler de H'.*

(iv) *Si $\mathcal{O}$ és un R-ordre de H, aleshores tenim la igualtat de discriminants $D_{\psi(\mathcal{O})} = D_{\mathcal{O}}$. En particular, si $\mathcal{O}$ i $\mathcal{O}'$ són R-ordres de H conjugats, aleshores són del mateix discriminant.*

DEMOSTRACIÓ: Recordem que α és un element enter si, i només si, $\mathrm{tr}(\alpha)$ i $n(\alpha) \in R$. Així, 1.1.16(iv) demostra (i).

La propietat (ii) s'obté si s'apliquen (i) i les definicions d'homomorfisme de K-àlgebres i de R-ordre.

Anem a veure (iii). Sigui $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$. Per (iii), els R-ordres $\mathcal{O}_i$ són maximals si, i només si, els R-ordres $\psi(\mathcal{O}_i)$ són maximals, per $i = 1, 2$. Així, $\psi(\mathcal{O}) = \psi(\mathcal{O}_1) \cap \psi(\mathcal{O}_2)$ és un R-ordre d'Eichler de H' si, i només si, $\mathcal{O}$ és un R-ordre d'Eichler de H.

Resta demostrar (iv). Per 1.2.5(ii), és suficient veure que $\mathrm{tr}(\psi(u_i)\psi(u_j)) = \mathrm{tr}(u_i u_j)$, on $\{u_i\}$ és una R-base de $\mathcal{O}$, ja que aleshores $\{\psi(u_i)\}$ és una R-base de l'ordre $\psi(\mathcal{O})$. Això és cert per 1.1.16. □

1.2.2 Ordres d'Eichler locals

Fixem una plaça finita v del cos K i considerem el cos local K_v i l'àlgebra de quaternions $H_v = H \otimes K_v$. Anem a fer un estudi dels ordres maximals i els ordres d'Eichler en aquest cas. Sigui R_v l'anell d'enters de K_v i sigui π una uniformitzant de R_v.

Recordem que H_v és o bé una àlgebra de divisió o bé una àlgebra de matrius. Ens podem reduir a l'estudi dels ordres en aquests dos casos, ja que, per la proposició 1.2.17, les propietats de ser maximal i ser d'Eichler es conserven per isomorfisme. Les proposicions següents descriuen els R_v-ordres maximals i els R_v-ordres d'Eichler.

Suposem que H_v és una àlgebra de divisió. Sigui w una valoració discreta de K_v. Aleshores es demostra que $\widetilde{w}(h) := w(\mathrm{n}(h))$, per a $h \in H_v$, defineix una valoració discreta de H_v. Sigui $\mathcal{O}_v$ l'anell de valoració de $\widetilde{w}$. Per a cada cos local commutatiu F_v, amb $K_v \subseteq F_v \subseteq H_v$, la restricció de $\widetilde{w}$ a F_v és també una valoració discreta que té com a anell de valoració discreta $\mathcal{O}_v \cap F_v$ igual a l'anell d'enters de F_v. Per tant, es dedueix que $\mathcal{O}_v$ conté tots els elements enters de H_v i, per tant, és l'únic ordre maximal de H_v. Aleshores, es prova que $\pi\mathcal{O}_v = \mathfrak{p}^2$, on $\mathfrak{p}$ és l'únic ideal maximal de $\mathcal{O}_v$. Així, tenim el següent resultat.

1.2.18 Proposició. *Sigui H_v una K_v-àlgebra de divisió local.*

(i) *H_v conté un únic R_v-ordre maximal, $\mathcal{O}_v = \{x \in H_v : n(x) \in R_v\}$.*

(ii) *L'ideal πR_v ramifica en $\mathcal{O}_v$.*

(iii) *H_v conté un únic R_v-ordre d'Eichler, igual a l'únic ordre maximal.* □

Suposem que H_v és la K-àlgebra de matrius $\mathrm{M}(2, K_v)$. Aleshores tenim els resultats següents.

1.2.19 Proposició. *Si H_v és l'àlgebra de matrius $\mathrm{M}(2, K_v)$, els R_v-ordres maximals són els conjugats de l'ordre maximal $\mathcal{O}_v = \mathrm{M}(2, R_v)$ per elements de $\mathrm{GL}(2, K_v)$.* □

1.2.20 Corol·lari. *Si H_v és l'àlgebra de matrius $\mathrm{M}(2, K_v)$, aleshores*

$$\mathcal{O}_{\underline{n}} := \begin{pmatrix} R_v & R_v \\ \pi^n R_v & R_v \end{pmatrix} = \mathrm{M}(2, R_v) \cap \begin{pmatrix} R_v & \pi^{-n} R_v \\ \pi^n R_v & R_v \end{pmatrix}$$

és un R_v-ordre d'Eichler, que s'anomena l'ordre d'Eichler canònic de nivell $\pi^n R_v$. □

1.2.21 Proposició. *Sigui $\mathcal{O}_v$ un R_v-ordre de $\mathrm{M}(2, K_v)$. Les afirmacions següents són equivalents:*

(a) *L'ordre $\mathcal{O}_v$ és un ordre d'Eichler.*

(b) *Existeix una única parella $\{\mathcal{O}_1, \mathcal{O}_2\}$ d'ordres maximals de $\mathrm{M}(2, K_v)$ tal que $\mathcal{O}_v = \mathcal{O}_1 \cap \mathcal{O}_2$.*

(c) *Existeix un únic $n \in \mathbb{N} \cup \{0\}$ tal que l'ordre $\mathcal{O}_v$ és conjugat de l'ordre $\mathcal{O}_{\underline{n}}$.*

(d) *L'ordre $\mathcal{O}_v$ conté un subanell conjugat de*

$$\begin{pmatrix} R_v & 0 \\ 0 & R_v \end{pmatrix} := \left\{ \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix} : r_1, r_2 \in R_v \right\}.$$

L'ideal $N_{\mathcal{O}_v} := \pi^n R_v$, determinat en l'apartat (c)*, s'anomena el nivell de l'ordre d'Eichler local $\mathcal{O}_v \subseteq \mathrm{M}(2, K_v)$.* □

La condició (c) diu que els ordres d'Eichler locals d'un mateix nivell són conjugats. Observem que els anells d'enters locals R_v són principals. Quan l'anell d'enters global R és principal i l'àlgebra de quaternions és indefinida, es té també que els ordres d'Eichler globals són conjugats, com a conseqüència de resultats d'Eichler, cf. 1.2.33.

Volem ara definir el nivell d'un ordre d'Eichler $\mathcal{O}_v$ en una K_v-àlgebra de quaternions local H_v qualsevol.

1.2.22 Definició. Siguin H_v una K_v-àlgebra de quaternions i $\mathcal{O}_v$ un ordre d'Eichler de H_v. Es defineix el nivell de $\mathcal{O}_v$ com l'ideal

$$N_{\mathcal{O}_v} = \begin{cases} R_v & \text{si } H_v \text{ és una àlgebra de divisió,} \\ N_{\varphi(\mathcal{O}_v)} & \text{si } \varphi : H_v \to \mathrm{M}(2, K_v) \text{ és un isomorfisme.} \end{cases} \square$$

1.2.23 Remarca. Es comprova directament que, per a l'ordre d'Eichler canònic de $\mathrm{M}(2, K_v)$, se satisfà que $D_{\mathcal{O}_{\underline{n}}} = \pi^n R_v$. Com que el discriminant no varia per isomorfismes, per a tot ordre d'Eichler de $\mathrm{M}(2, K_v)$ i, per tant, per a tot ordre d'Eichler d'una àlgebra local $H_v \simeq \mathrm{M}(2, K_v)$, el discriminant i el nivell coincideixen.

1.2.3 Ordres d'Eichler globals

Tornem al cas global, en què H és una K-àlgebra de quaternions i K un cos de nombres d'anell d'enters R. Sigui $\mathcal{O}$ un R-ordre d'Eichler de H.

1.2.24 Proposició. (i) *Un R-ordre $\mathcal{O}$ és maximal si, i només si, $\mathcal{O}_v$ és un R_v-ordre maximal per a tota plaça finita v.*

(ii) *Un R-ordre $\mathcal{O}$ és d'Eichler si, i només si, $\mathcal{O}_v$ és un R_v-ordre d'Eichler per a tota v plaça finita.* $\square$

Per als ordres maximals, tenim el resultat següent.

1.2.25 Proposició. *Sigui $\mathcal{O}$ un R-ordre en una K-àlgebra de quaternions H. Aleshores, $\mathcal{O}$ és un ordre maximal si, i només si, $D_{\mathcal{O}} = D_H$. En particular, tots els ordres maximals tenen el mateix discriminant.* $\square$

Aquest resultat és útil per a reconèixer ordres maximals. Per exemple, $\mathrm{M}(2, R)$ és un R-ordre maximal de $\mathrm{M}(2, K)$, ja que té discriminant reduït igual a R.

1.2.26 Definició. El nivell d'un ordre d'Eichler global $\mathcal{O}$ és l'únic ideal enter N de R tal que N_v és el nivell de cada $\mathcal{O}_v$ per a cada plaça finita v de K. El denotem per $N_{\mathcal{O}}$. Així, $N_{\mathcal{O}} := \prod_v N_{\mathcal{O}_v}$. En general, $\mathcal{O}(D, N)$ denotarà un ordre d'Eichler de nivell N en una àlgebra de quaternions de discriminant D. $\square$

Observem que el nivell d'un ordre d'Eichler global $\mathcal{O}$ està ben definit. Sigui $\mathcal{O} = \mathcal{O}' \cap \mathcal{O}'' \subseteq H$ un ordre d'Eichler global, amb $\mathcal{O}'$ i $\mathcal{O}''$ ordres maximals.

Per 1.2.2, existeixen $a, b \in K^*$ tals que $a\mathcal{O}' \subseteq \mathcal{O}'' \subseteq b\mathcal{O}'$. Però a_v i b_v són unitats quasi per a tota v. Així, $\mathcal{O}'_v = \mathcal{O}''_v$ i, per tant, $\mathcal{O}_v$ és maximal i de nivell $N_{\mathcal{O}_v} = R_v$ gairebé per a tota v. Per tant, existeix un únic ideal N tal que $N_v = N_{\mathcal{O}_v}$ per a tota v.

Hi ha altres definicions d'ordre d'Eichler que inclouen explícitament el nivell. La proposició següent, enunciada per al cas de $\mathbb{Q}$-àlgebres de quaternions, assegura que són definicions equivalents amb la donada. Observem que els resultats següents són vàlids igualment per a R-ordres d'Eichler de K-àlgebres de quaternions.

1.2.27 Proposició. *Siguin H una $\mathbb{Q}$-àlgebra de quaternions de discriminant D_H, N un ideal de $\mathbb{Z}$ primer amb D_H i $\mathcal{O} \subseteq H$ un $\mathbb{Z}$-ordre. Aleshores, les afirmacions següents són equivalents:*

(a) *$\mathcal{O}$ és un ordre d'Eichler de H de nivell N.*

(b) *$\mathcal{O}$ satisfà: si $p \nmid N$, el $\mathbb{Z}_p$-ordre local $\mathcal{O}_p$ és maximal, i si $p|N$, $\mathcal{O}_p$ és isomorf a l'ordre* $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.

(c) *$\mathcal{O}$ satisfà: si $p|D_H$, el $\mathbb{Z}_p$-ordre local $\mathcal{O}_p$ és maximal, i si $p \nmid D_H$, $\mathcal{O}_p$ és isomorf a l'ordre* $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.

DEMOSTRACIÓ: Per 1.2.24, ens podem reduir a veure l'equivalència per a tota plaça p finita, ja que aquesta és una propietat local.

Si $p \nmid D_H \cdot N$, aleshores per una banda tenim que $H_p \simeq \mathrm{M}(2, \mathbb{Q}_p)$ i, per l'altra, que $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} = \mathrm{M}(2, \mathbb{Z}_p)$, perquè N_p és una unitat a $\mathbb{Z}_p$. Així, l'afirmació de (a) diu que $\mathcal{O}_p$ és un ordre d'Eichler de nivell 1, és a dir, un ordre maximal, la qual cosa coincideix directament amb el que diu (b). En aquest mateix cas, (c) diu que $\mathcal{O}_p$ és isomorf a $\mathrm{M}(2, \mathbb{Z}_p)$, la qual cosa és equivalent al fet que sigui maximal, perquè tots els ordres maximals són conjugats a aquest, per 1.2.18.

Si $p \mid D_H$, aleshores H_p és de divisió, per la qual cosa hi ha un únic ordre maximal, condició exigida a (c) i a (b), gràcies a que N i D_H són primers entre si. En aquest cas, la condició (a) diu que $\mathcal{O}_p$ és un ordre d'Eichler de nivell 1, que equival a dir que és maximal; per tant, coincideixen.

Finalment, en el cas $p \mid N$, H_p és l'àlgebra de matrius local. Si apliquem 1.2.17 i 1.2.21, la condició (a) és equivalent a que $\mathcal{O}_p$ sigui conjugat llevat isomorfisme de $\mathcal{O}_{\underline{n}}$, la qual cosa concorda amb (b) i (c). □

1.2.28 Proposició. *Sigui H una $\mathbb{Q}$-àlgebra de quaternions. Siguin $\mathcal{O}(D,1)$, $\mathcal{O}(D,N) \subseteq H$, un $\mathbb{Z}$-ordre maximal i un $\mathbb{Z}$-ordre d'Eichler de nivell N de H, respectivament, i suposem que $\mathcal{O}(D,N) \subseteq \mathcal{O}(D,1)$. Denotem per $[\mathcal{O}(D,1) : \mathcal{O}(D,N)]$ l'índex com a $\mathbb{Z}$-mòdul d'un ordre en l'altre. Aleshores,*

$$[\mathcal{O}(D,1) : \mathcal{O}(D,N)] = N.$$

DEMOSTRACIÓ: Com a $\mathbb{Z}$-mòduls, tenim que

$$\mathcal{O}(D,1)/\mathcal{O}(D,N) \simeq \oplus_p \mathcal{O}(D,1)_p/\mathcal{O}(D,N)_p,$$

d'on es dedueix la igualtat $[\mathcal{O}(D,1) : \mathcal{O}(D,N)] = \prod_p [\mathcal{O}(D,1)_p : \mathcal{O}(D,N)_p]$. Per la proposició 1.2.27, per als primers $p \nmid N$ tenim que $\mathcal{O}(D,1)_p = \mathcal{O}(D,N)_p$; per tant, $[\mathcal{O}(D,1)_p : \mathcal{O}(D,N)_p] = 1$. Per als primers $p|N$ posem $N = p^r N'$, amb $p \nmid N'$, i és clar que $[\mathcal{O}(D,1)_p : \mathcal{O}(D,N)_p] = p^r$. Per tant, efectivament $[\mathcal{O}(D,1) : \mathcal{O}(D,N)] = N$. □

A diferència del cas dels ordres maximals (cf. 1.2.25), no tenim una caracterització explícita dels ordres d'Eichler en funció del seu discriminant. Les propietats següents permeten determinar alguns ordres d'Eichler.

1.2.29 Proposició. *Sigui H una $\mathbb{Q}$-àlgebra de quaternions de discriminant D_H. Considerem un $\mathbb{Z}$-ordre $\mathcal{O} \subseteq H$.*

(i) *Si $\mathcal{O}$ és un ordre d'Eichler, aleshores $D_{\mathcal{O}} = D_H \cdot N_{\mathcal{O}}$ i $\operatorname{mcd}(D_H, N_{\mathcal{O}}) = 1$.*

(ii) *Si $D_{\mathcal{O}} = D_H \cdot N$ és un enter lliure de quadrats, aleshores $\mathcal{O}$ és un ordre d'Eichler de nivell N.*

(iii) *Siguin $\mathcal{O}$ i $\mathcal{O}'$ $\mathbb{Z}$-ordres de H conjugats. Aleshores, $\mathcal{O}$ és un ordre d'Eichler de nivell N si, i només si, $\mathcal{O}'$ és un ordre d'Eichler de nivell N.*

DEMOSTRACIÓ: Com que els conceptes de maximalitat i nivell són locals, aplicant 1.2.5(iv), només cal comprovar (i) localment. Per a les places p ramificades, apliquem 1.2.25. Per a les places no ramificades, ja hem comentat

en una remarca anterior que el nivell i el discriminant coincidien. Suposem que no fossin coprimers; és a dir, sigui $p|D_H$, $p|N$. Aleshores, $\mathcal{O}_p$ seria un ordre d'Eichler de H_p de nivell $N_p \neq 1$, però H_p és un cos i té un únic ordre maximal; per tant, arribem a una contradicció.

Per a veure l'apartat (ii), només cal demostrar que $\mathcal{O}_p$ és un $\mathbb{Z}$-ordre d'Eichler, ja que aleshores, per (i), el nivell ja és N. Novament ho analitzem localment. És suficient veure-ho per a $p|N$, ja que per les altres places té nivell $N_p = 1$; per tant, és maximal (cf. 1.2.25) i, en particular, és d'Eichler.

Suposem $p|N$. En particular, $p \nmid D_H$; per tant, $\mathcal{O}_p$ és un $\mathbb{Z}$-ordre de $H_p \simeq \mathrm{M}(2,\mathbb{Q}_p)$ de discriminant $D_{\mathcal{O}_p} = D_p = p$, ja que D és lliure de quadrats. Utilitzant que la condició d'Eichler passa per isomorfisme i que el valor del discriminant també es conserva per isomorfisme, només cal veure que a $\mathrm{M}(2,\mathbb{Q}_p)$ un ordre amb discriminant p és forçosament d'Eichler. Per la proposició 1.2.21 és equivalent a veure que és conjugat de l'ordre canònic $\mathcal{O}_1$, la qual cosa està provada a [Eic55b].

Finalment, l'apartat (iii) s'obté aplicant l'apartat (i) anterior junt amb la proposició 1.2.17 (iii),(iv). □

1.2.30 Remarca. Siguin $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ una àlgebra de quaternions de discriminant D, $\mathcal{O}(D,N) \subseteq H$ un $\mathbb{Z}$-ordre d'Eichler de nivell N amb una $\mathbb{Z}$-base fixada, i P la matriu de canvi de la base de $\mathcal{O}(D,N)$ a la base de H. Com que $D_{\mathcal{O}(D,N)} = DN$, si apliquem el corol·lari 1.2.6, tenim que $|\det P| = \dfrac{DN}{|4ab|}$. Per tant, $|\det P|$ només depèn de paràmetres relatius a l'àlgebra, a, b i D, i del nivell N. Si N és lliure de quadrats i posem $\det P = \dfrac{r}{s} \in \mathbb{Q}$, fracció irreductible, aleshores $2|s$. D'aquí deduïm també que $2|m_{\mathcal{O}}$.

1.2.31 Proposició. *Sigui Λ una xarxa d'una K-àlgebra de quaternions H. Per a cada plaça finita v de K, considerem una xarxa local L_v de l'àlgebra de quaternions local H_v. Suposem que $L_v = \Lambda_v$ gairebé per a tot v. Aleshores, existeix una xarxa Λ' de H tal que $\Lambda'_v = L_v$ per a tota plaça finita v.* □

En particular, d'aquesta proposició deduïm el corol·lari següent.

1.2.32 Corol·lari. *Sigui H una $\mathbb{Q}$-àlgebra de quaternions de discriminant D. Aleshores, per a tot enter N tal que $\mathrm{mcd}(D,N) = 1$, existeixen ordres d'Eichler de nivell N.*

DEMOSTRACIÓ: Només cal aplicar la proposició anterior usant la descripció local dels ordres d'Eichler donada a 1.2.27. Així, obtenim una xarxa Λ' amb les característiques locals desitjades. Notem que Λ'_v és un $\mathbb{Z}_v$-ordre per a tota plaça v; per tant, $\Lambda' = \cap_v \Lambda'_v$ és un $\mathbb{Z}$-ordre de H que, per construcció, és un ordre d'Eichler del nivell N desitjat. □

En la secció següent donem taules d'ordres d'Eichler explícits per a algunes àlgebres poc ramificades.

Tots els ordres d'Eichler d'un nivell donat són localment conjugats. El resultat d'Eichler que esmentem a continuació ens assegura, en particular, que per a les $\mathbb{Q}$-àlgebres indefinides els ordres d'Eichler són, a més, globalment conjugats. Més en general el resultat és el següent.

1.2.33 Teorema. *Siguin K un cos de nombres totalment real i H una K-àlgebra de quaternions indefinida. Si el nombre de classes d'ideals de K és senar, els ordres d'Eichler d'un nivell N donat són tots conjugats. En particular, en aquest cas els ordres maximals són tots conjugats.* □

Donat un ordre $\mathcal{O}$ d'una àlgebra de quaternions H qualsevol, considerem el normalitzador

$$\mathrm{Nor}(\mathcal{O}) := \{\sigma \in H^* : \sigma \mathcal{O} \sigma^{-1} = \mathcal{O}\}.$$

És clar que si $\mathcal{O}$ i $\mathcal{O}'$ són ordres conjugats, aleshores $\mathrm{Nor}(\mathcal{O}) = \mathrm{Nor}(\mathcal{O}')$.

Si $\mathcal{O}$ és un ordre d'una àlgebra de quaternions sobre un cos de nombres K, es pot estudiar el seu normalitzador localment, ja que se satisfà que

$$\mathrm{Nor}(\mathcal{O}) = \{h \in H^* : h \in \mathrm{Nor}(\mathcal{O}_v), \text{ per a tota } v \text{ plaça finita de } K\}.$$

Suposem que $\mathcal{O}$ és un ordre d'Eichler. Si $v | D_H$, H_v és una àlgebra de divisió i $\mathcal{O}_v$ és l'únic ordre maximal; per tant, en aquest cas $\mathrm{Nor}(\mathcal{O}_v) = H_v^*$. Si $v \nmid D_H$ i $\mathcal{O}_v$ és un ordre maximal de $M(2, K_v)$, aleshores $\mathrm{Nor}(\mathcal{O}_v) = K^* \mathcal{O}_v^*$. Si $v \nmid D_H$ i $\mathcal{O}_v$ és l'ordre d'Eichler canònic $\mathcal{O}_{\underline{n}}$ de $M(2, K_v)$, aleshores $\mathrm{Nor}(\mathcal{O}_{\underline{n}})$ està generat per $K^* \mathcal{O}_v^*$ i $\begin{pmatrix} 0 & 1 \\ \pi^n & 0 \end{pmatrix}$.

1.2.4 Ordres d'Eichler de les $\mathbb{Q}$-àlgebres no ramificades i poc ramificades

En primer lloc, explicitem els ordres maximals de les $\mathbb{Q}$-àlgebres de quaternions no ramificades i poc ramificades. En el llibre [Vig80] n'hi ha alguns

exemples, però la majoria es refereixen a $\mathbb{Q}$-àlgebres de quaternions definides.

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

(i) *Si H és una $\mathbb{Q}$-àlgebra no ramificada, aleshores tot $\mathbb{Z}$-ordre maximal de $\mathcal{O} \subseteq H$ és isomorf a l'ordre $\mathcal{O}_0(1,1) := \mathrm{M}(2,\mathbb{Z})$, ordre maximal de $\mathrm{M}(2,\mathbb{Q})$. Equivalentment, $\mathcal{O}$ és isomorf a l'ordre de l'àlgebra de matrius $\left(\frac{1,-1}{\mathbb{Q}}\right)$*

$$\mathcal{O}_M(1,1) := \mathbb{Z}\left[1, \frac{j+ij}{2}, \frac{-j+ij}{2}, \frac{1-i}{2}\right].$$

(ii) *Si H és una $\mathbb{Q}$-àlgebra poc ramificada de tipus A, de discriminant $D_H = 2p$, aleshores tot ordre maximal de H és isomorf a l'ordre de $H_A(p)$*

$$\mathcal{O}_A(2p,1) := \mathbb{Z}\left[1, i, j, \frac{1+i+j+ij}{2}\right].$$

(iii) *Si H és una $\mathbb{Q}$-àlgebra poc ramificada de tipus B, de discriminant $D_H = pq$, aleshores tot ordre maximal de H és isomorf a l'ordre de $H_B(p,q)$*

$$\mathcal{O}_B(pq,1) := \mathbb{Z}\left[1, i, \frac{1+j}{2}, \frac{i+ij}{2}\right].$$

DEMOSTRACIÓ: Per 1.2.17, els ordres maximals es conserven per isomorfisme de K-àlgebres; per tant, és suficient veure que els ordres $\mathcal{O}_0(1,1)$, $\mathcal{O}_A(2p,1)$ i $\mathcal{O}_B(pq,1)$ són ordres maximals a les àlgebres $\mathrm{M}(2,\mathbb{Q})$, $H_A(p)$ i $H_B(p,q)$. Notem que l'ordre $\mathcal{O}_M(1,1)$ s'obté a partir de l'ordre $\mathcal{O}_0(1,1)$ per l'isomorfisme ψ^{-1} de 1.1.10. Per a $\mathrm{M}(2,\mathbb{Q})$ és conegut.

Per veure (ii), es calcula $D_{\mathcal{O}_A(2p,1)} = 2p$ utilitzant 1.2.5. Per 1.1.29, aquest valor coincideix amb el discriminant de $H_A(p)$. Si apliquem 1.2.25, tenim que $\mathcal{O}_A(2p,1)$ és un ordre maximal. A més, per 1.2.33, tots els ordres maximals de $H_A(p)$ són conjugats.

De forma anàloga es demostra (iii): en aquest cas, $D_{\mathcal{O}_B(pq,1)} = pq = D_{H(p,q)}$. □

Notem que per a les $\mathbb{Q}$-àlgebres de quaternions no ramificades i les poc ramificades de tipus A i B, llevat conjugació, podem suposar que tot ordre $\mathcal{O}$ està

contingut en l'ordre maximal donat en la proposició anterior. En particular, per aquestes àlgebres podem expressar qualsevol element $\omega \in \mathcal{O}$ en funció d'una base de $\mathcal{O}_0(1,1)$ o bé $\mathcal{O}_M(1,1)$, $\mathcal{O}_A(2p,1)$, $\mathcal{O}_B(pq,1)$, respectivament.

A continuació donem $\mathbb{Z}$-ordres d'Eichler explícits per a aquestes àlgebres.

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

(i) *A l'àlgebra de matrius* $\mathrm{M}(2,\mathbb{Q})$, *el $\mathbb{Z}$-ordre*

$$\mathcal{O}_0(1,N) := \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} : a,b,c,d \in \mathbb{Z} \right\}$$

és un ordre d'Eichler de nivell N.
A l'àlgebra de matrius no ramificada $\left(\frac{1,-1}{\mathbb{Q}}\right)$, *el $\mathbb{Z}$-ordre*

$$\mathcal{O}_M(1,N) := \mathbb{Z}\left[1, \frac{j+ij}{2}, N\frac{(-j+ij)}{2}, \frac{1-i}{2}\right]$$

és un ordre d'Eichler de nivell N.

(ii) *A la $\mathbb{Q}$-àlgebra $H_A(p)$, el $\mathbb{Z}$-ordre*

$$\mathcal{O}_A(2p,N) := \mathbb{Z}\left[1, i, Nj, \frac{1+i+j+ij}{2}\right]$$

és un ordre d'Eichler de nivell N, per a $N \mid \frac{p-1}{2}$, N lliure de quadrats.

(iii) *A la $\mathbb{Q}$-àlgebra $H_B(p,q)$, el $\mathbb{Z}$-ordre*

$$\mathcal{O}_B(pq,N) := \mathbb{Z}\left[1, Ni, \frac{1+j}{2}, \frac{i+ij}{2}\right]$$

és un ordre d'Eichler de nivell N, per a $N|\frac{q-1}{4}$, $\mathrm{mcd}(N,p) = 1$, N lliure de quadrats.

(iv) *Si* $H = \left(\frac{p,q}{\mathbb{Q}}\right)$ *és de tipus A, amb* $q \equiv 3 \mod 4$ *i* $D_H = 2p$, *aleshores*

$$\mathbb{Z}\left[1, i, j, \frac{1+i+j+ij}{2}\right]$$

és un ordre d'Eichler de H de nivell q.

DEMOSTRACIÓ: El cas (i) és clar.

Per tal que $\mathcal{O}_A(2p, N)$ sigui un $\mathbb{Z}$-ordre de $H_A(p)$ cal que $N \mid \frac{p-1}{2}$. De manera anàloga al cas anterior, obtenim que $D_{\mathcal{O}_A(2p,N)} = 2pN$. En aquest cas, per 1.1.28, $D_{H_A(p)} = 2p$. Notem que N i $2p$ són primers entre si, per les condicions sobre N i ser $p \equiv 3 \mod 4$. Aleshores, $\mathcal{O}_A(2p, N)$ és un ordre d'Eichler de nivell N, per 1.2.29. Això prova (ii).

Anem a veure (iii). La condició $N|\frac{q-1}{4}$ ens assegura que $\mathcal{O}_B(pq, N)$ és un $\mathbb{Z}$-ordre de $H_B(p, q)$. El seu discriminant és $D_{\mathcal{O}_B(pq,N)} = pqN$. En aquest cas, $D_{H_B(p,q)} = pq$, i automàticament $\text{mcd}(N, q) = 1$. Si imposem que N i p siguin primers entre si, aleshores $\mathcal{O}_B(pq, N)$ és un ordre d'Eichler de nivell N, com abans.

En el cas (iv), la condició sobre el discriminant implica que $p \equiv 3 \mod 4$. Així, es comprova fàcilment que $\mathbb{Z}\left[1, i, j, \frac{1+i+j+ij}{2}\right]$ és un $\mathbb{Z}$-ordre de discriminant igual a $2pq$. Aleshores, si apliquem 1.2.29, obtenim que l'ordre donat és un ordre d'Eichler de nivell q. □

1.3 Algoritmes i taules

En aquesta secció descrivim breument els algoritmes implementats relatius als resultats d'aquest capítol sobre àlgebres de quaternions i ordres quaterniònics, que formen part del paquet `Poincare`. Ens referirem sempre a $\mathbb{Q}$-àlgebres de quaternions.

Bàsicament les instruccions s'estructuren en tres blocs, depenent de la seva finalitat: instruccions relatives a les operacions amb quaternions (remarquem la no-commutativitat del producte), instruccions sobre les àlgebres de quaternions en si mateixes i instruccions sobre els ordres quaterniònics.

Totes les instruccions relatives a àlgebres de quaternions utilitzen l'àlgebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, respecte de la base $\{1, i, j, k\}$, on $k := ij$. Així, les variables i, j, k, a i b estan protegides i no se'ls pot assignar cap valor mentre tinguem el paquet `Poincare` actiu. Això s'aconsegueix amb una rutina que es carrega automàticament en inicialitzar el paquet i n'esborra els valors anteriors. Algunes instruccions es poden utilitzar amb a i b com a paràmetres, altres requereixen haver fixat l'àlgebra de quaternions, la qual cosa es realitza amb

la instrucció `defQuatAlg`.

Definim un quaternió a partir dels polinomis de *Maple* multivariables, utilitzant les variables i, j, k. La instrucció `qcoeffs` dóna els coeficients d'un quaternió respecte de la base $\{1, i, j, k\}$ i `Mcoor` dóna els coeficients d'una llista de quaternions escrivint-los a les columnes d'una matriu. Destaquem les funcions lògiques `type/quaternion` i `type/purequaternion`, que comproven el tipus d'element introduït i interven en la construcció d'altres instruccions.

Les operacions suma de quaternions i producte per un escalar coincideixen amb les ja definides en *Maple V* per als polinomis. Només és necessari definir el producte de quaternions, que no és commutatiu, per a la qual cosa utilitzem la instrucció `qmul`. Per comoditat, introduïm també l'abreviació `&q`, com a símbol del producte de quaternions, que emula la instrucció anterior. Definim el conjugat, la norma, la traça i l'invers d'un quaternió amb les instruccions `qbar`, `qnorm`, `qtrace` i `qinv`, respectivament.

Podem parlar d'un segon bloc d'instruccions relatives a les àlgebres de quaternions com a objectes. El discriminant d'una àlgebra es calcula amb la instrucció `DiscH`, la qual utilitza la instrucció `Hilbert` per a calcular símbols de Hilbert (que no es troba en el *Maple V R4*). Pel que fa als morfismes d'àlgebres, tenim la instrucció `embH` per a la immersió de l'àlgebra de quaternions en l'àlgebra de les matrius reals donada a 1.1.25, i la instrucció `embHg`, que n'és una variació que admet paràmetres. Per als automorfismes interns hem implementat la instrucció `qconj`.

Els teoremes 1.1.29 i 1.1.31 donen algoritmes per a calcular àlgebres de quaternions amb determinades característiques. Les instruccions `canH` i `canHdisc` són les implementacions d'aquests algoritmes. Així, donats dos nombres primers p i q, `canH` retorna una parella (a, b) que determini una àlgebra de quaternions isomorfa a $\left(\frac{p,q}{\mathbb{Q}}\right)$, que permet classificar les àlgebres de quaternions de partida en àlgebres no ramificades, àlgebres poc ramificades de tipus A i àlgebres poc ramificades de tipus B. Donats p i q primers diferents, `canHdisc` retorna una parella (a, b) que determini una àlgebra de quaternions de discriminant $D = pq$. La instrucció `typeH` comprova si l'àlgebra de quaternions és ramificada o poc ramificada de tipus A o de tipus B.

Agrupem en un tercer bloc les instruccions relatives als ordres. Per a totes aquestes instruccions, observem que la manera d'introduir un ordre serà per mitjà d'una base, donada com una llista de quatre quaternions, que denotem per l. Ara bé, no tota llista l de quatre quaternions és necessàriament una $\mathbb{Z}$-base d'un ordre. Destaquem així, en primer lloc, la funció lògica

`isOrder`, que comprova si l genera o no un ordre, indicant-ne el motiu en cas negatiu, mitjançant un paràmetre opcional. A partir d'aquí, la resta d'instruccions referents a ordres tindran com a entrada una llista l formada per quatre quaternions, que donaran per descomptat que determina un ordre; generalment, si no és així s'obtindrà un error o una resposta sense sentit. Per evitar aquests errors, totes les instruccions que usen ordres disposen de l'argument opcional `true`. Si afegim aquest argument a continuació dels arguments de la instrucció, en ser executada aquesta comprovarà prèviament que la llista l donada determini un ordre; en cas afirmatiu s'executarà la instrucció pròpiament dita i en cas negatiu ens dirà el motiu pel qual l no és ordre i pararà amb resposta buida.

Pel que fa a les bases d'un ordre, destaquem les instruccions: `HermiteOr`, per a simplificar la base de l'ordre; `isnBasisOr`, funció lògica que comprova si una base és normalitzada; `nBasisOr`, que retorna una base normalitzada de l'ordre; `McbOr`, per a obtenir la matriu de canvi de base entre dos bases de l'ordre; `coorOr`, que dóna les coordenades d'un element respecte d'una base, i `OrM`, que transforma una matriu en la llista de quaternions determinada per les seves columnes, respecte de la base $\{1, i, j, k\}$. Calculem també constants associades a l'ordre. Les instruccions `DiscOr`, `ParOr` i `denOr` retornen el discriminant, la paritat i el denominador de l'ordre. La funció lògica `isMaxOrder` identifica si l'ordre és maximal o no. Per al cas d'ordres d'Eichler, `NivOr` en dóna el nivell.

Donats dos ordres, els algoritmes que comproven si hi ha inclusió o igualtat entre aquests s'han implementat en les funcions lògiques `IncOr` i `EqOr`, respectivament. Obtenim l'índex d'un ordre en un altre amb la instrucció `IndOr` (suposant la inclusió dels ordres donats i amb l'argument opcional `true` per tal de comprovar prèviament aquesta inclusió). La instrucció `IndMaxOr` dóna l'índex de l'ordre en un ordre maximal que el contingui. Destaquem també la instrucció `IntOr`, que implementa un algoritme per a calcular la intersecció de dos ordres. La instrucció `ConjOr` calcula el conjugat d'un ordre per un quaternió. Finalment, la instrucció `IntConjOr`, elaborada a partir de les dues anteriors, busca la intersecció d'un ordre amb un cert conjugat seu. Notem que si apliquem les instruccions `IntOr` i `IntConjOr` a ordres maximals, obtenim ordres d'Eichler.

Els resultats sobre la classificació de les $\mathbb{Q}$-àlgebres de quaternions donades per una parella de primers s'han recopilat en la taula 1.1, per als primers p, q inferiors a 55. La taula 1.2 dóna un representant de les classes d'isomorfia de les àlgebres de quaternions poc ramificades de discriminant $D < 240$. En la taula 1.3 donem una àlgebra de quaternions H de discriminant producte de

quatre nombres primers, $D_H = p_1p_2p_3p_4 \leq 1000$. Notem que, si ampliem la taula 1.2 fins a discriminant 1000, tenim un representant de totes les classes d'isomorfia de les àlgebres de quaternions indefinides de discriminant menor que 1000.

En les taules 1.4, 1.5, 1.6 i 1.7 hem calculat $\mathbb{Z}$-bases explícites d'ordres representants de les classes de conjugació dels ordres d'Eichler de nivell N per a les àlgebres no ramificades $H_A(3)$, $H_B(2,5)$, $H_A(7)$ i $H_B(3,5)$.

Taula 1.1 *Representants* **H** *de les classes d'isomorfia de les* $\mathbb{Q}$*-àlgebres de quaternions no ramificades o poc ramificades de la forma* $H = \left(\frac{p,q}{\mathbb{Q}}\right)$*, on* $p, q \leq 55$ *primers.*

H	D_H	**H**
$(2,2)$	1	$(1,-1)$
$(2,3)$	6	$(3,-1)$
$(2,5)$	10	$(2,5)$
$(2,7)$	1	$(1,-1)$
$(2,11)$	22	$(11,-1)$
$(2,13)$	26	$(2,13)$
$(2,17)$	1	$(1,-1)$
$(2,19)$	38	$(19,-1)$
$(2,23)$	1	$(1,-1)$
$(2,29)$	58	$(2,29)$
$(2,31)$	1	$(1,-1)$
$(2,37)$	74	$(2,37)$
$(2,41)$	1	$(1,-1)$
$(2,43)$	86	$(43,-1)$
$(2,47)$	1	$(1,-1)$
$(2,53)$	106	$(2,53)$
$(3,3)$	6	$(3,-1)$
$(3,5)$	15	$(3,5)$
$(3,7)$	14	$(7,-1)$
$(3,11)$	6	$(3,-1)$
$(3,13)$	1	$(1,-1)$
$(3,17)$	51	$(3,17)$
$(3,19)$	38	$(19,-1)$
$(3,23)$	6	$(3,-1)$
$(3,29)$	87	$(3,29)$
$(3,31)$	62	$(31,-1)$
$(3,37)$	1	$(1,-1)$
$(3,41)$	123	$(3,41)$
$(3,43)$	86	$(43,-1)$
$(3,47)$	6	$(3,-1)$
$(3,53)$	159	$(3,53)$
$(5,5)$	1	$(1,-1)$
$(5,7)$	35	$(5,7)$
$(5,11)$	1	$(1,-1)$
$(5,17)$	85	$(5,17)$
$(5,19)$	1	$(1,-1)$
$(5,23)$	115	$(5,23)$
$(5,29)$	1	$(1,-1)$
$(5,31)$	1	$(1,-1)$
$(5,37)$	185	$(5,37)$
$(5,41)$	1	$(1,-1)$
$(5,43)$	215	$(5,43)$
$(5,47)$	235	$(5,47)$
$(5,53)$	265	$(5,53)$
$(7,7)$	14	$(7,-1)$
$(7,11)$	22	$(11,-1)$
$(7,13)$	91	$(7,13)$
$(7,17)$	119	$(7,17)$
$(7,19)$	14	$(7,-1)$
$(7,23)$	46	$(23,-1)$
$(7,29)$	1	$(1,-1)$
$(7,31)$	14	$(7,-1)$
$(7,37)$	1	$(1,-1)$
$(7,41)$	287	$(7,41)$
$(7,43)$	86	$(43,-1)$
$(7,47)$	14	$(7,-1)$
$(7,53)$	1	$(1,-1)$
$(11,11)$	22	$(11,-1)$
$(11,13)$	143	$(11,13)$
$(11,17)$	187	$(11,17)$
$(11,19)$	22	$(11,-1)$
$(11,23)$	46	$(23,-1)$
$(11,29)$	319	$(11,29)$
$(11,31)$	62	$(31,-1)$
$(11,37)$	1	$(1,-1)$
$(11,41)$	451	$(11,41)$
$(11,43)$	22	$(11,-1)$
$(11,47)$	94	$(47,-1)$

H	D_H	$\mathbf{H}$
$(11,53)$	1	$(1,-1)$
$(13,13)$	1	$(1,-1)$
$(13,17)$	1	$(1,-1)$
$(13,19)$	247	$(13,19)$
$(13,23)$	1	$(1,-1)$
$(13,29)$	1	$(1,-1)$
$(13,31)$	403	$(13,31)$
$(13,37)$	481	$(13,37)$
$(13,41)$	533	$(13,41)$
$(13,43)$	1	$(1,-1)$
$(13,47)$	611	$(13,47)$
$(13,53)$	1	$(1,-1)$
$(17,17)$	1	$(1,-1)$
$(17,19)$	1	$(1,-1)$
$(17,23)$	391	$(17,23)$
$(17,29)$	493	$(17,29)$
$(17,31)$	527	$(17,31)$
$(17,37)$	629	$(17,37)$
$(17,41)$	697	$(17,41)$
$(17,43)$	1	$(1,-1)$
$(17,47)$	1	$(1,-1)$
$(17,53)$	1	$(1,-1)$
$(19,19)$	38	$(19,-1)$
$(19,23)$	46	$(23,-1)$
$(19,29)$	551	$(19,29)$
$(19,31)$	38	$(19,-1)$
$(19,37)$	703	$(19,37)$
$(19,41)$	779	$(19,41)$
$(19,43)$	86	$(43,-1)$
$(19,47)$	94	$(47,-1)$
$(19,53)$	1007	$(19,53)$
$(23,23)$	46	$(23,-1)$
$(23,29)$	1	$(1,-1)$

H	D_H	$\mathbf{H}$
$(23,31)$	62	$(31,-1)$
$(23,37)$	851	$(23,37)$
$(23,41)$	1	$(1,-1)$
$(23,43)$	46	$(23,-1)$
$(23,47)$	94	$(47,-1)$
$(23,53)$	1219	$(23,53)$
$(29,29)$	1	$(1,-1)$
$(29,31)$	899	$(29,31)$
$(29,37)$	1073	$(29,37)$
$(29,41)$	1189	$(29,41)$
$(29,43)$	1247	$(29,43)$
$(29,47)$	1363	$(29,47)$
$(29,53)$	1	$(1,-1)$
$(31,31)$	62	$(31,-1)$
$(31,37)$	1147	$(31,37)$
$(31,41)$	1	$(1,-1)$
$(31,43)$	62	$(31,-1)$
$(31,47)$	94	$(47,-1)$
$(31,53)$	1643	$(31,53)$
$(37,37)$	1	$(1,-1)$
$(37,41)$	1	$(1,-1)$
$(37,43)$	1591	$(37,43)$
$(37,47)$	1	$(1,-1)$
$(37,53)$	1	$(1,-1)$
$(41,41)$	1	$(1,-1)$
$(41,43)$	1	$(1,-1)$
$(41,47)$	1927	$(41,47)$
$(41,53)$	2173	$(41,53)$
$(43,43)$	86	$(43,-1)$
$(43,47)$	94	$(47,-1)$
$(43,53)$	1	$(1,-1)$
$(47,47)$	94	$(47,-1)$
$(47,53)$	1	$(1,-1)$

Taula 1.2 *Representants* **H** *de les classes d'isomorfia de les* $\mathbb{Q}$*-àlgebres de quaternions poc ramificades de discriminant* $D < 240$.

D	$p \cdot q$	**H**
6	2·3	$(3,-1)$
10	2·5	$(2,5)$
14	2·7	$(7,-1)$
15	3·5	$(3,5)$
21	3·7	$(21,-1)$
22	2·11	$(11,-1)$
26	2·13	$(2,13)$
33	3·11	$(33,-1)$
34	2·17	$(34,-3)$
35	5·7	$(5,7)$
38	2·19	$(19,-1)$
39	3·13	$(39,-7)$
46	2·23	$(23,-1)$
51	3·17	$(3,17)$
55	5·11	$(55,-3)$
57	3·19	$(57,-1)$
58	2·29	$(2,29)$
62	2·31	$(31,-1)$
65	5·13	$(5,13)$
69	3·23	$(69,-1)$
74	2·37	$(2,37)$
77	7·11	$(77,-1)$
82	2·41	$(82,-3)$
85	5·17	$(5,17)$
86	2·43	$(43,-1)$
87	3·29	$(3,29)$
91	7·13	$(7,13)$
93	3·31	$(93,-1)$
94	2·47	$(47,-1)$
95	5·19	$(95,-7)$
106	2·53	$(2,53)$
111	3·37	$(111,-19)$
115	5·23	$(5,23)$
118	2·59	$(59,-1)$
119	7·17	$(7,17)$
122	2·61	$(2,61)$

D	$p \cdot q$	**H**
123	3·41	$(3,41)$
129	3·43	$(129,-1)$
133	7·19	$(133,-1)$
134	2·67	$(67,-1)$
141	3·47	$(141,-1)$
142	2·71	$(71,-1)$
143	11·13	$(11,13)$
145	5·29	$(145,-3)$
146	2·73	$(146,-5)$
155	5·31	$(155,-7)$
158	2·79	$(79,-1)$
159	3·53	$(3,53)$
161	7·23	$(161,-1)$
166	2·83	$(83,-1)$
177	3·59	$(177,-1)$
178	2·89	$(178,-3)$
183	3·61	$(183,-7)$
185	5·37	$(5,37)$
187	11·17	$(11,17)$
194	2·97	$(194,-5)$
201	3·67	$(201,-1)$
202	2·101	$(2,101)$
203	7·29	$(203,-2)$
205	5·41	$(205,-3)$
206	2·103	$(103,-1)$
209	11·19	$(209,-1)$
213	3·71	$(213,-1)$
214	2·107	$(107,-1)$
215	5·43	$(5,43)$
217	7·31	$(217,-1)$
218	2·109	$(2,109)$
219	3·73	$(219,-7)$
221	13·17	$(221,-5)$
226	2·113	$(226,-3)$
235	5·47	$(5,47)$
237	3·79	$(237,-1)$

Taula 1.3 *Representants* $\mathbf{H}$ *de les classes d'isomorfia de les* $\mathbb{Q}$*-àlgebres de quaternions de discriminant* $D = p_1 \cdot p_2 \cdot p_3 \cdot p_4 < 1000$*, on* p_1, p_2, p_3, p_4 *primers.*

D	$p_1 \cdot p_2 \cdot p_3 \cdot p_4$	$\mathbf{H}$
210	$2 \cdot 3 \cdot 5 \cdot 7$	$(2 \cdot 3 \cdot 7, 5)$
330	$2 \cdot 3 \cdot 5 \cdot 11$	$(2, 3 \cdot 5 \cdot 11)$
390	$2 \cdot 3 \cdot 5 \cdot 13$	$(2 \cdot 3 \cdot 13, 5)$
462	$2 \cdot 3 \cdot 7 \cdot 11$	$(3 \cdot 7 \cdot 11, -1)$
510	$2 \cdot 3 \cdot 5 \cdot 17$	$(2 \cdot 3 \cdot 17, 5)$
546	$2 \cdot 3 \cdot 7 \cdot 13$	$(2 \cdot 13, 3 \cdot 7)$
570	$2 \cdot 3 \cdot 5 \cdot 19$	$(2, 3 \cdot 5 \cdot 19)$
690	$2 \cdot 3 \cdot 5 \cdot 23$	$(2 \cdot 3 \cdot 23, 5)$
714	$2 \cdot 3 \cdot 7 \cdot 17$	$(2 \cdot 7, 3 \cdot 7 \cdot 17)$
770	$2 \cdot 5 \cdot 7 \cdot 11$	$(2 \cdot 5, 11 \cdot 7)$
798	$2 \cdot 3 \cdot 7 \cdot 19$	$(3 \cdot 7 \cdot 19, -1)$
858	$2 \cdot 3 \cdot 11 \cdot 13$	$(2, 3 \cdot 11 \cdot 13)$
870	$2 \cdot 3 \cdot 5 \cdot 29$	$(2, 3 \cdot 5 \cdot 29)$
910	$2 \cdot 5 \cdot 7 \cdot 13$	$(2 \cdot 7 \cdot 13, 5)$
930	$2 \cdot 3 \cdot 5 \cdot 31$	$(3 \cdot 31, 2 \cdot 3 \cdot 5)$
966	$2 \cdot 3 \cdot 7 \cdot 23$	$(3 \cdot 7 \cdot 23, -1)$

Taula 1.4 *Representants $\mathcal{O}(6,N)$ de les classes de conjugació dels ordres d'Eichler de nivell N, on $N \leq 100$, en l'àlgebra de quaternions $H_A(3)$.*

N	$\mathcal{O}(6,N)$
1	$\mathbb{Z}[1,i,j,1/2+1/2i+1/2j+1/2ij]$
5	$\mathbb{Z}[1,5i,2i+j,1/2+3/2i+1/2j+1/2ij]$
7	$\mathbb{Z}[1,7i,i+j,1/2+5/2i+1/2j+1/2ij]$
11	$\mathbb{Z}[1,i,11j,1/2+1/2i+5/2j+1/2ij]$
13	$\mathbb{Z}[1,i,13j,1/2+1/2i+17/2j+1/2ij]$
17	$\mathbb{Z}[1,17i,i+j,1/2+7/2i+1/2j+1/2ij]$
19	$\mathbb{Z}[1,19i,14i+j,1/2+27/2i+1/2j+1/2ij]$
23	$\mathbb{Z}[1,23i,4i+j,1/2+5/2i+1/2j+1/2ij]$
25	$\mathbb{Z}[1,25i,3i+j,1/2+29/2i+1/2j+1/2ij]$
29	$\mathbb{Z}[1,29i,23i+j,1/2+45/2i+1/2j+1/2ij]$
31	$\mathbb{Z}[1,31i,i+j,1/2+9/2i+1/2j+1/2ij]$
35	$\mathbb{Z}[1,35i,20i+j,1/2+3/2i+1/2j+1/2ij]$
37	$\mathbb{Z}[1,i,37j,1/2+1/2i+59/2j+1/2ij]$
41	$\mathbb{Z}[1,41i,34i+j,1/2+67/2i+1/2j+1/2ij]$
43	$\mathbb{Z}[1,43i,2i+j,1/2+67/2i+1/2j+1/2ij]$
47	$\mathbb{Z}[1,i,47j,1/2+1/2i+35/2j+1/2ij]$
49	$\mathbb{Z}[1,49i,2i+j,1/2+35/2i+1/2j+1/2ij]$
53	$\mathbb{Z}[1,53i,6i+j,1/2+7/2i+1/2j+1/2ij]$
55	$\mathbb{Z}[1,55i,37i+j,1/2+43/2i+1/2j+1/2ij]$
59	$\mathbb{Z}[1,59i,10i+j,1/2+71/2i+1/2j+1/2ij]$
61	$\mathbb{Z}[1,61i,39i+j,1/2+71/2i+1/2j+1/2ij]$
65	$\mathbb{Z}[1,65i,45i+j,1/2+67/2i+1/2j+1/2ij]$
67	$\mathbb{Z}[1,67i,15i+j,1/2+17/2i+1/2j+1/2ij]$
71	$\mathbb{Z}[1,71i,i+j,1/2+13/2i+1/2j+1/2ij]$
73	$\mathbb{Z}[1,73i,5i+j,1/2+79/2i+1/2j+1/2ij]$
77	$\mathbb{Z}[1,77i,26i+j,1/2+31/2i+1/2j+1/2ij]$
79	$\mathbb{Z}[1,79i,49i+j,1/2+1/2i+1/2j+1/2ij]$
83	$\mathbb{Z}[1,83i,36i+j,1/2+97/2i+1/2j+1/2ij]$
85	$\mathbb{Z}[1,85i,67i+j,1/2+163/2i+1/2j+1/2ij]$
89	$\mathbb{Z}[1,89i,35i+j,1/2+129/2i+1/2j+1/2ij]$
91	$\mathbb{Z}[1,91i,47i+j,1/2+161/2i+1/2j+1/2ij]$
95	$\mathbb{Z}[1,95i,8i+j,1/2+9/2i+1/2j+1/2ij]$
97	$\mathbb{Z}[1,97i,25i+j,1/2+107/2i+1/2j+1/2ij]$

Taula 1.5 *Representants $\mathcal{O}(10,N)$ de les classes de conjugació dels ordres d'Eichler de nivell N, on $N \leq 85$, en l'àlgebra de quaternions $H_B(2,5)$.*

N	$\mathcal{O}(10,N)$
1	$\mathbb{Z}[1,i,1/2+1/2j,1/2i+1/2ij]$
3	$\mathbb{Z}[1,3i,1/2+2i+1/2j,1/2i+1/2ij]$
7	$\mathbb{Z}[1,i,7/2+7/2j,1/2+5/2i+1/2j+5/2ij]$
9	$\mathbb{Z}[1,9i,1/2+2i+1/2j,1/2i+1/2ij]$
11	$\mathbb{Z}[1,11i,1/2+7i+1/2j,1/2i+1/2ij]$
13	$\mathbb{Z}[1,13i,1/2+9i+1/2j,9/2i+1/2ij]$
17	$\mathbb{Z}[1,i,17/2+17/2j,1/2+7i+1/2j+7ij]$
19	$\mathbb{Z}[1,19i,1/2+3i+1/2j,1/2i+1/2ij]$
21	$\mathbb{Z}[1,21i,1/2+16i+1/2j,11/2i+1/2ij]$
23	$\mathbb{Z}[1,23i,1/2+4i+1/2j,31/2i+1/2ij]$
27	$\mathbb{Z}[1,27i,1/2+16i+1/2j,1/2i+1/2ij]$
29	$\mathbb{Z}[1,29i,1/2+i+1/2j,39/2i+1/2ij]$
31	$\mathbb{Z}[1,i,31/2+31/2j,1/2+27/2i+1/2j+27/2ij]$
33	$\mathbb{Z}[1,33i,1/2+20i+1/2j,53/2i+1/2ij]$
37	$\mathbb{Z}[1,37i,1/2+10i+1/2j,19/2i+1/2ij]$
39	$\mathbb{Z}[1,39i,1/2+16i+1/2j,47/2i+1/2ij]$
41	$\mathbb{Z}[1,41i,1/2+12i+1/2j,79/2i+1/2ij]$
43	$\mathbb{Z}[1,43i,1/2+14i+1/2j,81/2i+1/2ij]$
47	$\mathbb{Z}[1,47i,1/2+40i+1/2j,63/2i+1/2ij]$
49	$\mathbb{Z}[1,i,49/2+49/2j,1/2+22i+1/2j+22ij]$
51	$\mathbb{Z}[1,51i,1/2+i+1/2j,77/2i+1/2ij]$
53	$\mathbb{Z}[1,53i,1/2+5i+1/2j,29/2i+1/2ij]$
57	$\mathbb{Z}[1,57i,1/2+26i+1/2j,25/2i+1/2ij]$
59	$\mathbb{Z}[1,59i,1/2+17i+1/2j,55/2i+1/2ij]$
61	$\mathbb{Z}[1,61i,1/2+46i+1/2j,67/2i+1/2ij]$
63	$\mathbb{Z}[1,63i,1/2+19i+1/2j,101/2i+1/2ij]$
67	$\mathbb{Z}[1,67i,1/2+46i+1/2j,7/2i+1/2ij]$
69	$\mathbb{Z}[1,69i,1/2+53i+1/2j,35/2i+1/2ij]$
71	$\mathbb{Z}[1,71i,131/2i+1/2ij,1/2+11i+1/2j]$
73	$\mathbb{Z}[1,73i,1/2+2i+1/2j,57/2i+1/2ij]$
77	$\mathbb{Z}[1,77i,1/2+47i+1/2j,11/2i+1/2ij]$
79	$\mathbb{Z}[1,79i,1/2+1/2j,99/2i+1/2ij]$
81	$\mathbb{Z}[1,81i,1/2+71i+1/2j,61/2i+1/2ij]$
83	$\mathbb{Z}[1,83i,1/2+7i+1/2j,139/2i+1/2ij]$

Taula 1.6 *Representants $\mathcal{O}(14,N)$ de les classes de conjugació dels ordres d'Eichler de nivell N, on $N \leq 80$, en l'àlgebra de quaternions $H_A(7)$.*

N	$\mathcal{O}(14,N)$
1	$\mathbb{Z}[1,i,j,1/2+1/2i+1/2j+1/2ij]$
3	$\mathbb{Z}[1,i,3j,1/2+1/2i+5/2j+1/2ij]$
5	$\mathbb{Z}[1,5i,i+j,1/2+7/2i+1/2j+1/2ij]$
9	$\mathbb{Z}[1,3i,2i+3j,1/2+1/2i+1/2j+1/2ij]$
11	$\mathbb{Z}[1,11i,6i+j,1/2+9/2i+1/2j+1/2ij]$
13	$\mathbb{Z}[1,13i,2i+j,1/2+3/2i+1/2j+1/2ij]$
15	$\mathbb{Z}[1,5i,3i+3j,1/2+1/2i+5/2j+1/2ij]$
17	$\mathbb{Z}[1,17i,j,1/2+13/2i+1/2j+1/2ij]$
19	$\mathbb{Z}[1,19i,4i+j,1/2+27/2i+1/2j+1/2ij]$
23	$\mathbb{Z}[1,23i,i+j,1/2+13/2i+1/2j+1/2ij]$
25	$\mathbb{Z}[1,25i,15i+j,1/2+47/2i+1/2j+1/2ij]$
27	$\mathbb{Z}[1,i,27j,1/2+1/2i+13/2j+1/2ij]$
29	$\mathbb{Z}[1,29i,16i+j,1/2+31/2i+1/2j+1/2ij]$
31	$\mathbb{Z}[1,i,31j,1/2+1/2i+41/2j+1/2ij]$
33	$\mathbb{Z}[1,11i,5i+3j,1/2+13/2i+1/2j+1/2ij]$
37	$\mathbb{Z}[1,37i,8i+j,1/2+23/2i+1/2j+1/2ij]$
39	$\mathbb{Z}[1,39i,10i+j,1/2+43/2i+1/2j+1/2ij]$
41	$\mathbb{Z}[1,41i,22i+j,1/2+17/2i+1/2j+1/2ij]$
43	$\mathbb{Z}[1,43i,18i+j,1/2+1/2i+1/2j+1/2ij]$
45	$\mathbb{Z}[1,15i,13i+3j,1/2+5/2i+1/2j+1/2ij]$
47	$\mathbb{Z}[1,47i,13i+j,1/2+77/2i+1/2j+1/2ij]$
51	$\mathbb{Z}[1,17i,4i+3j,1/2+7/2i+5/2j+1/2ij]$
53	$\mathbb{Z}[1,53i,i+j,1/2+19/2i+1/2j+1/2ij]$
55	$\mathbb{Z}[1,55i,4i+j,1/2+5/2i+1/2j+1/2ij]$
57	$\mathbb{Z}[1,19i,12i+3j,1/2+35/2i+5/2j+1/2ij]$
59	$\mathbb{Z}[1,59i,17i+j,1/2+21/2i+1/2j+1/2ij]$
61	$\mathbb{Z}[1,61i,3i+j,1/2+65/2i+1/2j+1/2ij]$
65	$\mathbb{Z}[1,65i,20i+j,1/2+113/2i+1/2j+1/2ij]$
67	$\mathbb{Z}[1,67i,45i+j,1/2+83/2i+1/2j+1/2ij]$
69	$\mathbb{Z}[1,23i,14i+3j,1/2+1/2i+1/2j+1/2ij]$
71	$\mathbb{Z}[1,71i,5i+j,1/2+99/2i+1/2j+1/2ij]$
73	$\mathbb{Z}[1,73i,7i+j,1/2+139/2i+1/2j+1/2ij]$
75	$\mathbb{Z}[1,25i,2i+3j,1/2+41/2i+5/2j+1/2ij]$
79	$\mathbb{Z}[1,79i,21i+j,1/2+41/2i+1/2j+1/2ij]$

Taula 1.7 *Representants $\mathcal{O}(15,N)$ de les classes de conjugació dels ordres d'Eichler de nivell N, on $N \leq 60$, en l'àlgebra de quaternions $H_B(3,5)$.*

N	$\mathcal{O}(15,N)$
1	$\mathbb{Z}[1, i, 1/2+1/2j, 1/2i+1/2ij]$
2	$\mathbb{Z}[1, i, j, 1/2+1/2i+1/2j+1/2ij]$
4	$\mathbb{Z}[1, 4i, 1/2+i+1/2j, 1/2i+1/2ij]$
7	$\mathbb{Z}[1, 7i, 1/2+4i+1/2j, 1/2i+1/2ij]$
8	$\mathbb{Z}[1, 4i, 3i+j, 1/2+3/2i+1/2j+1/2ij]$
11	$\mathbb{Z}[1, i, 11/2+11/2j, 1/2+9/2i+1/2j+9/2ij]$
13	$\mathbb{Z}[1, 13i, 1/2+2i+1/2j, 1/2i+1/2ij]$
14	$\mathbb{Z}[1, 14i, 1/2+5i+1/2j, 19/2i+1/2ij]$
16	$\mathbb{Z}[1, 8i, 3i+j, 1/2+11/2i+1/2j+1/2ij]$
17	$\mathbb{Z}[1, 17i, 1/2+i+1/2j, 17/2i+1/2ij]$
19	$\mathbb{Z}[1, 19i, 1/2+1/2j, 29/2i+1/2ij]$
22	$\mathbb{Z}[1, 11i, 6i+j, 1/2+1/2i+1/2j+1/2ij]$
23	$\mathbb{Z}[1, 23i, 1/2+16i+1/2j, 31/2i+1/2ij]$
26	$\mathbb{Z}[1, i, 13j, 1/2+1/2i+17/2j+1/2ij]$
28	$\mathbb{Z}[1, 28i, 1/2+3i+1/2j, 1/2i+1/2ij]$
29	$\mathbb{Z}[1, 29i, 1/2+12i+1/2j, 15/2i+1/2ij]$
31	$\mathbb{Z}[1, 31i, 1/2+17i+1/2j, 1/2i+1/2ij]$
32	$\mathbb{Z}[1, 16i, 11i+j, 1/2+15/2i+1/2j+1/2ij]$
34	$\mathbb{Z}[1, 34i, 1/2+7i+1/2j, 41/2i+1/2ij]$
37	$\mathbb{Z}[1, 37i, 1/2+27i+1/2j, 61/2i+1/2ij]$
38	$\mathbb{Z}[1, 38i, 1/2+i+1/2j, 51/2i+1/2ij]$
41	$\mathbb{Z}[1, 41i, 1/2+38i+1/2j, 61/2i+1/2ij]$
43	$\mathbb{Z}[1, 43i, 1/2+9i+1/2j, 69/2i+1/2ij]$
44	$\mathbb{Z}[1, 2i, i+11j, 1/2+3/2i+5/2j+1/2ij]$
46	$\mathbb{Z}[1, 23i, 13i+j, 1/2+25/2i+1/2j+1/2ij]$
47	$\mathbb{Z}[1, i, 47/2+47/2j, 1/2+43/2i+1/2j+43/2ij]$
49	$\mathbb{Z}[1, 49i, 1/2+45i+1/2j, 1/2i+1/2ij]$
52	$\mathbb{Z}[1, 26i, 7i+j, 1/2+49/2i+1/2j+1/2ij]$
53	$\mathbb{Z}[1, 53i, 1/2+41i+1/2j, 39/2i+1/2ij]$
56	$\mathbb{Z}[1, 28i, 13i+j, 1/2+5/2i+1/2j+1/2ij]$
58	$\mathbb{Z}[1, 58i, 1/2+47i+1/2j, 93/2i+1/2ij]$
59	$\mathbb{Z}[1, 59i, 1/2+10i+1/2j, 5/2i+1/2ij]$

Capítol 2

Corbes de Shimura: introducció

En aquest capítol es defineixen les corbes de Shimura $X(D,N)$ mitjançant l'acció en el semiplà de Poincaré de certs grups fuchsians definits a partir d'ordres d'Eichler $\mathcal{O}(D,N)$ de $\mathbb{Q}$-àlgebres de quaternions. En primer lloc, descrivim l'estructura hiperbòlica del semiplà de Poincaré i donem resultats referents a les homografies i a les formes quadràtiques binàries associades. A continuació, definim els grups d'homografies quaterniònics $\Gamma(D,N)$ i els explicitem per als casos no ramificat i poc ramificat de tipus A i B. Utilitzant les notacions anteriors, donem la definició de corba de Shimura i les principals propietats que caracteritzen el model canònic, així com també la interpretació modular. Una recopilació de resultats sobre les constants associades a aquestes corbes ens permet implementar instruccions en el paquet `Poincare` per a calcular les constants associades a les corbes de Shimura i mostrar-ne taules.

2.1 El semiplà de Poincaré

Denotem per ι el nombre complex imaginari tal que $\iota^2 = -1$ i per $\mathrm{Re}(z)$ i $\mathrm{Im}(z)$, la part real i la part imaginària, respectivament, d'un punt $z \in \mathbb{C}$. Es coneix amb el nom de semiplà de Poincaré el semiplà complex superior $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Re}(z) > 0\}$, amb l'estructura donada per la geometria hiperbòlica. Com a referències principals citem [Vig80] i [Sie71].

Els punts hiperbòlics de $\mathcal{H}$ són els punts habituals $z \in \mathcal{H}$. Les rectes hiperbòliques són els semicercles de centre un nombre real i les semirectes ortogonals a l'eix real. Dos punts hiperbòlics z_1, z_2 determinen una única

recta hiperbòlica. La recta hiperbòlica determinada per dos punts $z_1, z_2 \in \mathcal{H}$, amb $\mathrm{Re}(z_1) \neq \mathrm{Re}(z_2)$, és el semicercle que passa per z_1 i z_2, i té com a centre el punt real donat per la intersecció de la recta perpendicular al segment $z_1 z_2$ i l'eix real. D'altra banda, aquesta recta conté els quatre punts complexos z_1, z_2, $\overline{z}_1^{-1}$ i $\overline{z}_2^{-1}$, la qual cosa també la determina.

La distància hiperbòlica $\delta(z_1, z_2)$ entre dos punts $z_1, z_2 \in \mathcal{H}$ es defineix com

$$\delta(z_1, z_2) := \left| \operatorname{arccosh} \left(1 + \frac{|z_1 - z_2|^2}{2 z_1 z_2} \right) \right|.$$

També es pot calcular d'altres maneres. Si els dos punts tenen la mateixa part real, $\delta(y_1, y_2) = \left| \log \left| \frac{y_2}{y_1} \right| \right|$. Si la recta hiperbòlica que uneix els dos punts és un arc de cercle, $\delta(z_1, z_2) = \left| \log \left| \frac{\tan(\theta_1/2)}{\tan(\theta_2/2)} \right| \right|$, on θ_1 i θ_2 són els angles determinats pels punts z_1 i z_2. La mesura hiperbòlica dels angles coincideix amb la mesura euclidiana.

La distància hiperbòlica és additiva sobre les rectes hiperbòliques i, en general, satisfà la desigualtat triangular. Les geodèsiques són les rectes hiperbòliques. Donat un punt $z \in \mathcal{H}$, per a trobar un punt que disti de z una distància d en una direcció prefixada s'utilitza una aplicació que porti el punt z a 0 i la direcció prefixada al semieix real positiu. Aleshores, s'escull el punt real que estigui a distància euclidiana t del 0, on $t = \dfrac{e^d - 1}{e^d + 1} = \tanh\left(\dfrac{d}{2}\right)$, i se li aplica la transformació inversa de l'anterior.

Els cercles hiperbòlics, és a dir, el lloc geomètric dels punts de $\mathcal{H}$ que disten r d'un punt z_0 donat, coincideixen amb els cercles euclidians continguts en $\mathcal{H}$.

Donats un punt $z \in \mathcal{H}$ i una recta hiperbòlica r, existeix una única recta hiperbòlica que passa per z i és perpendicular a r. Donats dos punts $z_1, z_2 \in \mathcal{H}$, la recta hiperbòlica perpendicular a la recta determinada per z_1, z_2 que passa pel seu punt mig (en el sentit hiperbòlic) és el lloc geomètric de $\mathcal{H}$ format pels punts que equidisten de z_1, z_2.

De les diferències entre la geometria euclidiana i la hiperbòlica, destaquem el fet que en aquesta última no se satisfà l'axioma de les paral·leles. Així, per un punt exterior a una recta hiperbòlica passen infinites rectes hiperbòliques que no tenen intersecció amb la recta inicial; a més, cap d'aquestes és equidistant de la recta inicial.

Es diu que un subconjunt de $\mathcal{H}$ és un conjunt convex hiperbòlic si per a cada

parella de punts del subconjunt, el segment de recta hiperbòlica que uneix els dos punts està contingut en el subconjunt. Tot conjunt convex hiperbòlic és connex i la intersecció d'una col·lecció de conjunts convexos també és un conjunt convex.

Un polígon hiperbòlic de $\mathcal{H}$ és un subconjunt de $\mathcal{H}$ acotat per una corba simple, formada per un nombre finit de segments hiperbòlics. El volum hiperbòlic d'un polígon hiperbòlic es calcula mitjançant la mesura

$$d\omega = \frac{4}{(1-|z|^2)^2}.$$

2.1.1 Proposició. *Sigui n el nombre de vèrtexs d'un polígon hiperbòlic P i siguin $\theta_1, \ldots, \theta_n$ els angles en els vèrtexs. Aleshores, el volum hiperbòlic del polígon, que denotem per $V_h(P)$, és*

$$V_h(P) = (n-2)\pi - (\theta_1 + \ldots + \theta_n).$$

Els vèrtexs d'un polígon hiperbòlic que són sobre l'eix real s'anomenen vèrtexs impropis; en cas contrari, s'anomenen vèrtexs propis. Observem que l'angle en un vèrtex impropi sempre és 0. Per la proposició anterior, el volum d'un polígon hiperbòlic és sempre $\leq (n-2)\pi$ i la igualtat es dóna només en el cas que tots els vèrtexs siguin impropis. En particular, la suma dels angles d'un triangle hiperbòlic és menor que π; aquesta és una altra de les diferències entre la geometria euclidiana i la geometria hiperbòlica.

Fixada una geometria, es diu que una aplicació és conforme si conserva els angles, en mesura i en signe. Notem que una aplicació és conforme respecte de la geometria hiperbòlica si, i només si, ho és respecte de la geometria euclidiana. En particular, les aplicacions conformes del pla hiperbòlic $\mathcal{H}$ coincideixen amb les isometries de $\mathcal{H}$: preserven la distància hiperbòlica, apliquen rectes hiperbòliques en rectes hiperbòliques i conserven la raó doble de 4 punts. Es demostra que les isometries de $\mathcal{H}$ són les aplicacions γ tals que

$$\gamma(z) = \frac{az+b}{cz+d}, \quad \text{on } a,b,c,d \in \mathbb{R},\ ad-bc=1,$$

anomenades, també, homografies.

2.2 Homografies

En aquesta secció, descrivim les homografies del semiplà de Poincaré amb més detall. Interpretem el seu caràcter en funció de la seva forma de Jordan i de

la forma quadràtica binària associada. Les definicions generals i els resultats coneguts d'aquesta secció es poden trobar a [Poi1887], [Shi71] i [Sie71].

Una homografia de $\mathcal{H}$, $\gamma : \mathcal{H} \to \mathcal{H}$, ve definida per

$$\gamma(z) = \frac{az+b}{cz+d}, \quad \text{on } a,b,c,d \in \mathbb{R},\ ad-bc=1.$$

El conjunt d'homografies de $\mathcal{H}$ és un grup isomorf a $\mathrm{PSL}(2,\mathbb{R})$. Habitualment, tractarem amb grups de matrius $\Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$. Cal tenir en compte que, com a grup homografies, cal prendre $\overline{\Gamma} := \Gamma/\pm\mathrm{Id}$, ja que γ i $-\gamma$ donen la mateixa homografia. En un abús del llenguatge, quan ens referim a un grup d'homografies Γ entendrem el grup d'homografies $\overline{\Gamma}$ corresponent.

Les homografies també es poden considerar com a aplicacions del pla complex $\mathbb{C}$ en si mateix. A continuació, descrivim unes altres aplicacions importants del pla complex en ell mateix: les inversions. Encara que no són aplicacions conformes, ens permetran interpretar geomètricament les homografies.

2.2.1 Definició. Sigui C el cercle de centre $o \in \mathbb{C}$ i radi r. La inversió respecte del cercle C és la transformació $f\colon \mathbb{C}\cup\{\infty\} \to \mathbb{C}\cup\{\infty\}$, que intercanvia els punts o i ∞ i que a cada punt $z \in \mathbb{C}-\{o\}$ fa correspondre el punt w de la recta que determinen z i o, de manera que el producte escalar de $\overrightarrow{oz}$ amb $\overrightarrow{ow}$ (pensats com a vectors de $\mathbb{R}^2$) sigui igual a r^2.

La inversió respecte d'un cercle és composició de la conjugació complexa i una aplicació conforme. Per tant, aquestes inversions canvien l'orientació dels angles, però en conserven la magnitud. Es demostra que tota homografia de $\mathrm{PSL}(2,\mathbb{R})$ s'expressa com a composició de dues inversions respecte de cercles escaients. En el lema següent donem dues expressions analítiques de la inversió respecte d'un cercle C.

2.2.2 Lema. *Siguin C un cercle del pla complex i $f\colon \mathbb{C}\cup\{\infty\} \to \mathbb{C}\cup\{\infty\}$ la inversió respecte de C. Aleshores:*

(i) *Si, en termes de variable complexa, $az\overline{z} + bz + \overline{b}\overline{z} + c = 0$ és l'equació del cercle C, la inversió f ve donada per $f(z) = \dfrac{-\overline{b}\overline{z}-c}{a\overline{z}+b}$.*

(ii) *Si C és el cercle de centre $o \in \mathbb{C}$ i radi r, la inversió f ve donada per $f(z) = o + \dfrac{r^2}{\overline{z}-\overline{o}}$.* □

2.2.3 Remarca. Notem que (i) inclou el cas $a = 0$, en el qual C és un recta vertical; en aquest cas la inversió és exactament la simetria axial d'eix C. Pel que fa a l'expressió de (ii), observem que si C és centrat a l'origen, $f(z) = r^2/\overline{z}$. En particular, per al cercle unitat obtenim l'expressió estàndard $f(z) = 1/\overline{z}$. En general, en el semiplà $\mathcal{H}$, si C és una recta hiperbòlica, aleshores la inversió respecte de C és la simetria respecte d'aquesta recta (en el sentit de la geometria hiperbòlica). L'anomenarem simetria hiperbòlica respecte de C. □

Sigui $\gamma \in \mathrm{SL}(2,\mathbb{R})$. Per a calcular els punts fixos de γ a $\mathbb{C}\cup\{\infty\}$, cal resoldre l'equació quadràtica $cz^2 + (d-a)z - b = 0$. Aquesta equació té com a solució un punt real, dos punts reals o bé dos punts complexos conjugats. Això dóna lloc a la definició següent.

2.2.4 Definició. Sigui $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$. Suposem que defineix una homografia de $\mathbb{C}$ diferent de $\pm\mathrm{Id}$.

(a) Es diu que γ és una homografia hiperbòlica si té dos punts fixos diferents a $\mathbb{R}\cup\{\infty\}$; equivalentment, si $(a+d)^2 > 4$; és a dir, $|\operatorname{tr}(\gamma)| > 2$.

(b) Es diu que γ és una homografia el·líptica si té un punt fix $z \in \mathcal{H}$ i l'altre punt fix és $\overline{z}$; equivalentment, si $(a+d)^2 < 4$; és a dir, $|\operatorname{tr}(\gamma)| < 2$.

(c) Es diu que γ és una homografia parabòlica si té únicament un punt fix a $\mathbb{R}\cup\{\infty\}$; equivalentment, si $(a+d)^2 = 4$; és a dir, $|\operatorname{tr}(\gamma)| = 2$. □

Observem que cada matriu $\gamma \in \mathrm{SL}(2,\mathbb{R})$, $\gamma \neq \pm\mathrm{Id}$, és conjugada sobre $\mathbb{C}$ d'una de les dues formes canòniques de Jordan següents:

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \text{ amb } \lambda_1 \neq \lambda_2, \quad \text{o bé } \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}.$$

El caràcter parabòlic, hiperbòlic o el·líptic d'una homografia es pot definir també a partir dels valors propis de la matriu, tal com s'indica en la proposició següent.

2.2.5 Proposició. *Donada una homografia $\gamma \in \mathrm{SL}(2,\mathbb{R})$, siguin λ_1, λ_2 els seus valors propis sobre $\mathbb{C}$ i posem $\mu := \dfrac{\lambda_1}{\lambda_2}$. Aleshores,*

(i) *γ és hiperbòlica si, i només si, $\mu \in \mathbb{R}^+$, on $\mu \neq 1$. En particular, si γ és hiperbòlica, els dos valors propis són diferents; per tant, γ és diagonalitzable.*

(ii) *γ és el·líptica si, i només si, $\mu = e^{\iota\theta}$, amb $0 < \theta < 2\pi$; en aquest cas es té que $\lambda_1 + \lambda_2 = 2\cos\theta$. En particular, si γ és el·líptica, els dos valors propis són diferents; per tant, γ és diagonalitzable.*

(iii) *γ és parabòlica si, i només si, $\mu = 1$. En particular, si γ és parabòlica, té un sol valor propi amb multiplicitat 2; per tant, γ no és diagonalitzable.*

DEMOSTRACIÓ: Per ser $\gamma \in \mathrm{SL}(2,\mathbb{R})$, tenim que $\lambda_1 + \lambda_2 = \mathrm{tr}(\gamma) = a + d \in \mathbb{R}$ i $\lambda_1\lambda_2 = \det(\gamma) = 1$, d'on $\mu = \lambda_1^2$. El polinomi característic de γ és $x^2 - (a+d)x + 1$. Distingirem tres casos, segons els valors propis.

Suposem que γ té dos valors propis reals, $\lambda_1 \neq \lambda_2$. D'una banda, això és equivalent a $\mu = \lambda_1^2 \in \mathbb{R}^+$, on $\mu \neq 1$; d'altra banda, això passa si, i només si, $(a+d)^2 > 4$, la qual cosa equival al fet que l'homografia sigui hiperbòlica.

Si suposem que s'obtenen dos valors propis complexos, aquests són conjugats. D'una banda, tenim $\overline{\lambda_1} = \lambda_2 = 1/\lambda_1$, que és equivalent a $n(\lambda_1) = 1$; d'altra banda, això passa si, i només si, $(a+d)^2 < 4$, la qual cosa equival al fet que l'homografia sigui el·líptica.

Finalment, suposem que hi ha un sol valor propi, de multiplicitat 2. D'una banda, es té que $\lambda_1 = \lambda_2 = \pm 1$, la qual cosa és equivalent a $\mu = 1$; d'altra banda, això passa si, i només si, $(a+d)^2 = 4$, la qual cosa equival al fet que l'homografia sigui parabòlica. □

Per als casos no parabòlics, el valor μ s'anomena el multiplicador de γ, la qual cosa sembla natural a partir de la interpretació geomètrica següent. Considerem la homografia γ, donada per certa matriu M i el canvi de variables que transforma M en la seva matriu de Jordan. Si γ és hiperbòlica o el·líptica, aquest canvi de variables porta els seus dos punts fixos al 0 i a l'infinit, respectivament. Aleshores la homografia s'interpreta geomètricament com una homotècia de raó μ amb centre en l'origen per al cas hiperbòlic i com una rotació d'angle θ igual a l'argument de μ al voltant de l'origen per al cas el·líptic. En el cas d'una homografia parabòlica, el canvi porta el seu únic punt fix a l'infinit i geomètricament és una translació.

Observem que les homografies el·líptiques tals que $\theta = \frac{p}{q}\pi$, amb $p, q \in \mathbb{Z}$, tenen ordre finit. Les homografies parabòliques són ordre infinit.

2.2.6 Lema. *Sigui $\gamma \in \Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$ una homografia el·líptica.*

(i) *Si $\mathrm{tr}(\gamma) = 0$, aleshores γ és d'ordre 2 o bé 4, segons que $-\mathrm{Id} \in \Gamma$ o bé $-\mathrm{Id} \notin \Gamma$, respectivament.*

(ii) *Si* $\mathrm{tr}(\gamma) = 1$, *aleshores* γ *és d'ordre* 3 *o bé* 6, *segons que* $-\mathrm{Id} \in \Gamma$ *o bé* $-\mathrm{Id} \notin \Gamma$, *respectivament.*

DEMOSTRACIÓ: Només cal calcular les potències d'una expressió general de l'homografia γ. Si $\mathrm{tr}(\gamma) = 0$, s'obté que $\gamma^2 = -\mathrm{Id}$. Si $\mathrm{tr}(\gamma) = 1$, s'obté que $\gamma^3 = -\mathrm{Id}$. Recordem que com a grup d'homografies ens cal considerar $\Gamma/\pm\mathrm{Id}$.

Notem que aquestes són les dues úniques possibilitats per a les homografies el·líptiques de traça a $\mathbb{Z}$. □

Es pot interpretar també la classificació de les homografies i els seus punts fixos en funció del caràcter de determinades formes quadràtiques binàries i dels punts que determinen. Les definicions generals sobre formes quadràtiques es donaran en el capítol 4.

2.2.7 Definicions. Donada una matriu $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2,\mathbb{R})$, la forma quadràtica binària associada és

$$f_\gamma(X,Y) := cX^2 + (d-a)XY - bY^2.$$

Per a una forma quadràtica binària f de coeficients reals, $f(X,Y) = AX^2 + BXY + CY^2$, posem $\mathcal{P}(f)$ el conjunt de punts complexos de part imaginària no negativa solució de l'equació quadràtica determinada $AX^2 + BX + C = 0$. És a dir,

$$\mathcal{P}(f) = \{z : Az^2 + Bz + C = 0,\ \mathrm{Re}(z) \geq 0\}.$$

Si $\mathcal{P}(f) \cap \mathcal{H} \neq \emptyset$, aleshores $\mathcal{P}(f)$ conté un únic punt, que denotem per $\tau(f)$. □

A partir de la definició de forma binària associada a una homografia i del conjunt de punts que determina, obtenim la proposició següent.

2.2.8 Proposició. *Sigui* $\gamma \in \mathrm{M}(2,\mathbb{R})$.

(i) *Per a tot* $\lambda, \mu \in \mathbb{Q}$, *tenim que* $f_{\lambda\gamma} = \lambda f_\gamma$ *i* $f_{\gamma+\mu\,\mathrm{Id}} = f_\gamma$; *en particular,* $\mathcal{P}(f_{\lambda\gamma+\mu\,\mathrm{Id}}) = \mathcal{P}(f_\gamma)$.

(ii) *Sigui* $z \in \mathcal{H} \cup \mathbb{R}$. *Aleshores,* z *és un punt fix de* γ *si, i només si,* $z \in \mathcal{P}(f_\gamma)$.

(iii) *Sigui* $P \in \mathrm{GL}(2,\mathbb{R})$. *Aleshores,* $f_{P^{-1}\gamma P} = (\det P^{-1}) P^t f_\gamma P$. □

2.2.9 Proposició. *Sigui* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2,\mathbb{R})$ *i sigui* f_γ *la forma quadràtica binària associada. Aleshores,*

(i) f_γ *és indefinida si, i només si,* $(\mathrm{tr}(\gamma))^2/4 > \det(\gamma)$*, si, i només si,* $\mathcal{P}(f_\gamma) = \{x_1, x_2\} \subseteq \mathbb{R}$.

(ii) f_γ *és definida si, i només si,* $(\mathrm{tr}(\gamma))^2/4 < \det(\gamma)$*, si, i només si,* $\mathcal{P}(f_\gamma) = \{\tau, \overline{\tau}\} \subseteq \mathbb{C}$, $\tau \in \mathcal{H}$.

(iii) f_γ *és degenerada si, i només si,* $(\mathrm{tr}(\gamma))^2/4 = \det(\gamma)$*, si, i només si,* $\mathcal{P}(f_\gamma) = \{x\} \subseteq \mathbb{R}$.

DEMOSTRACIÓ: Tenim que $\det_1(f_\gamma) := -bc - \frac{1}{4}(d-a)^2 = \det(\gamma) - \frac{(a+d)^2}{4}$. Així, la forma quadràtica f_γ és indefinida, definida o degenerada segons que $(\mathrm{tr}(\gamma))^2/4$ sigui més gran, més petit o igual a $\det(\gamma)$, respectivament. Observem que, en el cas definit, serà definida positiva o definida negativa depenent del signe de c. □

En el corol·lari següent donem una interpretació geomètrica que justifica els noms donats a les homografies.

2.2.10 Corol·lari. *Siguin* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ *i* f_γ *la forma binària associada. Sigui* $\kappa \in \mathbb{R}$*, on* $\kappa \neq 0$*. Aleshores,*

(i) γ *és hiperbòlica si, i només si,* f_γ *és indefinida, si, i només si, la cònica* $f_\gamma = \kappa$ *és una hipèrbola.*

(ii) γ *és el·líptica si, i només si,* f_γ *és definida, si, i només si, la cònica* $f_\gamma = \kappa$ *és una el·lipse.*

(iii) γ *és parabòlica si, i només si,* f_γ *és degenerada, si, i només si, la cònica* $f_\gamma = \kappa$ *és una paràbola.*

DEMOSTRACIÓ: Tenim que $\det_1(f_\gamma) = -bc - \frac{1}{4}(d-a)^2) = 1 - \frac{(a+d)^2}{4}$, ja que $\det\gamma = 1$. Així, segons el seu signe, la forma quadràtica f_γ és indefinida, definida o degenerada depenent de si $(a+d)^2$ és més gran, més petit o igual a 4, respectivament. Aquesta condició equival, precisament, al fet que l'homografia sigui hiperbòlica, el·líptica o bé parabòlica, respectivament. □

2.2.11 Lema. *Sigui* $\gamma \in \mathrm{GL}(2,\mathbb{R})$ *de* $\det(\gamma) > 0$. *Aleshores es té que* $\sigma^{-1}\gamma\sigma \neq -\gamma$, *per a tot* $\sigma \in \mathrm{GL}(2,\mathbb{R})$.

DEMOSTRACIÓ: D'entrada, si $\mathrm{tr}(\gamma) \neq 0$, és cert, ja que la traça es conserva per conjugació, $\mathrm{tr}(\sigma^{-1}\gamma\sigma) = \mathrm{tr}(\gamma)$ i $\mathrm{tr}(-\gamma) = -\mathrm{tr}(\gamma)$.

Suposem, doncs, $\mathrm{tr}(\gamma) = 0$ i considerem les formes quadràtiques associades. Si $\det(\gamma) > 0$, aleshores f_γ i $f_{-\gamma}$ seran formes quadràtiques binàries definides, definida positiva l'una i definida negativa l'altra. La signatura és un invariant de la classe d'equivalència sobre $\mathbb{R}$; per tant, no poden ser equivalents. □

2.2.12 Remarca. El resultat anterior no s'estén a $\det(\gamma) < 0$. Per exemple, tenim que $\sigma^{-1}\gamma\sigma = -\gamma$ si

$$\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{i} \quad \gamma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \square$$

En particular, si $z \in \mathbb{R}$ és un punt fix de γ, aleshores f_γ és isòtropa sobre $\mathbb{R}$, ja que $f_\gamma(z,1) = 0$. El cas el·líptic es presenta quan la forma quadràtica f_γ és anisòtropa sobre $\mathbb{R}$.

2.2.13 Definició. Sigui $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$ un grup d'homografies que actua en el semiplà de Poincaré $\mathcal{H}$. Es diu que Γ actua de forma pròpia i discontínua si existeixen un punt z_0 i un nombre real $\varepsilon > 0$ tals que, per a tot $\gamma \in \Gamma$, $\gamma \neq \pm\mathrm{Id}$, es té que $|\gamma(z_0) - z_0| > \varepsilon$. En aquest cas, es diu que z_0 és un punt estàndard respecte de Γ. La definició d'acció pròpia i discontínua equival al fet que Γ sigui un subgrup discret de $\mathrm{SL}(2,\mathbb{R})$.

L'acció de Γ en $\mathcal{H}$ dóna una relació d'equivalència entre els seus punts. Es diu que dos punts $z, z' \in \mathcal{H}$ són equivalents respecte de Γ si, i només si, $z' = \gamma(z)$ per a algun $\gamma \in \Gamma$.

2.2.14 Definicions. Un punt $x \in \mathbb{R} \cup \{\infty\}$ es diu que és un punt parabòlic, respectivament hiperbòlic, respecte de Γ si existeix una homografia $\gamma \in \Gamma$ parabòlica, respectivament hiperbòlica, tal que $\gamma(x) = x$. Un punt $z \in \mathcal{H}$ es diu que és un punt el·líptic respecte de Γ si existeix una homografia el·líptica $\gamma \in \Gamma$, $\gamma \neq \pm\mathrm{Id}$, tal que $\gamma(z) = z$. El grup d'isotropia d'un punt z respecte de Γ és el grup $\Gamma_z = \{\gamma \in \Gamma \mid \gamma(z) = z\}$. □

Si Γ és un subgrup discret de $\mathrm{SL}(2,\mathbb{R})$, el grup d'isotropia d'un punt el·líptic és un grup cíclic finit, format per matrius el·líptiques. De fet, els únics

elements no trivials de Γ d'ordre finit són precisament les matrius el·líptiques. Les matrius d'ordre 2 donen lloc a les homografies anomenades involucions; són les de multiplicador $\mu = -1$.

2.2.15 Definició. L'ordre d'un punt el·líptic $z \in \mathcal{H}$ respecte de Γ és l'ordre del seu grup d'isotropia respecte de Γ a $\mathrm{PSL}(2,\mathbb{R})$. És a dir, l'ordre d'un punt el·líptic z és $\sharp\Gamma_z$ si $-\mathrm{Id} \notin \Gamma$, o bé $\frac{1}{2}\sharp\Gamma_z$ si $-\mathrm{Id} \in \Gamma$. □

Si z és un punt el·líptic respecte de Γ, aleshores es veu fàcilment que $\gamma(z)$, per a tot $\gamma \in \Gamma$, és també un punt el·líptic respecte de Γ. A més, dos punts el·líptics equivalents són del mateix ordre, ja que els seus grups d'isotropia són conjugats, $\Gamma_{\gamma(z)} = \gamma\Gamma_z\gamma^{-1}$.

2.2.16 Lema. *Sigui* $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$ *un subgrup tal que per a tota matriu* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *és* $\gamma' := \begin{pmatrix} -a & b \\ c & -d \end{pmatrix} \in \Gamma$.

(i) *Dos punts de* $\mathcal{H}$ *són* Γ*-equivalents si, i només si, els seus simètrics respecte de l'eix imaginari també ho són.*

(ii) *Un punt de* $\mathcal{H}$ *és el·líptic respecte de* Γ *si, i només si, el seu simètric respecte de l'eix imaginari també ho és. En aquest cas són del mateix ordre.*

DEMOSTRACIÓ: Siguin $z, w \in \mathcal{H}$ tals que $\gamma(z) = w$, amb $\gamma \in \Gamma$. Aleshores, tenim que $\gamma'(-\overline{z}) = -\overline{w}$, la qual cosa demostra (i).

Considerant en particular $z = w$, s'obté l'apartat (ii). Notem que γ i γ' tenen el mateix ordre com a homografies, per la qual cosa els punts, en cas de ser el·líptics, són també del mateix ordre. □

2.2.17 Definició. Un subconjunt tancat connex $\mathcal{D} \subseteq \mathcal{H} \cup \mathbb{R} \cup \{\infty\}$ és un domini fonamental per l'acció de Γ en $\mathcal{H}$ si els punts de l'interior de $\mathcal{D}$ no són dos a dos Γ-equivalents i cada punt de $\mathcal{H}$ és Γ-equivalent a algun punt de $\mathcal{D}$. □

Evidentment, el domini fonamental d'un grup Γ no és únic. Per exemple, si $\mathcal{D}$ és un domini fonamental de Γ, aleshores $\gamma(\mathcal{D})$ també ho és, per a qualsevol $\gamma \in \Gamma$.

2.2.18 Definició. Un cicle d'un domini fonamental és una òrbita de vèrtexs. Direm que un cicle és el·líptic d'ordre k si està format per vèrtexs el·líptics

d'ordre k. El cicle és parabòlic, si està format per vèrtexs parabòlics; convenim aleshores que és d'ordre $k = \infty$. □

2.3 Grups d'homografies quaterniòniques

Sigui $D \geq 1$ un nombre natural producte d'un nombre parell de primers diferents. Sigui $N \geq 1$ un nombre natural tal que $\mathrm{mcd}(D, N) = 1$. Tot seguit definim uns grups de matrius que només depenen de D i N, llevat conjugació.

Considerem a aquest efecte una àlgebra de quaternions H sobre $\mathbb{Q}$ de discriminant D. L'àlgebra H és una àlgebra indefinida, ramificada o no, determinada llevat isomorfismes. Sigui un $\mathbb{Z}$-ordre d'Eichler $\mathcal{O}(D, N) \subseteq H$ de nivell N. Considerem el grup d'unitats quaterniòniques format per les unitats de norma positiva:

$$\mathcal{O}(D, N)^*_+ := \{\alpha \in \mathcal{O}(D, N)^* : n(\alpha) = 1\}.$$

Per 1.2.33, $\mathcal{O}(D, N)^*_+$ només depèn de D i de N, llevat conjugació.

Com a conseqüència dels resultats d'Eichler [Eic38], per als ordres d'Eichler de les $\mathbb{Q}$-àlgebres de quaternions, el grup d'unitats quaterniòniques $\mathcal{O}(D, N)^*_+$ té les propietats següents.

2.3.1 Proposició. *Siguin H una $\mathbb{Q}$-àlgebra de quaternions definida i $\mathcal{O}(D, 1)$ un ordre maximal. Aleshores no hi ha cap element de $\mathcal{O}(D, 1)$ de norma reduïda -1; per tant, $\mathcal{O}(D, 1)^*_+ = \mathcal{O}(D, 1)^*$. A més, $\mathcal{O}(D, 1)^*$ és un grup cíclic d'ordre 2, 4 o bé 6, excepte si:*

(i) $H = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, *que té $D_H = 2$; aleshores, $\mathcal{O}(D, 1)^*$ és isomorf a $E_{24} := \{\pm 1, \pm i, \pm j, \pm ij, \frac{\pm 1 \pm i \pm j \pm ij}{2}\}$, el grup binari tetraedral.*

(ii) $H = \left(\frac{-1,-3}{\mathbb{Q}}\right)$, *que té $D_H = 3$; aleshores, $\mathcal{O}(D, 1)^* \simeq < s_6, j >$, un grup dicíclic, amb $s_6 = \cos 2\pi/6 + \sin 2\pi/6$.* □

2.3.2 Teorema. *Siguin H una $\mathbb{Q}$-àlgebra de quaternions indefinida i $\mathcal{O}(D, N)$ un ordre d'Eichler. Aleshores, $\mathcal{O}(D, N)$ té unitats de norma reduïda -1. Per tant, $\mathcal{O}(D, N)^*_+$ és d'índex 2 en $\mathcal{O}(D, N)^*$.* □

Fixem un isomorfisme $\Phi : H \otimes \mathbb{R} \to \mathrm{M}(2,\mathbb{R})$, que existeix per ser H una àlgebra de quaternions indefinida. Per 1.1.4, aquest isomorfisme és únic llevat conjugació. Aleshores,

$$\Gamma(D,N) := \Phi(\mathcal{O}(D,N)^*_+)$$

és un subgrup discret de $\mathrm{SL}(2,\mathbb{R})$, determinat per D i N, llevat conjugació. Així, el grup $\Gamma(D,N)$ actua en el semiplà de Poincaré i l'anomenarem grup d'homografies quaterniòniques. Recordem que, com a grup d'homografies, cal pensar els elements a $\Gamma(D,N)/\pm\mathrm{Id}$.

Fixem el monomorfisme explícit de la proposició 1.1.25. Així, per a una àlgebra de quaternions indefinida $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, suposem que $a > 0$ i considerem el monomorfisme $\Phi : H \hookrightarrow \mathrm{M}(2,\mathbb{R})$ que està donat per

$$\Phi(x+\sqrt{a}y+\sqrt{b}z+\sqrt{a}\sqrt{b}t) = \begin{pmatrix} x+\sqrt{a}y & z+\sqrt{a}t \\ b(z-\sqrt{a}t) & x-\sqrt{a}y \end{pmatrix}.$$

Per tant, $\Gamma(D,N) \subseteq \left\{ \begin{pmatrix} \alpha & \beta \\ b\beta' & \alpha' \end{pmatrix} : \alpha,\beta \in \mathbb{Q}(\sqrt{a}) \right\} \subseteq \mathrm{SL}(2,\mathbb{Q}(\sqrt{a}))$. El cas $a = 1$ correspon necessàriament a una àlgebra de quaternions no ramificada; és a dir, $D = 1$. En aquest cas, s'obté que $\Gamma(1,N) \subseteq \mathrm{SL}(2,\mathbb{Q})$.

En funció del monomorfisme Φ que hem fixat, explicitem els grups d'homografies quaterniòniques per a les àlgebres de quaternions no ramificades i poc ramificades del primer capítol.

2.3.3 Cas no ramificat. Considerem l'àlgebra de quaternions no ramificada $H = M(2,\mathbb{Q})$. En aquest cas, Φ és la immersió canònica. Per a cada N, considerem l'ordre d'Eichler de nivell N

$$\mathcal{O}_0(1,N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} : a,b,c,d \in \mathbb{Z} \right\}.$$

Obtenim directament que $\Gamma(1,N) = \mathcal{O}(1,N)^*_+$ és el grup de congruència denotat habitualment per $\Gamma_0(N)$.

Si considerem l'àlgebra de quaternions no ramificada $H' = \left(\frac{1,-1}{\mathbb{Q}}\right)$ i l'ordre d'Eichler $\mathcal{O}_M(1,N) := \mathbb{Z}[1, \frac{j+ij}{2}, N\frac{(-j+ij)}{2}, \frac{1-i}{2}]$, de nivell N, obtenim igualment que $\Phi(\mathcal{O}_M(1,N)^*_+) = \Gamma_0(N)$. □

2.3.4 Cas poc ramificat de tipus A. Considerem l'àlgebra de quaternions $H_A(p) = \left(\frac{p,-1}{\mathbb{Q}}\right)$ i l'ordre $\mathcal{O}_A(2p,N) = \mathbb{Z}\left[1, i, Nj, \frac{1+i+j+ij}{2}\right]$, per a $N \left| \frac{p-1}{2}\right.$ lliure de quadrats, que és un ordre d'Eichler de nivell N. Posem $F = \mathbb{Q}(\sqrt{p})$ i denotem $\alpha \mapsto \alpha'$ la conjugació en F.

Obtenim les següents descripcions equivalents per al grup $\Gamma(2p,N)$:

(i) $\gamma = \frac{1}{2}\begin{pmatrix} (2x+t)+(2y+t)\sqrt{p} & (2Nz+t)+t\sqrt{p} \\ -(2Nz+t)+t\sqrt{p} & (2x+t)-(2y+t)\sqrt{p} \end{pmatrix} \in \Gamma(2p,N)$ si, i només si, $x,y,z,t \in \mathbb{Z}$ i $\det(\gamma) = 1$.

(ii) $\gamma = \frac{1}{2}\begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ -c+d\sqrt{p} & a-b\sqrt{p} \end{pmatrix} \in \Gamma(2p,N)$ si, i només si, a,b,c,d enters, $a \equiv b \equiv c \equiv d \mod 2$, $N \mid c-d$ i $\det(\gamma) = 1$.

(iii) $\gamma = \frac{1}{2}\begin{pmatrix} \alpha & \beta \\ -\beta' & \alpha' \end{pmatrix} \in \Gamma(2p,N)$ si, i només si, $\alpha, \beta \in \mathbb{Z}[\sqrt{p}]$, $\alpha \equiv \beta \equiv \alpha\sqrt{p} \mod 2$, $N \mid \left(\mathrm{tr}(\beta) - \frac{\beta-\beta'}{\sqrt{p}}\right)$ i $\det(\gamma) = 1$. □

2.3.5 Cas poc ramificat de tipus B. Considerem l'àlgebra de quaternions $H_B(p,q) = \left(\frac{p,q}{\mathbb{Q}}\right)$. Sigui N lliure de quadrats, $N \left| \frac{q-1}{4}\right.$, $\mathrm{mcd}(N,p) = 1$ i considerem l'ordre d'Eichler

$$\mathcal{O}_B(pq,N) = \mathbb{Z}\left[1, Ni, \frac{1+j}{2}, \frac{i+ij}{2}\right].$$

Aleshores, tenim les següents descripcions equivalents del grup $\Gamma(pq,N)$:

(i) $\gamma = \frac{1}{2}\begin{pmatrix} (2x+z)+(2Ny+t)\sqrt{p} & z+t\sqrt{p} \\ q(z+t\sqrt{p}) & (2x+z)-(2Ny+t)\sqrt{p} \end{pmatrix}$ és del grup $\Gamma(pq,N)$ si, i només si, $x,y,z,t \in \mathbb{Z}$ i $\det(\gamma) = 1$.

(ii) $\gamma = \frac{1}{2}\begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ q(c-d\sqrt{p}) & a-b\sqrt{p} \end{pmatrix}$ és del grup $\Gamma(pq,N)$ si, i només si, $a,b,c,d \in \mathbb{Z}$, $a \equiv c \mod 2$, $b \equiv d \mod 2$, $2N \mid b-d$ i $\det(\gamma) = 1$.

(iii) $\gamma = \frac{1}{2}\begin{pmatrix} \alpha & \beta \\ -\beta' & \alpha' \end{pmatrix}$ és del grup $\Gamma(pq, N)$ si, i només si, $\alpha, \beta \in \mathbb{Z}[\sqrt{p}]$, $\alpha \equiv \beta \mod 2$, $N \mid \frac{\alpha - \alpha' - \beta + \beta'}{2\sqrt{p}}$) i $\det(\gamma) = 1$. □

2.3.6 Remarca. Tots els grups $\Gamma(D, N)$ d'homografies quaterniòniques satisfan la hipòtesi del lema 2.2.16. Així, tindrem condicions de simetria pels punts el·líptics i els punts de $\mathcal{H}$ $\Gamma(D, N)$-equivalents.

També és cert que tots els grups $\Gamma(D, N)$ d'homografies quaterniòniques contenen sempre $-\mathrm{Id}$, ja que l'element -1 és sempre una unitat de l'ordre $\mathcal{O}(D, N)$ i $\Phi(-1) = -\mathrm{Id}$. Per tant, per 2.2.6, les homografies el·líptiques definides per $\Gamma(D, N)$ seran només d'ordre 2 o bé 3. □

2.4 Les corbes de Shimura $X(D, N)$

Siguin $D \geq 1$ un nombre natural producte d'un nombre parell de primers diferents i $N \geq 1$ un nombre natural tal que $\mathrm{mcd}(D, N) = 1$.

Fixem els objectes següents: una $\mathbb{Q}$-àlgebra de quaternions H indefinida, de discriminant $D_H = D$; un $\mathbb{Z}$-ordre d'Eichler $\mathcal{O}(D, N) \subseteq H$ de nivell N, i un monomorfisme $\Phi : H \hookrightarrow \mathrm{M}(2, \mathbb{R})$. Considerem el grup d'homografies quaterniòniques $\Gamma(D, N)$ definit per l'ordre $\mathcal{O}(D, N)$, el qual depèn només de D i de N, llevat conjugació. El grup $\Gamma(D, N)$ és un subgrup discret de $\mathrm{SL}(2, \mathbb{R})$, que actua en el semiplà de Poincaré $\mathcal{H}$ de forma pròpia i discontínua. De fet, és un grup fuchsià de primera espècie. Fent quocient per aquesta acció, obtenim la superfície de Riemann $\Gamma(D, N) \setminus \mathcal{H}$.

La teoria de Shimura proporciona un model canònic del quocient $\Gamma(D, N)\setminus\mathcal{H}$, que denotem per $X(D, N)$, amb les propietats següents:

(i) $X(D, N)$ és una corba projectiva definida sobre $\mathbb{Q}$.

(ii) Existeix una aplicació $j_{D,N} : \mathcal{H} \to X(D, N)(\mathbb{C})$ que factoritza en un isomorfisme entre l'espai analític $\Gamma(D, N) \setminus \mathcal{H}$ i un obert Zariski de $X(D, N)(\mathbb{C})$.

(iii) Sigui $F = \mathbb{Q}(\sqrt{d})$ un cos quadràtic imaginari que escindeix l'àlgebra H. Sigui φ una immersió de F en H. Sigui $z \in \mathcal{H}$ l'únic punt fix comú de tots els elements de $\Phi(\varphi(F^*))$. Aleshores, les coordenades del punt

$j_{D,N}(z)$ són algebraiques, més concretament $j_{D,N}(z) \in X(D,N)(F_{\mathrm{ab}})$, on $F_{\mathrm{ab}} \subseteq \mathbb{C}$ denota l'extensió abeliana maximal de F.

$X(D,N)_{/\mathbb{Q}}$ s'anomena la corba de Shimura associada al subgrup $\Gamma(D,N)$.

El cas $D = 1$ correspon a una àlgebra de quaternions no ramificada $H \simeq \mathrm{M}(2,\mathbb{Q})$. En aquest cas, $\Gamma(1,N) \setminus \mathcal{H}$ és una superfície de Riemann no compacta, amb covolum finit. Atesa l'expressió anterior dels grups $\Gamma(1,N)$, és clar que la corba $X(1,N)$ obtinguda en compactificar és precisament la corba modular $X_0(N)$.

Si $D > 1$, l'àlgebra de quaternions és ramificada. En aquest cas, la superfície de Riemann $\Gamma(D,N) \setminus \mathcal{H}$ ja és compacta. Al capítol 8 donarem una demostració senzilla d'aquest fet.

La interpretació modular de $X(D,N)$ és la següent. Un punt de $X(D,N)(\mathbb{C})$ correspon a una classe d'isomorfia de tripletes (A,i,G), on A és una superfície abeliana, $i : H \hookrightarrow \mathrm{End}(A) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ és tal que $i^{-1}(\mathrm{End}(A)) = \mathcal{O}(D,N)$ i G és un subgrup del grup de punts de A d'ordre N que és un $\mathcal{O}(D,N)$-mòdul cíclic d'ordre N.

A continuació, recopilem alguns resultats sobre el càlcul de constants associades a les corbes de Shimura.

Cal remarcar que certs càlculs es poden dur a terme de forma general per al cas ramificat i per al cas no ramificat alhora. Per exemple, es tenen fórmules explícites per al nombre de classes d'equivalència dels punts elíptics i per al volum que inclouen ambdós casos. En canvi, altres tipus de resultats com per exemple les equacions, presenten diferents graus de dificultat, i no només no hi ha resultats uniformes per als dos casos, sinó que, a més, hi ha molta diferència entre el que es coneix en un cas o en l'altre.

2.4.1 Notació. Donada una corba de Shimura $X(D,N)$, denotarem per $V_h(D,N)$ el volum hiperbòlic, per $e_i(D,N)$ el nombre de cicles elíptics d'ordre i i per $g(D,N)$ el gènere. Es considera també una normalització de la mesura hiperbòlica, donada per la mesura $\dfrac{\mathrm{d}x\mathrm{d}y}{2\pi y^2}$. Denotem per $V(D,N)$ el volum de $X(D,N)$ calculat amb aquesta mesura normalitzada. Així, s'obté que $V(D,N) = \dfrac{1}{2\pi} V_h(R)$ i es demostra que és un nombre racional. □

Les proposicions següents proporcionen una manera aritmètica de calcular aquestes constants, cf. [Shi71] i [Vig80].

2.4.2 Proposició. *El volum $V(D,N)$ de la corba $X(D,N)$ és igual a*

$$V(D,N) = \frac{N}{6}\prod_{p|D}(p-1)\prod_{p|N}(1+\frac{1}{p}).\square$$

2.4.3 Proposició. *Els cicles el·líptics per la corba $X(D,N)$ són d'ordre 2 o bé 3. El seu nombre ve donat per:*

$$e_2(D,N) = \begin{cases} \displaystyle\prod_{p|D}\left(1-\left(\frac{-4}{p}\right)\right)\prod_{p|N}\left(1+\left(\frac{-4}{p}\right)\right) & \text{si } 4 \nmid N, \\ 0 & \text{si } 4 \mid N, \end{cases}$$

$$e_3(D,N) = \begin{cases} \displaystyle\prod_{p|D}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|N}\left(1+\left(\frac{-3}{p}\right)\right) & \text{si } 9 \nmid N, \\ 0 & \text{si } 9 \mid N. \square \end{cases}$$

Per al cas $D = 1$, es recuperen les fórmules habituals, cf. [Shi71]; en particular, per a N primer, es demostren de forma directa en el capítol 3.

Per a les corbes de Shimura corresponents a les àlgebres de quaternions poc ramificades de tipus A i de tipus B, deduïm els dos resultats següents.

2.4.4 Corol·lari. *Sigui $X(2p,1)$ la corba de Shimura associada a un ordre maximal d'una àlgebra de discriminant $2p$ poc ramificada de tipus A. Aleshores,*

$$e_2(2p,1) = 2, \quad e_3(2p,1) = \begin{cases} 4 & \text{si } p \equiv 11 \mod 12, \\ 2 & \text{si } p = 3, \\ 0 & \text{si } p \equiv 7 \mod 12. \square \end{cases}$$

2.4.5 Corol·lari. *Sigui $X(pq,1)$ la corba de Shimura associada a un ordre maximal d'una àlgebra de discriminant $2p$ poc ramificada de tipus B. Aleshores,*

$$e_2(pq,1) = 0, \quad e_3(pq,1) = \begin{cases} 4 & \text{si } p \equiv 2 \mod 3 \text{ i } q \equiv 5 \mod 12, \\ 2 & \text{si } p = 3, \\ 0 & \text{altrament. } \square \end{cases}$$

2.4.6 Proposició. *El gènere de la corba $X(D,N)$ ve donat per la relació*

$$2 - 2g(D,N) = -V(D,N) + \frac{1}{2}e_2(D,N) + \frac{2}{3}e_3(D,N) + e_\infty(D,N). \square$$

A partir de la relació entre les constants anteriors, podem deduir propietats sobre els dominis fonamentals possibles per a la corba $X(D,N)$.

2.4.7 Proposició. *Sigui $X(D,N)$ una corba de Shimura amb $D>1$. Suposem que $X(D,N)$ té un domini fonamental tal que tots els seus vèrtexs són el·líptics. Aleshores, el nombre de vèrtexs d'aquest domini fonamental és*

$$n_e(D,N) = 2 + 2V(D,N) + e_2(D,N) + \frac{2}{3}e_3(D,N).$$

DEMOSTRACIÓ: Suposem que tenim un domini fonamental de $X(D,N)$ tal que tots els seus vèrtexs són el·líptics i sigui $n_e(D,N)$ el nombre de vèrtexs que conté. Aleshores, el volum hiperbòlic $V_h(D,N)$ es calcula com $V_h(D,N) = (n_e(D,N)-2)\pi - (\theta_1 + \cdots + \theta_n)$, on $\theta_1, \ldots, \theta_n$ són els angles en els vèrtexs.

En general, no coneixem els angles en els vèrtexs. Suposant que tots els vèrtexs són punts el·líptics, podem determinar-ne la suma a partir del nombre de cicles el·líptics d'ordre 2 i 3, ja que els angles d'un cicle d'ordre q sumen exactament $2\pi/q$. Així, la suma dels angles és $\pi e_2(D,N) + \frac{2\pi}{3}e_3(D,N)$.

Per tant, tenim que $2\pi V(D,N) = (n_e(D,N)-2)\pi - (\pi e_2(D,N) + \frac{2\pi}{3}e_3(D,N))$; d'aquí deduïm l'expressió per a $n_e(D,N)$ donada a l'enunciat. Notem que qualsevol domini fonamental que tingui tots els vèrtexs el·líptics ha de tenir exactament $n_e(D,N)$ vèrtexs. □

A continuació explicitem el resultat per al cas que l'ordre quaterniònic sigui maximal.

2.4.8 Corol·lari. *Sigui $X(D,1)$, amb $D>1$ una corba de Shimura. Suposem que existeix un domini fonamental de $X(D,1)$ tal que tots els seus vèrtexs són el·líptics. Aleshores, el nombre de vèrtexs d'aquest domini fonamental és*

$$n_e(D,1) = 2 + \frac{1}{3}\prod_{p|D}(p-1) + \prod_{p|D}(1-\left(\frac{-4}{p}\right)) + \frac{2}{3}\prod_{p|D}\left(1-\left(\frac{-3}{p}\right)\right).$$

DEMOSTRACIÓ: Només cal substituir en la fórmula de la proposició anterior les expressions que es tenen per al volum aritmètic i el nombre de punts el·líptics, les quals depenen directament dels primers que divideixen el discriminant de l'àlgebra de quaternions inicial. □

Aquests resultats no són aplicables a les corbes modulars, ja que aquestes tenen punts parabòlics.

2.5 Algoritmes i taules

Pel que fa al contingut d'aquest capítol, en el paquet `Poincare` hem implementat instruccions que fan referència a geometria hiperbòlica, homografies, grups quaterniònics i constants associades a les corbes de Shimura.

En relació amb la primera secció, comentem breument les comandes de geometria hiperbòlica que hem implementat. Donats dos punts del semiplà de Poincaré, `eqHypL`, `defHypL` i `plotHypL` retornen l'equació, la definició com a objecte geomètric i la representació gràfica de la recta hiperbòlica que passa pels dos punts, respectivament. La instrucció `disthip` dóna la distància hiperbòlica entre els dos punts. Per a calcular calcula l'angle determinat per tres punts ordenats del semiplà de Poincaré tenim les instruccions `angHypei` `angHyp`, que en calculen el valor expressat en decimals exactes o bé expressat en funció de π, respectivament; en el segon cas es realitza una aproximació. Donats n punts del semiplà que defineixen un polígon hiperbòlic, tenim les instruccions anàlogues `eqHypPol`, `defHypPol` i `plotHypPol`, que donen les equacions de les rectes determinades per les arestes, la definició com a objectes geomètrics i la representació gràfica del polígon hiperbòlic, respectivament. Per a calcular el volum hiperbòlic del polígon tenim la instrucció `volHypPol`, que utilitza l'expressió aproximada dels angles en funció de π.

Presentem també algunes instruccions referents a les homografies de coeficients reals, amb la finalitat de facilitar a l'usuari l'ús del paquet, sabent un mínim de *Maple V*. Així, a partir de les quatre entrades d'una matriu, o bé directament de la matriu, les comandes `Hom` i `HomM` defineixen l'homografia com una funció de *Maple V*. Per a calcular els punts fixos tenim `fixPHom` i `fixPHomM`, que varien en el format dels arguments d'entrada. Amb `multHom` obtenim el multiplicador relacionat amb la interpretació geomètrica. Les instruccions `bfHom` i `bfHomM` ens donen la forma quadràtica binària associada. La funció lògica `typeHom`, amb els arguments `elliptic`, `parabolic` i `hyperbolic`, classifica l'homografia. Destaquem també la comanda `cirInv`, per a definir la inversió respecte d'un cercle donat, com una funció de *Maple V*.

Donat un ordre d'Eichler $\mathcal{O}(D,N)$, a través d'una $\mathbb{Z}$-base, la instrucció `embOr` dóna l'expressió genèrica d'una matriu del grup d'homografies quaterniòniques $\Gamma(D,N)$, en funció de $x,y,z,t \in \mathbb{Z}$, a la qual s'ha d'imposar la condició que el determinant sigui 1.

Per al càlcul de les constants associades a la corba de Shimura $X(D,N)$ tenim les instruccions següents, que tenen com a arguments els paràmetres D i N:

`VolhX`, `VolX`, per al càlcul del volum hiperbòlic i el volum normalitzat; `e2X`, `e3X` i `einfX` per als nombres de cicles el·líptics i parabòlics; `genusX` per al gènere i `neX` per al nombre de vèrtexs d'un domini fonamental de $X(D,N)$ que tingui tots els vèrtexs el·líptics, si aquest existeix. Hem implementat també, com a instrucció accessòria, la funció d'Euler, `Euler`.

A continuació presentem un recull de taules amb dades numèriques sobre corbes de Shimura. La taula 2.1 mostra les constants per a les corbes de Shimura poc ramificades de $D < 200$ i $N = 1$; cf. [Vig80], per als primers casos. Les taules 2.2 – 2.5 contenen les constants associades a les corbes de Shimura $X(6,N)$, $X(10,N)$, $X(14,N)$ i $X(15,N)$, corresponents a les àlgebres poc ramificades de tipus A i poc ramificades de tipus B destacades en el capítol anterior, fins a cert valor de N. Les constants corresponents a les corbes de Shimura de discriminant producte de quatre primers es poden trobar a la taula 2.6, per a $D < 1000$ i $N = 1$.

Les taules que hi ha a continuació recopilen alguns resultats coneguts de corbes de Shimura. La taula 2.7 mostra les equacions de corbes de Shimura conegudes a partir dels treballs de Kurihara [Kur79], Jordan-Livnè [Jor81] i Michon [Mic81a]. La taula 2.8 llista tots els valors $D > 1$ i N tals que $X(D,N)$ és una corba de Shimura hiperel·líptica; en aquests casos s'indica també la involució hiperel·líptica w (cf. [Ogg83]).

Taula 2.1 *Constants associades a les corbes de Shimura* $X(D,1)$, *on* $D < 200$, *corresponents al cas poc ramificat.*

D	V	e_2	e_3	g
6	0.333333	2	2	0
10	0.666667	0	4	0
14	1	2	0	1
15	1.33333	0	2	1
21	2	4	0	1
22	1.66667	2	4	0
26	2	0	0	2
33	3.33333	4	2	1
34	2.66667	0	4	1
35	4	0	0	3
38	3	2	0	2
39	4	0	0	3
46	3.66667	2	4	1
51	5.33333	0	2	3
55	6.66667	0	4	3
57	6	4	0	3
58	4.66667	0	4	2
62	5	2	0	3
65	8	0	0	5
69	7.33333	4	2	3
74	6	0	0	4
77	10	4	0	5
82	6.66667	0	4	3
85	10.6667	0	4	5
86	7	2	0	4
87	9.33333	0	2	5
91	12	0	0	7
93	10	4	0	5

D	V	e_2	e_3	g
94	7.66667	2	4	3
95	12	0	0	7
106	8.66667	0	4	4
111	12	0	0	7
115	14.6667	0	4	7
118	9.66667	2	4	4
119	16	0	0	9
122	10	0	0	6
123	13.3333	0	2	7
129	14	4	0	7
133	18	4	0	9
134	11	2	0	6
141	15.3333	4	2	7
142	11.6667	2	4	5
143	20	0	0	11
145	18.6667	0	4	9
146	12	0	0	7
155	20	0	0	11
158	13	2	0	7
159	17.3333	0	2	9
161	22	4	0	11
166	13.6667	2	4	6
177	19.3333	4	2	9
178	14.6667	0	4	7
183	20	0	0	11
185	24	0	0	13
187	26.6667	0	4	13
194	16	0	0	9

Taula 2.2 *Constants associades a les corbes de Shimura $X(6,N)$, on $N \leq 200$, que corresponen al cas poc ramificat de tipus A.*

N	V	e_2	e_3	g
1	0.3333	2	2	0
5	2.	4	0	1
7	2.6667	0	4	1
11	4.	0	0	3
13	4.6667	4	4	1
17	6.	4	0	3
19	6.6667	0	4	3
23	8.	0	0	5
25	10.	4	0	5
29	10.	4	0	5
31	10.667	0	4	5
35	16.	0	0	9
37	12.667	4	4	5
41	14.	4	0	7
43	14.667	0	4	7
47	16.	0	0	9
49	18.667	0	4	9
53	18.	4	0	9
55	24.	0	0	13
59	20.	0	0	11
61	20.667	4	4	9
65	28.	8	0	13
67	22.667	0	4	11
71	24.	0	0	13
73	24.667	4	4	11
77	32.	0	0	17
79	26.667	0	4	13
83	28.	0	0	15
85	36.	8	0	17
89	30.	4	0	15
91	37.333	0	8	17
95	40.	0	0	21
97	32.667	4	4	15
101	34.	4	0	17

N	V	e_2	e_3	g
103	34.667	0	4	17
107	36.	0	0	19
109	36.667	4	4	17
113	38.	4	0	19
115	48.	0	0	25
119	48.	0	0	25
121	44.	0	0	23
125	50.	4	0	25
127	42.667	0	4	21
131	44.	0	0	23
133	53.333	0	8	25
137	46.	4	0	23
139	46.667	0	4	23
143	56.	0	0	29
145	60.	8	0	29
149	50.	4	0	25
151	50.667	0	4	25
155	64.	0	0	33
157	52.667	4	4	25
161	64.	0	0	33
163	54.667	0	4	27
167	56.	0	0	29
169	60.667	4	4	29
173	58.	4	0	29
175	80.	0	0	41
179	60.	0	0	31
181	60.667	4	4	29
185	76.	8	0	37
187	72.	0	0	37
191	64.	0	0	33
193	64.667	4	4	31
197	66.	4	0	33
199	66.667	0	4	33

Taula 2.3 *Constants associades a les corbes de Shimura* $X(10,N)$, *on* $N \leq 165$, *que corresponen al cas poc ramificat de tipus B.*

N	V	e_2	e_3	g
1	.66667	0	4	0
3	2.6667	0	4	1
7	5.3333	0	8	1
9	8.	0	0	5
11	8.	0	0	5
13	9.3333	0	8	3
17	12.	0	0	7
19	13.333	0	8	5
21	21.333	0	8	9
23	16.	0	0	9
27	24.	0	0	13
29	20.	0	0	11
31	21.333	0	8	9
33	32.	0	0	17
37	25.333	0	8	11
39	37.333	0	8	17
41	28.	0	0	15
43	29.333	0	8	13
47	32.	0	0	17
49	37.333	0	8	17
51	48.	0	0	25
53	36.	0	0	19
57	53.333	0	8	25
59	40.	0	0	21
61	41.333	0	8	19
63	64.	0	0	33
67	45.333	0	8	21
69	64.	0	0	33
71	48.	0	0	25
73	49.333	0	8	23
77	64.	0	0	33
79	53.333	0	8	25
81	72.	0	0	37

N	V	e_2	e_3	g
83	56.	0	0	29
87	80.	0	0	41
89	60.	0	0	31
91	74.667	0	16	33
93	85.333	0	8	41
97	65.333	0	8	31
99	96.	0	0	49
101	68.	0	0	35
103	69.333	0	8	33
107	72.	0	0	37
109	73.333	0	8	35
111	101.33	0	8	49
113	76.	0	0	39
117	112.	0	0	57
119	96.	0	0	49
121	88.	0	0	45
123	112.	0	0	57
127	85.333	0	8	41
129	117.33	0	8	57
131	88.	0	0	45
133	106.67	0	16	49
137	92.	0	0	47
139	93.333	0	8	45
141	128.	0	0	65
143	112.	0	0	57
147	149.33	0	8	73
149	100.	0	0	51
151	101.33	0	8	49
153	144.	0	0	73
157	105.33	0	8	51
159	144.	0	0	73
161	128.	0	0	65
163	109.33	0	8	53

Taula 2.4 *Constants associades a les corbes de Shimura* $X(14,N)$*, on* $N \leq 160$*, que corresponen al cas poc ramificat de tipus A.*

N	V	e_2	e_3	g
1	1.	2	0	1
3	4.	0	0	3
5	6.	4	0	3
9	12.	0	0	7
11	12.	0	0	7
13	14.	4	0	7
15	24.	0	0	13
17	18.	4	0	9
19	20.	0	0	11
23	24.	0	0	13
25	30.	4	0	15
27	36.	0	0	19
29	30.	4	0	15
31	32.	0	0	17
33	48.	0	0	25
37	38.	4	0	19
39	56.	0	0	29
41	42.	4	0	21
43	44.	0	0	23
45	72.	0	0	37
47	48.	0	0	25
51	72.	0	0	37
53	54.	4	0	27
55	72.	0	0	37
57	80.	0	0	41
59	60.	0	0	31
61	62.	4	0	31
65	84.	8	0	41
67	68.	0	0	35
69	96.	0	0	49
71	72.	0	0	37
73	74.	4	0	37
75	120.	0	0	61
79	80.	0	0	41
81	108.	0	0	55

N	V	e_2	e_3	g
83	84.	0	0	43
85	108.	8	0	53
87	120.	0	0	61
89	90.	4	0	45
93	128.	0	0	65
95	120.	0	0	61
97	98.	4	0	49
99	144.	0	0	73
101	102.	4	0	51
103	104.	0	0	53
107	108.	0	0	55
109	110.	4	0	55
111	152.	0	0	77
113	114.	4	0	57
115	144.	0	0	73
117	168.	0	0	85
121	132.	0	0	67
123	168.	0	0	85
125	150.	4	0	75
127	128.	0	0	65
129	176.	0	0	89
131	132.	0	0	67
135	216.	0	0	109
137	138.	4	0	69
139	140.	0	0	71
141	192.	0	0	97
143	168.	0	0	85
145	180.	8	0	89
149	150.	4	0	75
151	152.	0	0	77
153	216.	0	0	109
155	192.	0	0	97
157	158.	4	0	79
159	216.	0	0	109

Taula 2.5 *Constants associades a les corbes de Shimura* $X(15,N)$, *on* $N \leq 125$, *que corresponen al cas poc ramificat de tipus B.*

N	V	e_2	e_3	g
1	1.3333	0	2	1
2	4.	0	0	3
4	8.	0	0	5
7	10.667	0	4	5
8	16.	0	0	9
11	16.	0	0	9
13	18.667	0	4	9
14	32.	0	0	17
16	32.	0	0	17
17	24.	0	0	13
19	26.667	0	4	13
22	48.	0	0	25
23	32.	0	0	17
26	56.	0	0	29
28	64.	0	0	33
29	40.	0	0	21
31	42.667	0	4	21
32	64.	0	0	33
34	72.	0	0	37
37	50.667	0	4	25
38	80.	0	0	41
41	56.	0	0	29
43	58.667	0	4	29
44	96.	0	0	49
46	96.	0	0	49
47	64.	0	0	33
49	74.667	0	4	37
52	112.	0	0	57
53	72.	0	0	37
56	128.	0	0	65
58	120.	0	0	61
59	80.	0	0	41
61	82.667	0	4	41
62	128.	0	0	65

N	V	e_2	e_3	g
64	128.	0	0	65
67	90.667	0	4	45
68	144.	0	0	73
71	96.	0	0	49
73	98.667	0	4	49
74	152.	0	0	77
76	160.	0	0	81
77	128.	0	0	65
79	106.67	0	4	53
82	168.	0	0	85
83	112.	0	0	57
86	176.	0	0	89
88	192.	0	0	97
89	120.	0	0	61
91	149.33	0	8	73
92	192.	0	0	97
94	192.	0	0	97
97	130.67	0	4	65
98	224.	0	0	113
101	136.	0	0	69
103	138.67	0	4	69
104	224.	0	0	113
106	216.	0	0	109
107	144.	0	0	73
109	146.67	0	4	73
112	256.	0	0	129
113	152.	0	0	77
116	240.	0	0	121
118	240.	0	0	121
119	192.	0	0	97
121	176.	0	0	89
122	248.	0	0	125
124	256.	0	0	129

Taula 2.6 *Constants associades a les corbes de Shimura* $X(D,1)$, *on* $D = p_1p_2p_3p_4 < 1000$.

D	V	e_2	e_3	g
210	8.	0	0	5
330	13.333	0	8	5
390	16.	0	0	9
462	20.	8	0	9
510	21.333	0	8	9
546	24.	0	0	13
570	24.	0	0	13
690	29.333	0	8	13
714	32.	0	0	17
770	40.	0	0	21
798	36.	8	0	17
858	40.	0	0	21
870	37.333	0	8	17
910	48.	0	0	25
930	40.	0	0	21
966	44.	8	0	21

Taula 2.7 *Equacions de corbes de Shimura* $X(D,N)$, *on* $D > 1$, *segons* [Kur79], [Jor81], [Mic81a].

D	N	g	Equació de $X(D,N)$
6	1	0	$x^2+y^2+3=0$
10	1	0	$x^2+y^2+2=0$
22	1	0	$x^2+y^2+11=0$
14	1	1	$(x^2-13)^2+7^3+2y^2=0$
46	1	1	$(x^2-45)^2+23+2y^2=0$
15	1	1	$(x^2+243)(x^2+3)+3y^2=0$
21	1	1	$x^4-658x^2+7^6+7y^2=0$
33	1	1	$x^4+30x^2+3^8+3y^2=0$

Taula 2.8 *Totes les corbes de Shimura $X(D,N)$ hiperel·líptiques, on $D>1$, segons* [Ogg83].

D	N	$g(D,N)$	w
26	1	2	w_{26}
35	1	3	w_{35}
38	1	2	w_{38}
39	1	3	w_{39}
51	1	3	w_{51}
55	1	3	w_{55}
57	1	3	w_{19}
58	1	2	w_{29}
62	1	3	w_{62}
69	1	3	w_{69}
74	1	4	w_{74}
82	1	3	w_{41}
86	1	4	w_{86}
87	1	5	w_{87}
93	1	5	w_{31}
94	1	3	w_{94}
95	1	7	w_{95}
111	1	7	w_{111}
119	1	9	w_{119}
134	1	6	w_{134}
146	1	7	w_{146}
159	1	9	w_{159}
194	1	9	w_{194}
206	1	9	w_{206}

D	N	$g(D,N)$	w
6	11	3	w_{66}
6	17	3	w_{34}
6	19	3	w_{114}
6	29	5	w_{174}
6	31	5	w_{186}
6	37	5	w_{222}
10	11	5	w_{110}
10	13	3	w_{65}
10	19	5	w_{38}
10	23	9	w_{230}
14	3	3	w_{14}
14	5	3	w_{14}
15	2	3	w_{15}
15	4	5	w_{15}
21	2	3	w_{7}
22	3	3	w_{66}
22	5	5	w_{110}
26	3	5	w_{26}
39	2	7	w_{39}

Capítol 3

Uniformització hiperbòlica de corbes de Shimura: cas no ramificat

Sigui $X(1,N)$, on N és un nombre primer, una corba de Shimura corresponent al cas no ramificat. Resultats coneguts permeten determinar-ne dominis fonamentals (cf., per exemple, [Apo76] i [BT92]). En aquest capítol construïm dominis fonamentals d'aquestes corbes de manera alternativa, mitjançant la teoria dels cercles d'isometria. Presentem una forma sistemàtica per a obtenir tant la seva representació gràfica com els invariants principals.

En primer lloc revisem la definició i les propietats dels cercles d'isometria i els mètodes que els relacionen amb els dominis fonamentals. En derivem alguns resultats generals. En la secció 2 apliquem els mètodes i resultats anteriors. Determinem un domini fonamental del subgrup que fixa l'infinit i llistem propietats que permeten reobtenir fàcilment propietats conegudes dels grups modulars $\Gamma(1,p)$. Donem resultats que caracteritzen els punts el·líptics, i indiquem els criteris per a l'aparellament d'arestes. Una part d'aquests resultats es troba a [Als99b] i [Als99a].

3.1 Cercles d'isometria

Les homografies són aplicacions conformes, que no sempre conserven les longituds i les àrees euclidianes. Per exemple, sigui Γ un subgrup discret de $\mathrm{SL}(2,\mathbb{R})$ i sigui $\gamma \in \Gamma$ una homografia que fixa l'infinit. Aleshores γ és o bé

una homotècia o bé una translació. En el primer cas, γ altera totes les longituds; en el segon cas, les deixa totes invariants. Notem que en l'expressió de γ en funció de a, b, c i d, fixar l'infinit és equivalent a $c = 0$. Si considerem les aplicacions que no fixen l'infinit, el resultat és ben diferent. Això ens permet definir els cercles d'isometria. En general, el concepte de cercle d'isometria és inherent a totes les homografies que no fixen l'infinit. Com a referències bàsiques destaquem [For51] i [Leh64].

3.1.1 Definició. Donada una homografia $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{C})$ (definida sobre $\mathbb{C} \cup \{\infty\}$), on $c \neq 0$, el cercle $C_\gamma := \{z \in \mathbb{C} : |cz + d| = 1\}$ s'anomena cercle d'isometria de l'homografia γ. □

3.1.2 Notació. Donat un cercle C, escriurem $C = C(o, r)$ per a denotar que es tracta del cercle de centre o i radi r. Per a cada cercle d'isometria C_γ, denotem per r_γ i o_γ el radi i el centre, i designem per $\mathrm{int}(C_\gamma)$ i $\mathrm{ext}(C_\gamma)$ les regions interior i exterior, delimitades pel cercle. Donat un conjunt G (no necessàriament amb estructura de grup) d'homografies del pla complex que no fixin l'infinit, posem $\mathcal{C}_G = \{C_\gamma : \gamma \in G\}$. □

3.1.3 Remarca. Donada una homografia $\gamma \in \mathrm{SL}(2,\mathbb{C})$, notem que $\dfrac{d\gamma}{dz} = \dfrac{1}{(cz+d)^2}$. Així, $z \in C_\gamma$ si, i només si, $|d\gamma| = |dz|$. Per tant, el cercle C_γ és el lloc geomètric dels punts a l'entorn dels quals les longituds i les àrees euclidianes no són alterades en magnitud en aplicar l'homografia γ. De la mateixa manera, $z \in \mathrm{int}(C_\gamma)$ si, i només si, $|d\gamma| > |dz|$. Per tant, en aplicar γ als punts interiors al cercle C_γ, les magnituds augmenten; als punts exteriors, les magnituds disminueixen. □

3.1.4 Lema. *Sigui* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$, *on* $c \neq 0$. *Aleshores, tenim les propietats següents:*

(i) *Els radis i els centres de* C_γ *i* $C_{\gamma^{-1}}$ *són els nombres reals* $o_\gamma = -d/c$, $r_\gamma = 1/|c|$, $o_{\gamma^{-1}} = a/c$ *i* $r_{\gamma^{-1}} = r_\gamma = 1/|c|$.

(ii) *La distància entre* o_γ *i* $o_{\gamma^{-1}}$ *és* $\left|\dfrac{a+d}{c}\right|$; *a més,* $r_\gamma + r_{\gamma^{-1}} = \dfrac{2}{|c|}$.

(iii) *Sigui* $\sigma \in \Gamma$ *tal que ni* σ *ni* $\gamma\sigma$ *fixin l'infinit. Aleshores, tenim que*

$$r_{\gamma\sigma} = \frac{r_\gamma \cdot r_\sigma}{|o_{\sigma^{-1}} - o_\gamma|} \quad i \quad |o_{\gamma\sigma} - o_\gamma| = \frac{r_\sigma^2}{|o_{\sigma^{-1}} - o_\gamma|}.$$

(iv) *Tenim que* $\gamma(C_\gamma) = C_{\gamma^{-1}}$, $\gamma(\text{ext}(C_\gamma)) = \text{int}(C_{\gamma^{-1}})$ *i* $\gamma(o_\gamma) = \infty$. *Es dedueix que* $\gamma(\text{int}(C_\gamma)) = \text{ext}(C_{\gamma^{-1}})$ *i* $\gamma(\infty) = o(\gamma^{-1})$.

DEMOSTRACIÓ: Les propietats (i) i (ii) són immediates a partir de la definició de cercle d'isometria. La demostració de (iii) es pot trobar a [For51] i la de (iv) a [Leh64]. □

3.1.5 Definició. Fixat un conjunt $G \subseteq \text{SL}(2,\mathbb{R})$, diem que un cercle d'isometria $C \in \mathcal{C}_G$ és maximal respecte de G si no existeix cap cercle d'isometria $C' \in \mathcal{C}_G$, $C' \neq C$ tal que $C \subseteq (\text{int}(C') \cup C')$. □

Denotem $\mathcal{C}_G^{\max} = \{C_\gamma : C_\gamma \text{ maximal respecte de } G, \gamma \in G\}$. És clar que per a qualsevol conjunt G d'homografies, $\bigcap_{C \in \mathcal{C}_G} \text{ext}(C) = \bigcap_{C \in \mathcal{C}_G^{\max}} \text{ext}(C)$.

3.1.6 Definició. Sigui Γ un subgrup discret de $\text{SL}(2,\mathbb{R})$. Es diu que un punt de $\mathcal{H}$ és un punt límit respecte de Γ si és un punt d'acumulació del conjunt $\{o_\gamma : \gamma \in \Gamma\}$. La resta de punts de $\mathcal{H}$ s'anomenen punts ordinaris respecte de Γ. □

3.1.7 Lema. *Sigui* Γ *un subgrup discret de* $\text{SL}(2,\mathbb{R})$.

(i) *El conjunt de punts límit respecte de* Γ *és tancat per l'acció de* Γ.

(ii) *Tots els punts límit són a* $\mathbb{R}$. □

3.1.8 Proposició. *Per a tota homografia* $\gamma \in \text{SL}(2,\mathbb{R})$ *existeix una recta* L_γ *d'equació* $x = t$, *per a cert* $t \in \mathbb{R}$, *tal que:*

(i) γ *és igual a la inversió del cercle* C_γ *seguida de la reflexió respecte de la recta* L_γ.

(ii) *Un cercle és invariant per* γ *si, i només si, és ortogonal a* C_γ *i té el centre a* L_γ. □

3.1.9 Remarca. Si ens restringim al semiplà de Poincaré, amb l'estructura donada per la geometria hiperbòlica, la propietat (i) del lema 3.1.4 ens assegura que els cercles d'isometria són rectes hiperbòliques de $\mathcal{H}$. Així, les inversions respecte d'aquests cercles són simetries hiperbòliques. Això ens permet reformular la propietat (i) de la proposició anterior, dient que l'homografia γ és la composició de dues simetries hiperbòliques respecte del cercle d'isometria associat C_γ i la recta L_γ. En les proposicions següents veurem com queda determinada la recta L_γ. □

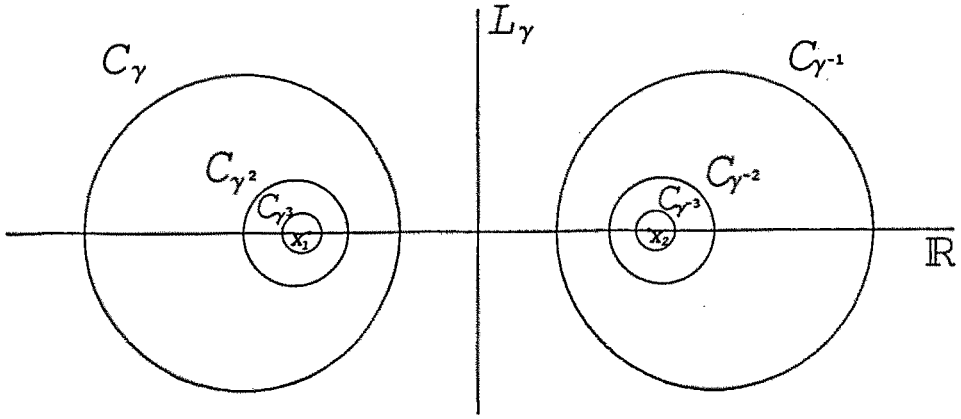

Figura 3.1: Cercles d'isometria associats a una homografia hiperbòlica $\gamma \in \mathrm{SL}(2,\mathbb{R})$.

Aplicant les propietats dels cercles d'isometria, recopilades en el lema 3.1.4, i la interpretació geomètrica de les homografies a l'entorn dels punts fixos, donada a la secció 2.2, s'obtenen noves propietats que caracteritzen les homografies segons siguin hiperbòliques, el·líptiques o parabòliques.

3.1.10 Proposició. *Sigui $\gamma \in \mathrm{SL}(2,\mathbb{R})$ una homografia hiperbòlica de punts fixos x_1, $x_2 \in \mathbb{R}$. Aleshores:*

(i) $C_\gamma \cap C_{\gamma^{-1}} = \emptyset$.

(ii) $C_{\gamma^n} \subset \mathrm{int}(C_{\gamma^{n-1}})$, *per a* $n > 0$. *A més,* $\lim_{n\to\infty} r_{\gamma^n} = 0$. *Per tant,* C_γ *és maximal respecte de* $\{\gamma^n : n > 0\}$ *i* $\mathcal{C}^{\max}_{<\gamma>} = \{C_\gamma, C_{\gamma^{-1}}\}$.

(iii) $\bigcap_{n>0} \mathrm{int}\, C_{\gamma^n} = x_1$, $\bigcap_{n>0} \mathrm{int}\, C_{\gamma^{-n}} = x_2$; x_1 *i* x_2 *són punts límit.*

(iv) L_γ *és el bisector del segment que uneix els centres de* C_γ *i* $C_{\gamma^{-1}}$. □

En la figura 3.1, il·lustrem la posició relativa dels cercles d'isometria corresponents a una homografia hiperbòlica $\gamma \in \mathrm{SL}(2,\mathbb{R})$, γ^{-1}, γ^2, γ^{-2}, γ^3 i γ^{-3}, així com la recta L_γ i els punts fixos x_1 i x_2.

3.1.11 Proposició. *Sigui $\gamma \in \mathrm{SL}(2,\mathbb{R})$ una homografia el·líptica d'ordre k de punts fixos z i $\overline{z}$. Aleshores,*

(i) $\{z, \overline{z}\} \subseteq \bigcap_{n\in\mathbb{Z}} C_{\gamma^n}$.

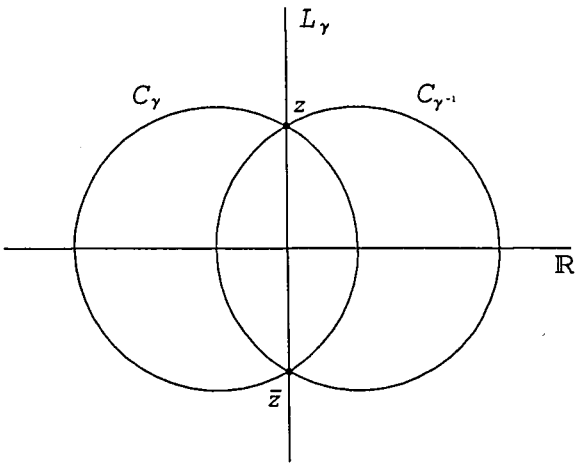

Figura 3.2: Cercles d'isometria associats a una homografia el·líptica $\gamma \in \mathrm{SL}(2,\mathbb{R})$ d'ordre $k > 2$.

(ii) *Si* $k = 2$, $C_{\gamma^{-1}} = C_\gamma$. *Si* $k > 2$, $C_\gamma \cap C_{\gamma^{-1}} = \{z, \overline{z}\}$.

(iii) *L'angle determinat per* C_γ *i* $C_{\gamma^{-1}}$ *en el punt* z *és* $\theta = 2\pi/k$.

(iv) L_γ *és la recta determinada per* z *i* $\overline{z}$. *Si* $k = 2$, L_γ *és un diàmetre; per a* $k > 2$, L_γ *és el bisector del segment que uneix els centres de* C_γ *i* $C_{\gamma^{-1}}$. □

En la figura 3.2, il·lustrem la posició relativa dels cercles d'isometria corresponents a una homografia el·líptica $\gamma \in \mathrm{SL}(2,\mathbb{R})$ d'ordre $k > 2$ i a γ^{-1}, així com la recta L_γ i els punts fixos z i $\overline{z}$.

3.1.12 Proposició. *Sigui* $\gamma \in \mathrm{SL}(2,\mathbb{R})$ *una homografia parabòlica de punt fix* $x \in \mathbb{R}$. *Aleshores,*

(i) $\bigcap_{n\in\mathbb{Z}} C_{\gamma^n} = \{x\}$.

(ii) *Per a* $n > 0$, $C_{\gamma^n} \subseteq \mathrm{int}(C_{\gamma^{n-1}})$. *Per tant,* C_γ *és maximal respecte de* $\{\gamma^n : n > 0\}$ *i* $\mathcal{C}^{\max}_{<\gamma>} = \{C_\gamma, C_{\gamma^{-1}}\}$.

(iii) $r_{\gamma^n} = \dfrac{1}{|nc|} \to 0$ *quan* $n \to \infty$; $o_{\gamma^n} = x - \dfrac{1}{nc} \in \mathbb{R}$, *i* x *és un punt límit.*

(iv) *La recta* L_γ *és la tangent comuna als cercles* C_{γ^n} *en el punt* x *per a tot* $n \neq 0$; L_γ *coincideix amb el bisector del segment que uneix els centres de* C_γ *i* $C_{\gamma^{-1}}$. □

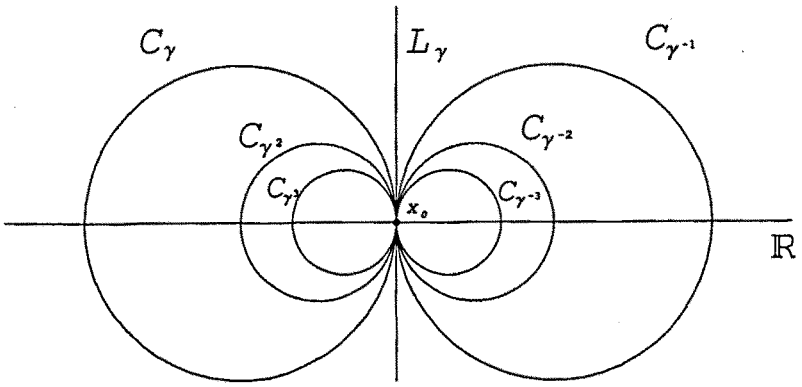

Figura 3.3: Cercles d'isometria associats a una homografia parabòlica $\gamma \in \mathrm{SL}(2,\mathbb{R})$.

En la figura 3.3, il·lustrem la posició relativa dels cercles d'isometria corresponents a una homografia parabòlica $\gamma \in \mathrm{SL}(2,\mathbb{R})$, γ^{-1}, γ^2, γ^{-2}, γ^3 i γ^{-3}, així com la recta L_γ i el punt fix x.

De les tres proposicions anteriors deduïm el corol·lari següent.

3.1.13 Corol·lari. *Sigui $\gamma \in \mathrm{SL}(2,\mathbb{R})$, que no fixa l'infinit. Aleshores,*

(i) *γ és hiperbòlica si, i només si, $C_\gamma \cap C_{\gamma^{-1}} = \emptyset$.*

(ii) *γ és el·líptica si, i només si, $C_\gamma \cap C_{\gamma^{-1}} \cap \mathcal{H} \neq \emptyset$.*

(iii) *γ és parabòlica si, i només si, $C_\gamma \cap C_{\gamma^{-1}} \in \mathbb{R}$.* □

Per a alguns dels resultats següents, caldrà que l'infinit sigui un punt estàndard respecte del grup Γ. Aquesta condició implica que els elements de Γ diferents de la identitat no fixen l'infinit, per la qual cosa tenen un cercle d'isometria associat.

3.1.14 Proposició. *Sigui $\Gamma \subseteq \mathrm{SL}(2,\mathbb{C})$ un grup d'homografies que actua de forma pròpia i discontínua, respecte del qual l'infinit és un punt estàndard. Aleshores tenim les propietats següents:*

i) Els centres dels cercles d'isometria estan a una distància acotada de l'origen.

(i) *Per a cada nombre real $r \in \mathbb{R}$ hi ha un nombre finit de cercles d'isometria amb radi més gran que r. Així, el conjunt de radis dels cercles d'isometria està acotat.*

(ii) *El conjunt* $\bigcup_{\gamma\in\Gamma} \mathrm{int}(C_\gamma)$ *és un subconjunt acotat del pla complex.*

(iii) *Homografies diferents tenen cercles d'isometria diferents.* □

3.1.15 Proposició. *Sigui* Γ *un grup amb tots els cercles d'isometria definits, tal que hi ha un entorn de l'infinit que no conté cap centre dels cercles d'isometria* C_γ*, per a tot* $\gamma \in \Gamma$*. Aleshores,*

$$\mathcal{D}_{st}(\Gamma) = \overline{\mathcal{H} \cap (\bigcap_{\gamma\in\Gamma} \mathrm{ext}\, C_\gamma)}$$

és un domini fonamental de Γ*. Aquest domini s'anomena domini fonamental estàndard de* Γ*.* □

És fàcil veure que dos punts de $\mathcal{D}_{st}(\Gamma)$ no són Γ−equivalents. Suposem $\gamma(z_1) = z_2$, on $z_1 \in \mathcal{D}_{st}(\Gamma)$, $\gamma \in \Gamma$. En particular, z_1 és exterior al cercle d'isometria C_γ. Aplicant el lema 3.1.4(iv), es té $z_2 \in \mathrm{int}(C_{\gamma^{-1}})$; per tant, $z_2 \notin \mathcal{D}_{st}(\Gamma)$. La demostració que els transformats de $\mathcal{D}_{st}(\Gamma)$ recobreixen $\mathcal{H}$, utilitzant que l'infinit és un punt estàndard, es pot trobar a [For51] o a [Leh64].

3.1.16 Definicions. Els vèrtexs del domini fonamental $\mathcal{D}_{st}(\Gamma)$ són els punts de la vora del domini que són intersecció de dos o més cercles d'isometria diferents (que corresponen als vèrtexs com a polígon hiperbòlic) o bé que són el·líptics d'ordre 2. Els vèrtexs que no són punts el·líptics ni parabòlics s'anomenen vèrtexs accidentals. Per analogia amb la definició de cicle el·líptic i parabòlic, un cicle accidental és una òrbita de vèrtexs accidentals; convenim que és d'ordre $k = 1$. El nombre de cicles accidentals pot dependre del domini fonamental considerat. Anomenem arestes de $\mathcal{D}_{st}(\Gamma)$ els arcs dels cercles d'isometria continguts en la vora del domini i delimitats per dos vèrtexs. □

Observem que els punts el·líptics i els parabòlics no poden ser a l'interior del domini fonamental estàndard, per 3.1.11 i 3.1.12. De fet, sempre podem suposar que els punts el·líptics i els parabòlics són vèrtexs del domini fonamental, encara que no tots els vèrtexs són punts el·líptics o parabòlics. Notem també que un vèrtex sempre té dues arestes adjacents. Com que les homografies transformen cercles d'isometria en cercles d'isometria, transformen també vèrtexs en vèrtexs.

3.1.17 Proposició. *Sigui* Γ *un subgrup discret de* $\mathrm{SL}(2,\mathbb{R})$*, respecte del qual l'infinit és un punt estàndard, i sigui* $\mathcal{D}_{st}(\Gamma)$ *el seu domini fonamental estàndard.*

(i) *Les arestes del domini fonamental* $\mathcal{D}_{st}(\Gamma)$ *són equivalents dos a dos per l'acció de* Γ*. És a dir, existeixen* $\gamma_j \in \Gamma$ *tals que les arestes es disposen en parells disjunts de la forma* $\{l_j, \gamma_j(l_j)\}$*.*

(ii) *Les arestes que són equivalents tenen la mateixa longitud hiperbòlica.*

(iii) *El conjunt d'homografies* $\gamma_j \in \Gamma$ *que identifiquen les parelles d'arestes formen un sistema de generadors del grup* Γ*.*

(iv) *Cada cicle d'ordre finit determina una relació entre els generadors. Sigui* $\{w_1, \ldots, w_m\}$ *un cicle d'ordre* $k \in \mathbb{N}$*. Considerem les homografies* $\gamma_j \in \Gamma$*,* $j = 1, \ldots, m$*, tals que* $\gamma_j(w_j) = w_{j+1}$ *per* $j = 1, \ldots, m-1$ *i* $\gamma_m(w_m) = w_1$*. Aleshores,* $(\gamma_m \gamma_{m-1} \ldots \gamma_1)^k = \pm \mathrm{Id}$*.*

(v) *El conjunt de generadors de* (iii)*, junt amb les relacions de* (iv)*, formen una presentació del grup* Γ*.*

(vi) *La suma dels angles en els vèrtexs d'un cicle no parabòlic és* $2\pi/k$*, on* k *és l'ordre del cicle. La suma dels angles en els vèrtexs d'un cicle parabòlic és* 0*.* □

3.1.18 Proposició. *Sigui* Γ *un grup que actua de forma pròpia i discontínua en* $\mathcal{H}$*. Aleshores, existeix un domini fonamental de* Γ *que satisfà les mateixes propietats de* 3.1.17*.*

DEMOSTRACIÓ: Si l'infinit és un punt estàndard respecte de Γ, considerem el domini fonamental estàndard $\mathcal{D}_{st}(\Gamma)$.

Suposem que l'infinit no és un punt estàndard respecte de Γ. Com que Γ actua de forma pròpia i discontínua en el pla complex, existeix almenys un punt estàndard z. Si considerem una homografia $\sigma \in \mathrm{SL}(2,\mathbb{C})$ tal que $\sigma(z) = \infty$, obtenim un transformat del grup Γ, $\sigma\Gamma\sigma^{-1}$, que actua sobre $\sigma\mathcal{H}$ i respecte del qual l'infinit és un punt estàndard. En aquest cas, es demostra que els resultats enunciats per a $\Gamma \in \mathrm{SL}(2,\mathbb{R})$ i $\mathcal{H}$, formulats d'acord amb la nova situació, també són vàlids i s'obté un domini fonamental estàndard amb les propietats de 3.1.17, $\mathcal{D}_{st}(\sigma\Gamma\sigma^{-1})$. Finalment, $\sigma^{-1}(\mathcal{D}_{st}(\sigma\Gamma\sigma^{-1}))$ és un domini fonamental de Γ que satisfà les propietats de 3.1.17. □

A continuació descrivim l'adaptació del mètode anterior, [For51], per a trobar un domini fonamental per a un grup Γ que actuï de forma pròpia i discontínua, i que tingui elements que fixin l'infinit, la qual, sovint, evita utilitzar transformats del grup i del semiplà de Poincaré.

Denotem per Γ_∞ el subgrup de Γ format pels elements de Γ que fixen l'infinit. La proposició anterior ens assegura l'existència d'un domini fonamental de Γ_∞, amb les propietats enunciades en 3.1.17. Sovint hi ha altres formes més directes de trobar un domini per al grup Γ_∞ amb aquestes propietats.

Denotem per Γ' la resta d'elements del grup, $\Gamma' = \Gamma - \Gamma_\infty$. Tots els elements del conjunt Γ' tenen cercles d'isometria, però Γ' no és un grup i no hi podem aplicar els resultats anteriors. Per exemple, pot ser que el conjunt de radis dels cercles d'isometria no estigui acotat, o que els centres dels cercles d'isometria no estiguin en una regió acotada, o que els cercles d'isometria d'homografies diferents siguin iguals (cf. seccions 3.2 i 8.2). Estudiant la interrelació entre Γ_∞ i Γ' es prova que les transformacions de Γ_∞ porten cercles d'isometria a cercles d'isometria, veient que $\gamma(C_\sigma) = C_{\gamma\sigma\gamma^{-1}}$, i es té el següent resultat (cf. [For51]).

3.1.19 Teorema. *Sigui Γ un grup d'homografies que actua de forma pròpia i discontínua. Sigui $\mathcal{D}(\Gamma_\infty)$ un domini fonamental de Γ_∞ que satisfà les propietats de* 3.1.17. *Si el conjunt*

$$\mathcal{D}(\Gamma) = \mathcal{D}(\Gamma_\infty) \cap \overline{(\bigcap_{\gamma\in\Gamma'} \operatorname{ext} C_\gamma)}$$

és diferent del buit, aleshores és un domini fonamental del grup Γ i satisfà les propietats enunciades en 3.1.17. □

3.1.20 Corol·lari. *Amb les hipòtesis i la notació del teorema anterior,*

$$\mathcal{D}(\Gamma) = \mathcal{D}(\Gamma_\infty) \cap \overline{(\bigcap_{C\in\mathcal{C}_{\Gamma'}^{\max}} \operatorname{ext}(C))}. \square$$

Notem que, a causa de la intersecció de la frontera de $\mathcal{D}(\Gamma_\infty)$ amb els cercles d'isometria de $\mathcal{C}_{\Gamma'}^{\max}$, hem de modificar lleugerament els conceptes de vèrtex i aresta definits per al domini fonamental estàndard (cf. 3.1.16).

3.1.21 Definició. El conjunt de vèrtexs del domini fonamental $\mathcal{D}(\Gamma)$ està format pels punts de la vora que satisfan una de les condicions següents: són vèrtexs de $\mathcal{D}(\Gamma_\infty)$; són intersecció de dos o més cercles d'isometria diferents;

són punts el·líptics d'ordre 2; són intersecció d'una aresta de $\mathcal{D}(\Gamma_\infty)$ amb un o més cercles d'isometria de Γ'. Els vèrtexs que no són punts el·líptics ni parabòlics s'anomenen vèrtexs accidentals. Les arestes de $\mathcal{D}(\Gamma)$ són els segments de rectes hiperbòliques, continguts a la frontera, delimitats per vèrtexs. □

3.2 Construcció d'un domini fonamental per a $X(1,p)$

Sigui $p = 1$ o bé p un nombre primer. Considerem el grup quaterniònic

$$\Gamma(1,p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad-bc=1,\ c \equiv 0 \mod p \right\},$$

que actua de forma pròpia i discontínua en el semiplà de Poincaré. El cas $p = 1$ correspon a $\Gamma_0(1) = \mathrm{SL}(2,\mathbb{Z})$; $\Gamma(1,p) = \Gamma_0(p)$ és un subgrup de congruència de nivell p de $\mathrm{SL}(2,\mathbb{Z})$.

Descrivim una forma sistemàtica de construir un domini fonamental de $X(1,p)$, utilitzant els resultats de les seccions anteriors.

En primer lloc, considerem el subgrup de $\Gamma(1,p)$, format pels elements que fixen l'infinit. Es tracta del conjunt de les matrius de la forma anterior que satisfan les condicions $c = 0$ i $ad = 1$:

$$\Gamma(1,p)_\infty := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\} = \{T^b : b \in \mathbb{Z}\}, \quad \text{on } T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Geomètricament, T actua com una translació de longitud 1. Per tant, un domini fonamental per $\Gamma(1,p)_\infty$ és:

$$\mathcal{D}(\Gamma(1,p)_\infty) = \left\{ z \in \mathcal{H} \ :\ -\frac{1}{2} \le \mathrm{Re}(z) \le \frac{1}{2} \right\}.$$

D'altra banda, considerem la resta d'elements del grup $\Gamma(1,p)$, $\Gamma(1,p)' = \Gamma(1,p) - \Gamma(1,p)_\infty$. Per a cada element d'aquest conjunt tenim un cercle d'isometria associat. Vegem quines característiques tenen i quina regió de $\mathcal{H}$ delimiten.

Recordem que $C(o,r)$ denota el cercle de centre o i radi r.

3.2.1 Proposició. *Sigui p un nombre primer i considerem el conjunt $\Gamma(1,p)'$. Aleshores,*

(i) $\mathcal{C}_{\Gamma(1,p)'} = \{C(k/sp, 1/sp) : k \in \mathbb{Z}, s \in \mathbb{N}, \text{mcd}(k, ps) = 1\}$.

(ii) $\mathcal{C}^{\max}_{\Gamma(1,p)'} = \{C(k/p, 1/p) : k \in \mathbb{Z}, p \nmid k\}$.

DEMOSTRACIÓ: Sigui $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1,p)'$. Aleshores li correspon el cercle d'isometria $C_\gamma = C(k/sp, 1/sp)$, on $s = \dfrac{|c|}{p} \in \mathbb{N}$ i $k = -d\dfrac{c}{|c|} \in \mathbb{Z}$. Com que $ad - bc = 1$, se satisfà $d \neq 0$ i $\text{mcd}(k, sp) = \text{mcd}(d, c) = 1$. Recíprocament, sigui $C(k/sp, 1/sp)$ un cercle que satisfaci $k \in \mathbb{Z}$, $s \in \mathbb{N}$ i $\text{mcd}(k, sp) = 1$. Aplicant la identitat de Bézout, existeixen $a, b \in \mathbb{Z}$ tals que $-ak - bsp = 1$; aleshores, $\gamma = \begin{pmatrix} a & b \\ sp & -k \end{pmatrix} \in \Gamma(1,p)'$ i satisfà $C_\gamma = C(k/sp, 1/sp)$. Això demostra (i).

El radi més gran possible d'un cercle d'isometria és $1/p$. Per tant, els cercles $C(k/p, 1/p)$, on $k \in \mathbb{Z}$ i $\text{mcd}(k,p) = 1$, són maximals respecte de $\Gamma(1,p)'$. Resta veure que són els únics cercles d'isometria maximals. Sigui $C = C(k/sp, 1/sp) \in \mathcal{C}_{\Gamma(1,p)'}$, on $k \in \mathbb{Z}$, $s \in \mathbb{N}$, $\text{mcd}(k, sp) = 1$ i $s > 1$. Com que k no és múltiple de s, tenim que $\dfrac{1}{s} \leq \dfrac{k}{s} - \left[\dfrac{k}{s}\right] \leq \dfrac{s-1}{s}$. Per tant, utilitzant $\dfrac{[k/s]}{p} \leq \dfrac{k}{sp} \leq \dfrac{[k/s]+1}{p}$ es verifiquen les dues desigualtats següents:

$$\left(\frac{k}{sp} + \frac{1}{sp}\right) - \frac{[k/s]}{p} \leq \frac{1}{p} \quad \text{i} \quad \frac{[k/s]+1}{p} - \left(\frac{k}{sp} - \frac{1}{sp}\right) \leq \frac{1}{p}.$$

D'aquí es dedueix que el cercle $C = C(k/sp, 1/sp)$ està contingut en els cercles $C\left(\frac{[k/s]}{p}, 1/p\right)$ i $C\left(\frac{[k/s]+1}{p}, 1/p\right)$. Però $\left[\frac{k}{s}\right]$ i $\left[\frac{k}{s}\right] + 1$ no poden ser simultàniament múltiples de p; per tant, com a mínim un d'aquests cercles pertany a $\mathcal{C}_{\Gamma(1,p)'}$ (de fet pertany a $\mathcal{C}^{\max}_{\Gamma(1,p)'}$ ja que té radi $1/p$). Això demostra que C no és maximal i completa (ii). □

De forma anàloga, es demostren els resultats corresponents a $p = 1$.

3.2.2 Proposició. *Considerem el conjunt* $\Gamma(1,1)$. *Aleshores,*

(i) $\mathcal{C}_{\Gamma(1,1)'} = \{C(k/s, 1/s) : k \in \mathbb{Z}, s \in \mathbb{N}, \text{mcd}(k, s) = 1\}$.

(ii) $\mathcal{C}^{\max}_{\Gamma(1,1)'} = \{C(k, 1) : k \in \mathbb{Z}\}$. □

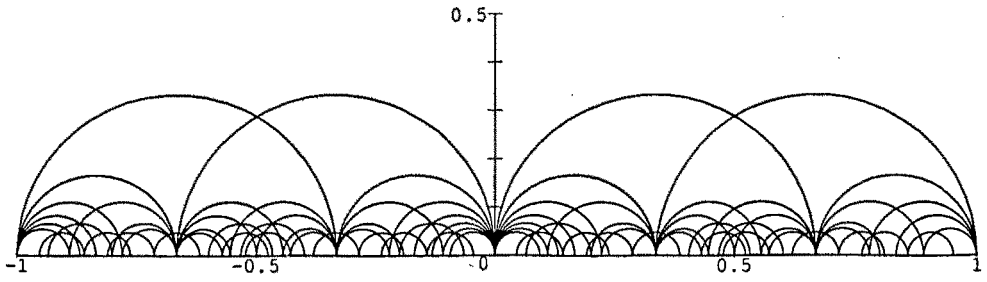

Figura 3.4: Cercles d'isometria de $\Gamma(1,3)'$.

3.2.3 Corol·lari. *Sigui p un nombre primer o $p = 1$. La intersecció d'un cercle d'isometria no maximal amb un cercle d'isometria maximal, si és diferent del buit, es troba sempre a $\mathbb{R}$. A més, la intersecció de tres cercles d'isometria maximals diferents sempre és buida.* □

Per a il·lustrar els resultats anteriors presentem la figura 3.4, que representa els cercles d'isometria de $\Gamma(1,3)'$ per a $s < 8$ i $\left|\frac{k}{3s}\right| < 1$.

Notem que no estem en les hipòtesis de la proposició 3.1.14. En particular, els radis són acotats, però la distància dels centres al 0 no està acotada i un cercle pot ser cercle d'isometria d'homografies diferents. En general, el radi i el centre del cercle d'isometria determinen els valors de c i d, excepte el signe; la condició que el determinant valgui 1 ens dóna, aleshores, una relació entre a i b que té diferents solucions.

3.2.4 Teorema. *Sigui p un nombre primer, $p > 2$. Aleshores,*

$$\mathcal{D}(\Gamma(1,p)) = \left\{ z \in \mathcal{H} \,:\, |\operatorname{Re}(z)| \leq 1/2, \left|z - \frac{k}{p}\right| > \frac{1}{p},\, k \in \mathbb{Z},\, 0 < |k| \leq \frac{p-1}{2} \right\}$$

és un domini fonamental de $\Gamma(1,p)$ en $\mathcal{H}$.

DEMOSTRACIÓ: Considerem el domini fonamental de $\Gamma(1,p)_\infty$ calculat al començament de la secció i apliquem el corol·lari 3.1.20, amb la qual cosa obtenim

$$\mathcal{D}(\Gamma(1,p)) = \{z \in \mathcal{H} \,:\, |\operatorname{Re}(z)| \leq 1/2\} \cap \overline{\left(\bigcap_{C \in C^{\max}_{\Gamma(1,p)'}} \operatorname{ext}(C)\right)}.$$

Completem la demostració utilitzant la descripció dels cercles d'isometria maximals donada en el teorema anterior. Els únics cercles d'isometria maxi-

mals que tenen intersecció significativa amb $\mathcal{D}(\Gamma(1,p)_\infty)$ són exactament els cercles $C(k/p,1/p)$, tals que $0<|k|\leq\frac{p-1}{2}$. □

3.2.5 Proposició. *Per als grups $\Gamma(1,1)$ i $\Gamma(1,2)$ tenim els dominis fonamentals*

$$\mathcal{D}(\Gamma(1,1))=\{z\in\mathcal{H}\,:\,|\mathrm{Re}(z)|\leq 1/2,|z|>1\},$$
$$\mathcal{D}(\Gamma(1,2))=\{z\in\mathcal{H}\,:\,|\mathrm{Re}(z)|\leq 1/2,|z|>1\}.$$

DEMOSTRACIÓ: De forma anàloga al teorema anterior, considerem el domini fonamental $\mathcal{D}(\Gamma(1,p)_\infty)$ i apliquem 3.1.20. Utilitzant la descripció dels cercles d'isometria maximals és fàcil veure que és suficient considerar el cercle d'isometria maximal $C(0,1)$ per al cas $p=1$ i els cercles $C(-1/2,1/2)$ i $C(-1/2,1/2)$ per al cas $p=2$. □

3.2.6 Notació. Denotem $\mathcal{J}(p)$ el subconjunt de cercles d'isometria maximals de $\Gamma(1,p)$ que determinen arestes del domini fonamental $\mathcal{D}(\Gamma(1,p))$. Pels resultats anteriors, si $p>2$ és un nombre primer, tenim que

$$\mathcal{J}(p)=\{C(k/p,1/p)\,:\,k\in\mathbb{Z},\,0<|k|\leq\frac{p-1}{2},\,\mathrm{mcd}(k,p)=1\}.$$

El cas $p=1$ dóna simplement $\mathcal{J}(1)=\{C(0,1)\}$. Per a $p=2$, tenim que $\mathcal{J}(2)=\{C(-1/2,1/2),\,C(-1/2,1/2)\}$. □

Vegem que aquest conjunt de cercles d'isometria maximals satisfà una propietat tècnica, important per a obtenir els principals resultats posteriors.

3.2.7 Lema. *Sigui p un nombre primer o $p=1$. Donat $C\in\mathcal{J}(p)$, existeix una única homografia $\gamma\in\Gamma(1,p)'$ tal que $C=C_\gamma$ i $C_{\gamma^{-1}}\in\mathcal{J}(p)$.*

DEMOSTRACIÓ: Sigui $C=C(k/p,1/p)\in\mathcal{J}(p)$. Determinarem de forma única una homografia $\gamma\in\Gamma(1,p)'$ tal que $C=C_\gamma\in\mathcal{J}(p)$ i $C_{\gamma^{-1}}\in\mathcal{J}(p)$. Qualsevol $\gamma=\begin{pmatrix}a & b\\ p & -k\end{pmatrix}$, amb $a,b\in\mathbb{Z}$ tals que $-ak-bp=1$, satisfà $\gamma\in\Gamma(1,p)'$ i $C=C_\gamma$. Hem d'escollir una solució $\{a,b\}$ de $-ak-bp=1$ tal que $C_{\gamma^{-1}}=C(a/p,1/p)$ pertanyi a $\mathcal{J}(p)$. Si $p>2$, considerem l'única solució amb $|a|\leq\frac{p-1}{2}$, $a\neq 0$. Si $p=1$, tenim que $k=0$ i considerem $a=0$ i $b=-1$; és clar que aleshores se satisfà $C_\gamma=C(0,1)=C_{\gamma^{-1}}$. Per a $p=2$, considerem $a=b=-1$ i els cercles d'isometria corresponents són $C_\gamma=C(-1/2,1/2)$ i $C_{\gamma^{-1}}=C(1/2,1/2)$. □

3.2.8 Notació. Considerem el domini fonamental $\mathcal{D}(\Gamma(1,p))$. Denotem per $n(1,p)$ el nombre total de vèrtexs. Denotem per $n_2(1,p)$, $n_3(1,p)$, $n_\infty(1,p)$ i $n_1(1,p)$ el nombre de vèrtexs el·líptics d'ordre 2, el·líptics d'ordre 3, parabòlics i accidentals, respectivament. Anàlogament, $e_2(1,p)$, $e_3(1,p)$, $e_\infty(1,p)$ i $e_1(1,p)$ denoten el nombre de cicles el·líptics d'ordre 2, el·líptics d'ordre 3, parabòlics i accidentals, respectivament. Denotem per $V_h(1,p)$ el volum hiperbòlic del polígon hiperbòlic $\mathcal{D}(\Gamma(1,p))$. □

3.2.9 Teorema. *Sigui p un nombre primer, $p > 2$. El domini fonamental $\mathcal{D}(\Gamma(1,p))$, té les propietats següents:*

(i) *Els punts* $z_j = \dfrac{2j-2-p}{2p} + \dfrac{\sqrt{3}}{2p}i$ *per a* $j = 1, \dots, \frac{p+1}{2} - 1$, $z_{\frac{p+1}{2}} = 0$, $z_j = \dfrac{2j-p}{2p} + \dfrac{\sqrt{3}}{2p}i$ *per a* $j = \frac{p+1}{2} + 1, \dots, p$ *i* $z_{p+1} = \infty$, *són vèrtexs de* $\mathcal{D}(\Gamma(1,p))$.

(ii) *L'angle interior a* $\mathcal{D}(\Gamma(1,p))$ *en els vèrtexs* $z_{\frac{p+1}{2}} = 0$ *i* $z_{p+1} = \infty$ *és 0; en els vèrtexs* z_1 *i* z_p, *és* $\pi/3$, *i en la resta de vèrtexs* z_j, *és* $2\pi/3$.

(iii) $\mathcal{D}(\Gamma(1,p))$ *és un polígon hiperbòlic d'un nombre parell de vèrtexs i arestes,* $n(1,p) = p + 1 + n_2(1,p)$.

(iv) *El volum hiperbòlic de* $\mathcal{D}(\Gamma(1,p))$ *és* $V_h(1,p) = (p+1)\dfrac{\pi}{3}$.

DEMOSTRACIÓ: Considerem els punts de $\mathcal{H}$ o $\mathbb{R}$ determinats per les interseccions dels cercles d'isometria maximals pertanyents a $\mathcal{J}(p)$, i les interseccions de les dues semirectes $\mathrm{Re}(z) = -1/2$ i $\mathrm{Re}(z) = 1/2$ amb aquests cercles. Tots aquests formen part del conjunt de vèrtexs del domini fonamental. Denotem per z_j, $j = 1, \dots, p$ aquests vèrtexs, segons ordre creixent de la part real. Posem, a més, $z_{p+1} = \infty$, vèrtex que prové directament de $\mathcal{D}(\Gamma(1,p)_\infty)$. Un simple càlcul demostra que, per a $j = 2, \dots, \frac{p+1}{2} - 1$, es té $z_j = C(\frac{2(j-1)-1-p}{2p}, \frac{1}{p}) \cap C(\frac{2j-1-p}{2p}, \frac{1}{p}) = \frac{2j-2-p}{2p} + \frac{\sqrt{3}}{2p}i$; el vèrtex $z_{\frac{p+1}{2}} = C(-1/p, 1/p) \cap C(1/p, 1/p) = 0$; i, per a $j = \frac{p+1}{2} + 1, \dots, p-1$, es té $z_j = C(\frac{2j-1-p}{2p}, \frac{1}{p}) \cap C(\frac{2(j+1)-1-p}{2p}, \frac{1}{p}) = \frac{2j-p}{2p} + \frac{\sqrt{3}}{2p}i$. Finalment, els vèrtexs z_1 i z_p s'obtenen intersecant els cercles d'isometria corresponents, $C(-\frac{p-1}{2p}, \frac{1}{p})$ i $C(\frac{p-1}{2p}, \frac{1}{p})$, amb les semirectes $\mathrm{Re}(z) = -1/2$ i $\mathrm{Re}(z) = 1/2$, respectivament. Aquests dos vèrtexs també es poden calcular com la intersecció de dos cercles d'isometria maximals, $z_1 = C(-\frac{p+1}{2p}, \frac{1}{p}) \cap C(-\frac{p-1}{2p}, \frac{1}{p})$, $z_p = C(\frac{p-1}{2p}, \frac{1}{p}) \cap C(\frac{p+1}{2p}, \frac{1}{p})$, amb $C(-\frac{p+1}{2p}, \frac{1}{p})$ i $C(\frac{p+1}{2p}, \frac{1}{p})$ no pertanyents a

$\mathcal{J}(p)$. Observem que és possible que z_j, $j = 1,\ldots,p+1$, no siguin tots els vèrtexs del domini fonamental, ja que no sabem si contenen els punts el·líptics d'ordre 2 inclosos en la frontera del domini fonamental $\mathcal{D}(\Gamma(1,p))$, considerats també com a vèrtexs.

Per a demostrar (ii), denotem θ_j l'angle interior a $\mathcal{D}(\Gamma(1,p))$ en el vèrtex z_j. Clarament $\theta_{\frac{p+1}{2}} = \theta_{p+1} = 0$. Observem que θ_j pren el mateix valor per a $j = 2,\ldots,\frac{p+1}{2}-1, \frac{p+1}{2}+1,\ldots,p-1$; denotem-lo θ. Tenim, a més, $\theta_1 = \theta_p = \theta/2$. Completem la demostració de (ii) provant $\theta = 2\pi/3$. En efecte, considerant, per exemple, $j = \frac{p+1}{2}+1$, els vectors directors de les rectes tangents als cercles $C(1/p,1/p)$ i $C(2/p,1/p)$ són $(-1,1/\sqrt{3})$ i $(1,1/\sqrt{3})$, respectivament, i formen un angle $\theta = 2\pi/3$.

La figura resultant és un polígon hiperbòlic de $\mathcal{H}$, ja que tant els arcs dels cercles d'isometria com el parell de semirectes provinents de $\mathcal{D}(\Gamma(1,p)_\infty)$ són segments de rectes hiperbòliques. A l'apartat (i) hem explicitat un nombre parell de vèrtexs, $p+1$. S'han d'afegir, si és el cas, els punts el·líptics d'ordre 2 continguts en la frontera de $\mathcal{D}(\Gamma(1,p))$, diferents dels anteriors. Ara bé, gràcies a 2.2.16 i a la simetria del domini, el nombre de vèrtexs el·líptics és també parell, amb la qual cosa obtenim que el nombre total de vèrtexs segueix sent parell. A partir de la paritat del nombre de vèrtexs es dedueix directament que el nombre d'arestes és també parell i coincideix amb l'anterior. Notem que l'existència de vèrtexs el·líptics d'ordre 2, diferents a z_1 i z_p, incrementa el nombre d'arestes en la mateixa quantitat en què s'incrementen els vèrtexs.

Precisem el nombre de vèrtexs total. Recordem que un cicle de punts el·líptics d'ordre 2 té suma d'angles en els seus vèrtexs igual a π, per 3.1.19. Notem també que els vèrtexs z_1 i z_p són equivalents, ja que $T(z_1) = z_p$. Utilitzant les dues afirmacions anteriors i els angles calculats a (ii), és obvi que, per a $p > 2$, els vèrtexs z_j no seran mai el·líptics d'ordre 2. Així, als vèrtexs anteriors s'hi han d'afegir exactament $n_2(1,p)$ vèrtexs, per la qual cosa el nombre total de vèrtexs serà exactament $p+1+n_2(1,p)$. Això completa la demostració de (iii).

Calculem el volum hiperbòlic a partir de l'expressió $V_h(1,p) = (n(1,p)-2)\pi - (\theta_1+\ldots+\theta_{n(1,p)})$, on $\theta_1,\ldots,\theta_{n(1,p)}$ són els angles en els vèrtexs. Considerem, en primer lloc els $p+1$ vèrtexs calculats en (i). La suma dels angles en aquests vèrtexs és $(p-2)\frac{2\pi}{3}$. Notem que no és necessari considerar els vèrtexs el·líptics d'ordre 2, ja que l'angle en cada un d'aquests vèrtexs és π, per la qual cosa no contribueixen al volum del polígon hiperbòlic. Així, $V_h(1,p) = (p+1-2)\pi - \frac{2}{3}(p-2)\pi = (p+1)\frac{\pi}{3}$. □

Conservarem la notació dels vèrtexs z_j per a la resta de la secció.

3.2.10 Lema. *Sigui $z \in \mathcal{H}$, on $z \in C$ amb $C \in \mathcal{C}^{\max}_{\Gamma(1,p)'}$. Aleshores, z és un punt el·líptic d'ordre 3 si, i només si, existeix una homografia $\gamma \in \Gamma(1,p)'$ tal que $C = C_\gamma$ i $z = C_\gamma \cap C_{\gamma^{-1}}$.*

DEMOSTRACIÓ: És immediat veure que es tracta d'una condició suficient. En efecte, si $\gamma \in \Gamma(1,p)'$ és una homografia tal que $z \in C_\gamma \cap C_{\gamma^{-1}}$, aplicant 3.1.13 i 3.1.11, s'obté que γ és una homografia el·líptica d'ordre 3 que té z com a punt fix en $\mathcal{H}$. Per tant, z és el·líptic d'ordre 3.

Recíprocament, vegem que es tracta d'una condició necessària. Sigui z el·líptic d'ordre 3, $z \in C$ amb $C \in \mathcal{C}^{\max}_{\Gamma(1,p)'}$. Sigui $\sigma \in \Gamma(1,p)'$ una homografia el·líptica d'ordre 3 tal que $\sigma(z) = z$. Per 3.1.11, tenim que $z \in C_\sigma \cap C_{\sigma^{-1}}$; en particular, z pertany als cercles d'isometria C, C_σ i $C_{\sigma^{-1}}$, que no poden ser tots tres iguals. Suposem $C \neq C_{\sigma^{-1}}$. Com que $z \in \mathcal{H}$, si apliquem 3.2.3, obtenim que $C_{\sigma^{-1}} \in \mathcal{C}^{\max}_{\Gamma(1,p)'}$. D'aquí deduïm que C_σ també és maximal. Però z no pot pertànyer a més de dos cercles d'isometria maximals; per tant, $C = C_\sigma$. Així considerem $\gamma = \sigma$. Si fos $C = C_{\sigma^{-1}}$, seria $C \neq C_\sigma$ i consideraríem $\gamma = \sigma^{-1}$. □

3.2.11 Teorema. *Considerem el grup $\Gamma(1,p)$, on $p > 2$, actuant en el semiplà de Poincaré. Aleshores el domini fonamental $\mathcal{D}(\Gamma(1,p))$ satisfà:*

i) $n_\infty(1,p) = e_\infty(1,p) = 2$.
Els cicles parabòlics són $\{z_{\frac{p+1}{2}}\} = \{0\}$ *i* $\{z_{p+1}\} = \{\infty\}$.

ii) $n_2(1,p) = e_2(1,p) = \begin{cases} 0 & \text{si } p \equiv 3 \mod 4, \\ 2 & \text{si } p \equiv 1 \mod 4. \end{cases}$
Si $p \equiv 1 \mod 4$, *els cicles el·líptics d'ordre 2 són*

$$\{w_{2,1}\} = \left\{\frac{-k_0}{p} + \frac{1}{p}i\right\}, \quad \{w_{2,2}\} = \left\{\frac{+k_0}{p} + \frac{1}{p}i\right\},$$

on $0 < k_0 \leq \frac{p-1}{2}$, $k_0^2 \equiv -1 \mod p$.

iii) $n_3(1,3) = 2$ *i* $e_3(1,3) = 1$.
Per a $p = 3$, *el cicle el·líptic d'ordre 3 és* $\{z_1, z_3\}$.

iv) *Si* $p > 3$, $n_3(1,p) = e_3(1,p) = \begin{cases} 0 & si\ p \equiv 2 \mod 3, \\ 2 & si\ p \equiv 1 \mod 3. \end{cases}$

Si $p \equiv 1 \mod 3$, *els cicles el·líptics d'ordre* 3 *són*

$$\{w_{3,1}\} = \left\{ \frac{-2k_1 - 1}{2p} + \frac{1}{p}i \right\}, \{w_{3,2}\} = \left\{ \frac{2k_1 + 1}{2p} + \frac{1}{p}i \right\},$$

on $k_1 \in \mathbb{Z}$, $0 < k_1 \leq (p-1)/2$, $k_1^2 + k_1 + 1 \equiv 0 \mod p$.

v) $n_1(1,p) = p - 1 - n_3(1,p)$ *i* $e_1(1,p) = \dfrac{p - 2 - e_3(1,p)}{3}$.

DEMOSTRACIÓ: En primer lloc, provem que els vèrtexs 0 i ∞ són parabòlics. Per al vèrtex ∞, que prové de $\mathcal{D}(\Gamma(1,p)_\infty))$, és obvi, ja que és el punt fix de l'homografia parabòlica T, considerada anteriorment. El vèrtex 0 correspon a la intersecció dels cercles d'isometria maximals tangents $C(-1/p, 1/p)$ i $C(1/p, 1/p)$. Considerem $\sigma = \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$ i obtenim $C_\sigma = C(-1/p, 1/p)$ i $C_{\sigma^{-1}} = C(1/p, 1/p)$. Si apliquem 3.1.12 i 3.1.13, tenim que σ és parabòlica i té el punt 0 com a punt fix; amb l'expressió explícita de σ arribem a la mateixa conclusió a partir directament de les definicions. A més, deduïm, també d'ambdues maneres, que $\sigma(z_{\frac{p+1}{2}-1}) = z_{\frac{p+1}{2}+1}$. El domini $\mathcal{D}(\Gamma(1,p))$ no té altres vèrtexs a $\mathbb{R}$, per la qual cosa no hi ha altres vèrtexs parabòlics. Finalment, comprovem que no són equivalents, ja que $\gamma(0) = \infty$ implicaria $\det\gamma \neq 1$. Així , hi ha exactament dos cicles parabòlics, $\{z_{\frac{p+1}{2}}\} = \{0\}$ i $\{z_{p+1}\} = \{\infty\}$, la qual cosa completa la demostració de (i).

Sigui w un vèrtex de $\mathcal{D}(\Gamma(1,p))$ el·líptic d'ordre 2. Recordem que hem provat que $w \neq z_j$, per a tot $j = 1, \ldots, p$, $p > 2$. Aleshores, existeix un únic cercle d'isometria maximal $C \in \mathcal{J}(p)$ tal que $w \in C$, i l'angle a w és π, cf. 3.1.11. Deduïm que els cicles el·líptics d'ordre 2 estan formats només per un vèrtex, i així $e_2(1,p) = n_2(1,p)$, que ja hem vist que és un nombre parell, aplicant 2.2.16. Com que el cicle $\{w\}$ està format per un sol vèrtex, les dues arestes adjacents al vèrtex w s'identifiquen entre si, i per tant són d'igual longitud per 3.1.19; així w és el punt mig de l'arc de C que forma part de la frontera del domini fonamental. Per 3.2.1, tenim que $C = C(k/p, 1/p)$ per a cert k, $0 < |k| \leq \frac{p-1}{2}$ i, per tant, $w = \frac{k}{p} + \frac{1}{p}i$. Vegem quines condicions ha de complir k perquè w sigui efectivament un punt el·líptic d'ordre 2 de $\Gamma(1,p)$. Observem que $w \notin C'$ per a qualsevol cercle d'isometria no maximal, $C' \in \mathcal{C}_{\Gamma(1,p)'} \setminus \mathcal{C}^{\max}_{\Gamma(1,p)'}$, per 3.2.3, és a dir, w només pertany al cercle d'isometria C. Així, per 3.1.11 w és el·líptic d'ordre 2 si, i només si, $C = C_\gamma = C_{\gamma^{-1}}$, per a certa homografia el·líptica d'ordre 2, $\gamma = \gamma^{-1}$. Com $C = C(k/p, 1/p)$, una

tal homografia ha de ser de la forma $\gamma = \begin{pmatrix} a & b \\ p & -k \end{pmatrix}$ per a certs valors de $a, b \in \mathbb{Z}$ que compleixin $-ak - bp = 1$ i $a = k$. Per tant, w és el·líptic d'ordre 2 si, i només si, $-k^2 - bp = 1$ té solució per a algun $b \in \mathbb{Z}$. Finalment, això és equivalent al fet que -1 sigui un residu quadràtic mòdul p; és a dir $p \equiv 1 \mod 4$. En aquest cas, l'equació $k^2 + bp = -1$ té dues úniques solucions, k_0 i $-k_0$ amb $0 < k_0 \leq \frac{p-1}{2}$, que donen lloc als dos vèrtexs el·líptics d'ordre 2 següents, clarament simètrics respecte de l'eix imaginari,

$$w_{2,1} = \frac{-k_0}{p} + \frac{1}{p}i, \quad w_{2,2} = \frac{k_0}{p} + \frac{1}{p}i.$$

Així doncs, $e_2(1,p) = 2$ si $p \equiv 1 \mod 4$ i $e_2(1,p) = 0$ en cas contrari. Això demostra els resultats per als vèrtexs el·líptics d'ordre 2 enunciats a (ii).

Considerem a continuació els vèrtexs el·líptics d'ordre 3. La suma dels angles en els vèrtexs d'un cicle de punts el·líptics d'ordre 3 és $2\pi/3$, per 3.1.19; per tant, utilitzant 3.2.9 (ii), un cicle el·líptic o bé està constituït per un sol vèrtex, entre $z_2, \ldots, z_{\frac{p+1}{2}-1}, z_{\frac{p+1}{2}+1}, \ldots, z_{p-1}$, o bé és el cicle $\{z_1, z_p\}$.

Suposem que z_1 és un punt el·líptic d'ordre 3. Aplicant el lema 3.2.10, els cercles d'isometria $C(-\frac{p+1/2}{p}, \frac{1}{p})$ i $C(-\frac{p-1/2}{p}, \frac{1}{p})$ corresponen a homografies inverses l'una de l'altra, i això dóna l'equació $p^2 + 4bp = 3$, que només té solució per a $p = 3$. Així, $\{z_1, z_p\}$ és un cicle el·líptic d'ordre 3 si, i només si, $p = 3$. En aquest cas, no hi ha més vèrtexs que puguin ser el·líptics d'ordre 3; per tant, $n_3(1,3) = 2$ i $e_3(1,3) = 1$, la qual cosa completa la demostració de (iii).

Suposem ara $p > 3$, per a demostrar (iv). En primer lloc, recordem que l'homografia parabòlica corresponent al vèrtex 0 relacionava els vèrtexs $z_{\frac{p+1}{2}-1}$ i $z_{\frac{p+1}{2}+1}$, per la qual cosa són vèrtexs equivalents. D'aquí deduïm que no són mai el·líptics, ja que els seus angles sumen $4\pi/3 > 2\pi/3$ (cf. 3.2.9). El mateix argument d'angles ens condueix al fet que els cicles el·líptics d'ordre 3 tenen un sol vèrtex, i així $n_3(1,p) = e_3(1,p)$; a més, és un nombre parell, per 2.2.16, de forma anàloga al cas d'ordre 2.

Determinem de forma efectiva quan hi ha vèrtexs el·líptics d'ordre 3. Suposem que un vèrtex $z \in \mathcal{H}$, obtingut com a intersecció de dos cercles d'isometria maximals consecutius, és un punt el·líptic d'ordre 3. Aplicant 3.2.10, aquests dos cercles d'isometria han de correspondre a homografies inverses l'una de l'altra, és a dir, $z = C_\gamma \cap C_{\gamma^{-1}}$, per a certa homografia el·líptica $\gamma \in \Gamma(1,p)'$. La descripció explícita de $\mathcal{C}^{\max}_{\Gamma(1,p)}$, donada a 3.2.1 ens porta a $C_\gamma = C(k/p, 1/p)$ i $C_{\gamma^{-1}} = C((k+1)/p, 1/p)$ per a cert valor de $k \in \mathbb{Z}$, $|k| \leq (p-1)/2$, $k \neq 0, -1$.

Així , γ serà de la forma $\begin{pmatrix} a & b \\ p & -k \end{pmatrix}$, amb $o_{\gamma^{-1}} = \dfrac{-a}{p} = \dfrac{k+1}{p}$; per tant, $a = -(k+1)$. Si imposem $\det(\gamma) = 1$, obtenim que $-(k+1)k - bp = 1$. En reduir mòdul p resulta l'equació $k^2 + k + 1 \equiv 0 \mod p$, que té solució si, i només si, -3 és un residu quadràtic mòdul p. Això demostra que un vèrtex de $\mathcal{D}(\Gamma(1,p))$ és el·líptic d'ordre 3 si, i només si, s'obté de la forma $C(k/p, 1/p) \cap C((k+1)/p, 1/p)$, on $|k| \leq (p-1)/2$, $k^2 + k + 1 \equiv 0 \mod p$. Així, doncs, $e_3(1,p) = 0$ si $p \equiv 2 \mod 3$ i $e_3(1,p) = 0$ si $p \equiv 2 \mod 3$. En aquest últim cas, els vèrtexs el·líptics són

$$w_{3,1} = \frac{-2k_1 - 1}{2p} + \frac{\sqrt{3}}{2p}i, \quad w_{3,2} = \frac{2k_1 + 1}{2p} + \frac{\sqrt{3}}{2p}i,$$

on $k_1 \in \mathbb{Z}$, $0 < k_1 \leq (p-1)/2$ és una solució de $k^2 + k + 1 \equiv 0 \mod p$. Això demostra (iv).

Els vèrtexs accidentals són els vèrtexs que no són ni el·líptics ni parabòlics i es troben forçosament entre els vèrtexs z_j calculats a 3.2.9. Així, $n_1(1,p) = n(1,p) - n_\infty(1,p) - n_2(1,p) - n_3(1,p) = p - 1 - n_3(1,p)$. Tenint en compte que la suma en cada cicle accidental ha de ser 2π (cf. 3.2.9), obtenim que els cicles accidentals estan formats per tres vèrtexs, excepte el cicle accidental al qual pertanyin z_1 i z_p, per a $p > 3$, que en tindrà quatre. Per tant, $3e_1(1,p) = p - 2 - e_3(1,p)$. □

3.2.12 Remarca. El domini fonamental $\mathcal{D}(\Gamma(1,p))$, per a $p > 3$, satisfà que els cicles el·líptics i parabòlics consten d'un sol vèrtex i que no hi ha vèrtexs accidentals en $\mathbb{R}$. □

3.2.13 Notació. Sigui p un nombre primer fixat, $p > 2$. Per a cada $k \in \mathbb{Z}$ amb $0 < |k| \leq \frac{p-1}{2}$, denotem

$$\gamma_k = \begin{pmatrix} a & b \\ p & -k \end{pmatrix} \in \Gamma(1,p),$$

on $a, b \in \mathbb{Z}$ vénen determinats unívocament per les condicions $-ak - bp = 1$ i $0 < |a| \leq \frac{p-1}{2}$. Notem que $\gamma_{-1} = \gamma_1^{-1}$. □

3.2.14 Proposició. *Sigui p un nombre primer, $p > 2$. El grup d'homografies definit per $\Gamma(1,p)$ està generat per T, γ_1 i les homografies γ_k tals que $|a| \geq |k|$ si $|k| > 1$. Les relacions entre aquests generadors són les següents:*

(i) $\gamma_{k_0}^2 = \gamma_{-k_0}^2 = 1$, *si* $k_0 > 0$ *amb* $k_0^2 \equiv -1 \mod p$;

(ii) $\gamma_{k_1}^3 = \gamma_{-k_1-1}^3 = 1$, *si* $k_1 > 0$ *amb* $k_1^2 + k_1 + 1 \equiv 0 \mod p$;

(iii) *una relació del tipus* $\gamma_{t_3}^{\varepsilon_{t_3}} \gamma_{t_2}^{\varepsilon_{t_2}} \gamma_{t_1}^{\varepsilon_{t_1}} = 1$ *per a cada cicle accidental de* $\mathcal{D}(\Gamma(1,p))$ *de la forma* $\{z_{j_1}, z_{j_2}, z_{j_3}\}$ *amb* $\gamma_{t_i}^{\varepsilon_{t_i}}(z_{j_i}) = z_{j_{i+1}}$, $z_{j_4} = z_{j_1}$, $\varepsilon_{t_i} = \pm 1$;

(iv) *la relació* $T^{-1}\gamma_{s_2}^{\varepsilon_{s_2}} \gamma_{s_1}^{\varepsilon_{s_1}} \gamma_{\frac{1-p}{2}} = 1$, *per a* $p > 3$, *que prové de l'únic cicle accidental de* $\mathcal{D}(\Gamma(1,p))$ *que conté quatre vèrtexs* $\{z_1, z_{a_1}, z_{a_2}, z_p\}$, *amb* $\gamma_{\frac{1-p}{2}}(z_1) = z_{a_1}$, $\gamma_{s_1}(z_{a_1}) = z_{a_2}$ *i* $\gamma_{s_2}(z_{a_2}) = z_p$, $\varepsilon_{s_i} = \pm 1$.

DEMOSTRACIÓ: El domini fonamental $\mathcal{D}(\Gamma(1,p))$ és un polígon hiperbòlic d'un nombre parell d'arestes identificades dos a dos i, per 3.1.19, les homografies que aparellen les arestes formen una família de generadors.

La translació T aparella les dues arestes que són semirectes verticals, que provenen de les arestes de $\mathcal{D}(\Gamma(1,p)_\infty)$, per la qual cosa forma part de la família de generadors. L'homografia γ_1 identifica les dues arestes que s'intersecten en el punt 0, per la qual cosa serà també un generador i, a l'igual que T, serà un element d'ordre infinit.

El lema 3.2.7 ens assegura que, donat $C \in \mathcal{J}(p)$, existeix una única homografia $\gamma \in \Gamma(1,p)'$ tal que $C = C_\gamma$ i $C_{\gamma^{-1}} \in \mathcal{J}(p)$. Aplicant les propietats dels cercles d'isometria i les homografies, cf. 3.1.8 i 3.1.10-3.1.12, és clar que l'homografia γ aparella les arestes que formen part dels cercles C_γ i $C_{\gamma^{-1}}$. Recordem que $\mathcal{J}(p)$ és precisament el conjunt de cercles d'isometria que donen arestes de $\mathcal{D}(\Gamma(1,p))$.

Així, per a aparellar les arestes de $\mathcal{D}(\Gamma(1,p))$ que són arcs de cercles d'isometria n'hi ha prou amb el conjunt d'homografies corresponents als cercles d'isometria de $\mathcal{J}(p)$, l'expressió explícita del qual es dóna en 3.2.6 i coincideix amb el conjunt dels γ_k. Òbviament, hem d'evitar les repeticions causades per una homografia i la seva inversa, per la qual cosa afegim la condició $|a| \geq |k|$, per a $|k| > 1$.

Pel que fa a les relacions, només cal recordar que s'obté una relació per a cada cicle d'ordre finit, cf. 3.1.19. Així, els cicles el·líptics d'ordre 2 i 3, si n'hi ha, ens aporten les relacions $\gamma_{k_0}^2 = \gamma_{-k_0}^2 = 1$ i $\gamma_{k_1}^3 = \gamma_{(-k_1-1)}^3 = 1$, on $k_0 > 0$ satisfà $k_0^2 \equiv -1 \mod p$ i $k_1 > 0$ satisfà $k_1^2 + k_1 + 1 \equiv 0 \mod p$, respectivament. A partir de cada cicle accidental, obtenim una relació de la forma indicada. □

La presentació obtinguda en la proposició anterior té $(p + 1 + e_2(1,p))/2$ generadors i $e_1(1,p) + e_2(1,p) + e_3(1,p)$ relacions. En general, no serà una

presentació minimal. Una forma de disminuir el nombre de relacions i de generadors seria disminuir el nombre de cicles accidentals, que no és pròpiament un invariant del grup i que depèn del tipus de domini fonamental escollit. De totes maneres, no es pot realitzar de forma indiscriminada per a tots els cicles accidentals, ja que hi ha repeticions de generadors entre les diferents relacions.

Finalment, per fer complets els resultats considerem els casos $p \leq 2$. El dominis fonamentals corresponents es troben a 3.2.5. Recuperem-ne les característiques en les proposicions següents, que es demostren utilitzant també arguments derivats de les propietats dels cercles d'isometria.

3.2.15 Proposició. *Considerem el domini fonamental $\mathcal{D}(\Gamma(1,1))$ del grup modular $\Gamma(1,1) = \mathrm{SL}(2,\mathbb{Z})$. Aleshores,*

(i) *$\mathcal{D}(\Gamma(1,1))$ té $n(1,1) = 4$ vèrtexs: $z_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$, $z_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, $z_3 = \infty$ i $w_{2,1} = i$.*

(ii) *L'angle interior a $\mathcal{D}(\Gamma(1,1))$ en els vèrtexs z_1 i z_2 és $\pi/3$ i en el vèrtex $w_{2,1}$, és π.*

(iii) *El volum hiperbòlic de $\mathcal{D}(\Gamma(1,1))$ és $V_h(1,1) = \dfrac{\pi}{3}$.*

(iv) *$n_\infty(1,1) = e_\infty(1,1) = 1$; el vèrtex parabòlic és ∞.*

(v) *$n_2(1,1) = e_2(1,1) = 1$; el vèrtex el·líptic d'ordre 2 és $w_{2,1}$.*

(vi) *$n_3(1,1) = 2$ i $e_3(1,1) = 1$; els vèrtexs el·líptics d'ordre 3 són z_1 i z_2.*

(vii) *$n_1(1,1) = e_1(1,1) = 0$; és a dir, no hi ha vèrtexs accidentals.*

(viii) *El grup $\mathrm{PSL}(2,\mathbb{Z})$ està generat per*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad i \quad S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

amb la relació $S^2 = 1$.

DEMOSTRACIÓ: En aquest cas, $\mathcal{J}(1) = \{C(0,1)\}$. El cercle d'isometria $C(0,1)$ és C_σ per a una homografia $\sigma \in \Gamma(1,1)$ tal que $c = \pm 1$, $d = 0$, $b = -c$ i $a \in \mathbb{Z}$. Així, és el cercle d'isometria de les homografies

$$\sigma_a = \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix}, \quad a \in \mathbb{Z}.$$

Per als valors $|a| > 2$, el centre del cercle $C_{\sigma_a^{-1}}$ és a; en aquest cas, els cercles $C_{\sigma_a^{-1}}$ i C_{σ_a} no es tallen i σ_a i σ_a^{-1} són transformacions hiperbòliques.

Tenim que σ_a és el·líptic si, i només si, $|a| < 2$. Per al valor $a = 0$, obtenim l'homografia $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. En aquest cas, se satisfà $\sigma_a = \sigma_a^{-1}$, i σ_a és una homografia el·líptica d'ordre 2. El punt el·líptic corresponent és $w_{2,1} = i$. Per als valors $a = \pm 1$, obtenim les homografies $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ i $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$, les dues d'ordre 3. Els punts el·líptics corresponents són $z_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ i $z_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, respectivament. Observem que els tres punts el·líptics són vèrtexs del domini fonamental que hem trobat. S'obtenen també directament a partir dels cercles d'isometria, utilitzant 3.1.11 i 3.1.19, com hem fet en el cas general. Si explicitem les homografies que corresponen als cercles, tenim que $w_{2,1} \in C_S$, $z_1 = C_{ST} \cap C_{(ST)^{-1}} = C(-1,1) \cap C(0,1)$, $z_2 = C_{TS} \cap C_{(TS)^{-1}} = C(0,1) \cap C(1,1)$.

Les homografies S i T són les que identifiquen les arestes del domini fonamental dos a dos; per tant, formen una família de generadors del grup modular $\mathrm{PSL}(2,\mathbb{Z})$, amb la relació $S^2 = 1$. □

Amb els mateixos arguments es demostra la proposició següent per al cas $p = 2$.

3.2.16 Proposició. *Sigui $\mathcal{D}(\Gamma(1,2))$ el domini fonamental de $\Gamma(1,2)$ en $\mathcal{H}$. Aleshores,*

(i) $n(1,2) = 4$. *Explícitament,* $z_1 = \frac{-1}{2} + \frac{1}{2}i$, $z_2 = 0$, $z_3 = \frac{1}{2} + \frac{1}{2}i$ *i* $z_4 = \infty$.

(ii) *L'angle interior a $\mathcal{D}(\Gamma(1,2))$ en els vèrtexs z_1 i z_3 és $\pi/2$ i en el vèrtex z_2, és* 0.

(iii) *El volum hiperbòlic de $\mathcal{D}(\Gamma(1,2))$ és $V_h(1,2) = \pi$.*

(iv) $n_\infty(1,2) = e_\infty(1,2) = 2$; *els cicles parabòlics són* $\{0\}$ *i* $\{\infty\}$

(v) $n_2(1,2) = 2$, $e_2(1,2) = 1$; *el cicle el·líptic d'ordre* 2 *és* $\{z_1, z_3\}$.

(vi) $n_3(1,2) = 0$; *és a dir, no hi ha vèrtexs el·líptics d'ordre* 3.

(vii) $n_1(1,2) = 0$; *és a dir, no hi ha vèrtexs accidentals.*

(viii) *El grup* $\Gamma(1,2)/\pm\mathrm{Id}$ *està generat per*

$$T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad i \quad \gamma_1=\begin{pmatrix}-1 & 0\\ 2 & -1\end{pmatrix},$$

amb la relació $(\gamma_1 T)^2=1$. □

3.3 Algoritmes, taules i gràfiques

Hem implementat els resultats obtinguts en les seccions anteriors com a part del paquet `Poincare`.

D'una banda, presentem instruccions per a facilitar la manipulació dels cercles d'isometria associats a les homografies. Així, tenim les instruccions `cenIC` i `radIC` per a obtenir el centre i el radi del cercle d'isometria associat a una homografia, respectivament. Per a definir el cercle d'isometria com a objecte geomètric hi ha la instrucció `defIC`. La instrucció `symLIC` determina la recta de simetria L_γ, cf. 3.1.8.

D'altra banda, tenim tot un bloc d'instruccions referents a les propietats i a la representació gràfica del domini fonamental de la corba $X(1,p)$, construït en la secció anterior. En la majoria d'instruccions l'única dada d'entrada és el nombre primer p.

En primer lloc, hem inclòs instruccions per a calcular les constants associades a la corba modular $X(1,p)$: `einfX1`, `e2X1`, `e3X1`, `volhX1`, `volhX1` i `genusX1`, que donen el nombre de cicles parabòlics, el·líptics d'ordre 2, el·líptics d'ordre 3, el volum hiperbòlic, el volum normalitzat i el gènere, respectivament. De fet, els mateixos valors es poden obtenir a partir de les instruccions comentades en el capítol anterior, que calculen les constants associades a una corba de Shimura $X(D,N)$ en general. Ara bé, les hem reprogramat utilitzant les fórmules simplificades obtingudes en aquest capítol, a partir de les propietats dels cercles d'isometria i del domini fonamental construït. A més, tenim en aquest cas la instrucció `e1X1`, que compta el nombre de cicles accidentals.

Per a obtenir tota la informació disponible referent al domini fonamental de $X(1,p)=X_0(p)$ construït, per a qualsevol nombre primer p, disposem d'instruccions per als cardinals dels conjunts de vèrtexs, instruccions per a donar-los explícitament i per a organitzar-los en cicles. Així, `ninfX1`, `n2X1`, `n3X1`, `n1X1` i `nvX1` proporcionen els cardinals dels conjunts de vèrtexs parabòlics, el·líptics d'ordre 2, el·líptics d'ordre 3, accidentals i el nombre total de vèrtexs, respectivament. Les comandes `vintX1`, `vpX1`, `ve3X1`, `ve2X1`, `vtoX1` i `vtcX1`

donen les llistes explícites dels vèrtexs obtinguts com a intersecció dels cercles d'isometria i les semirectes, dels parabòlics, dels el·líptics d'ordre 2, dels el·líptics d'ordre 3, la llista total de vèrtexs i la llista de vèrtexs classificats per tipus, respectivament. Obtenim els vèrtexs organitzats en cicles amb la instrucció `cyclesX1` i les parelles d'arestes que s'identifiquen amb `pairEdX1`. En particular, hem programat les instruccions `leq idx` i `seg` per a facilitar l'ordenació de les llistes de vèrtexs.

Pel que fa als resultats sobre el grup, obtenim una presentació explícita del grup $\Gamma(1,p)/\pm\mathrm{Id}$, amb generadors i relacions, amb les instruccions `geneX1` i `relX1`.

Finalment, la instrucció `plotFDX1` dóna la representació gràfica del domini fonamental $\mathcal{D}(\Gamma(1,p))$.

A continuació presentem alguns exemples per tal d'il·lustrar les propietats dels dominis fonamentals construïts per a $\Gamma(1,p)/\pm\mathrm{Id}$, que difereixen d'altres dominis fonamentals coneguts (cf. [BT92]). Potser la principal diferència sigui la seva gran simetria i la seva construcció sistemàtica, fàcilment implementable.

En la figura 3.5 reproduïm els dominis fonamentals de les corbes modulars $X(1,1)$, $X(1,2)$ i $X(1,3)$, respectivament.

En la figura 3.6 representem el domini fonamental de la corba modular $X(1,11)$, de gènere 1. Notem que no té cap vèrtex el·líptic. Els vèrtexs i els cicles accidentals, i una presentació del grup, els explicitem en la taula 3.1.

Incloem el cas $p=13$ com a exemple de domini fonamental amb el màxim nombre possible de cicles el·líptics. La figura 3.7 mostra el domini fonamental de $X(1,13)$, corba modular de gènere 0. Hem recopilat les dades calculades en la taula 3.1.

Donem també la representació del domini fonamental per al cas $p=23$, en la figura 3.8. Correspon al menor valor de p, nombre primer, tal que $X(1,p)$ és de gènere 2. Observem que tampoc té cicles el·líptics. Els cicles accidentals i una presentació del grup, els mostrem en la taula 3.3.

Finalment, donem també la representació gràfica del domini fonamental de la corba $X(1,41)$, de gènere 3, en la figura 3.9. En la taula 3.4 mostrem les dades referents al grup $\Gamma(1,41)$ i al domini fonamental construït.

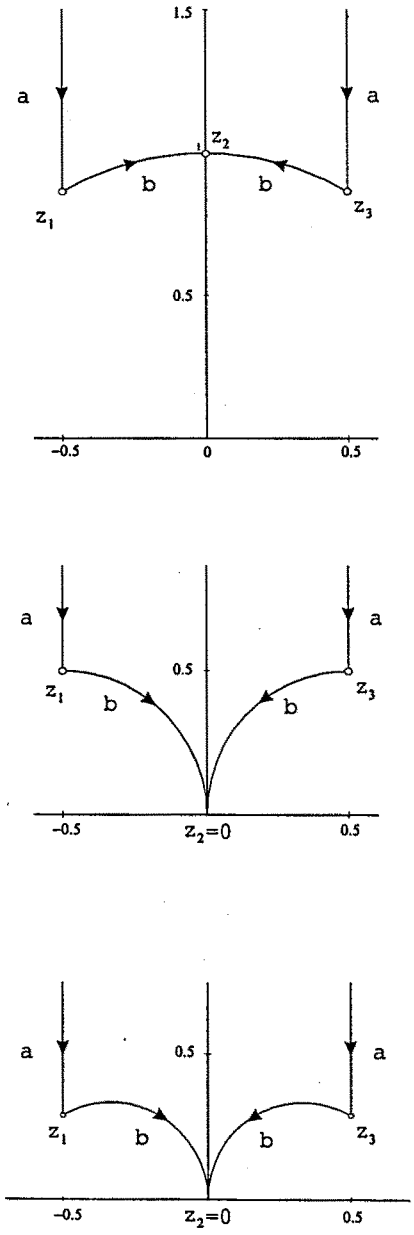

Figura 3.5: Dominis fonamentals de $X(1,1)$, $X(1,2)$ i $X(1,3)$.

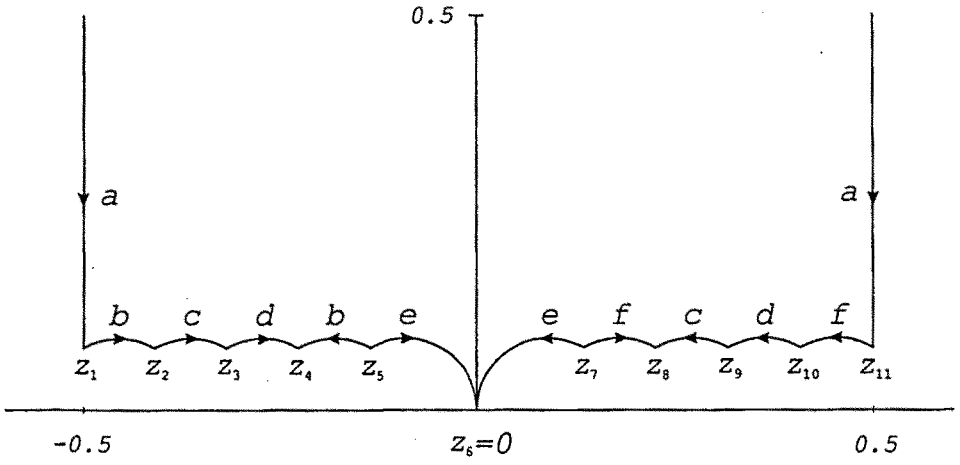

Figura 3.6: Domini fonamental de $X(1,11)$.

Taula 3.1 *Cicles de la corba de Shimura* $X(1,11)$ *i presentació del grup* $\Gamma(1,11)/\pm \mathrm{Id}$.

k	$n_k(1,11)$	$e_k(1,11)$	cicles d'ordre k
∞	2	2	$\{0\}$, $\{\infty\}$
2	0	0	
3	0	0	
1	10	3	$\{z_1, z_{11}, z_7, z_5\}$, $\{z_2, z_4, z_9\}$, $\{z_{10}, z_8, z_3\}$

generadors	relacions
T, γ_1, γ_2,γ_3, γ_{-2},γ_{-3}	$\gamma_{-2}\gamma_1\gamma_2^{-1}T = 1$, $\gamma_3\gamma_{-3}\gamma_{-2}^{-1} = 1$, $\gamma_{-3}\gamma_3\gamma_2^{-1} = 1$

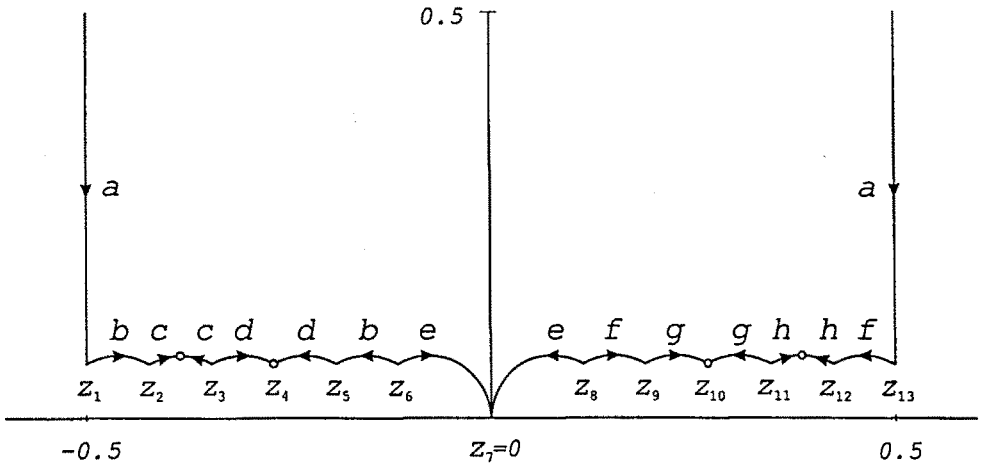

Figura 3.7: Domini fonamental de $X(1,13)$.

Taula 3.2 *Cicles de la corba de Shimura* $X(1,13)$ *i presentació del grup* $\Gamma(1,13)/\pm\mathrm{Id}$.

k	$n_k(1,13)$	$e_k(1,13)$	cicles d'ordre k
∞	2	2	$\{0\},\{\infty\}$
2	2	2	$\{w_{2,1}\}=\{\frac{-5}{13}+\frac{1}{13}i\}$, $\{w_{2,2}\}=\{\frac{5}{13}+\frac{1}{13}i\}$
3	2	2	$\{z_4\}=\{\frac{-7}{26}+\frac{\sqrt{3}}{26}i\}$, $\{z_{10}\}=\{\frac{7}{26}+\frac{\sqrt{3}}{26}i\}$
1	10	3	$\{z_1,z_{13},z_8,z_6\}$, $\{z_2,z_3,z_5\}$, $\{z_{12},z_{11},z_9\}$

generadors	relacions
$\gamma_5,\gamma_{-5},\gamma_3,\gamma_{-3}$	$\gamma_5^2=\gamma_{-5}^2=1$, $\gamma_3^3=\gamma_{-3}^3=1$,
$T,\gamma_1,\gamma_2,\gamma_{-2}$	$\gamma_{-2}\gamma_1\gamma_2^{-1}T=1$, $\gamma_{-2}\gamma_{-3}^{-1}\gamma_{-5}=1$,
	$\gamma_2\gamma_3^{-1}\gamma_5=1$

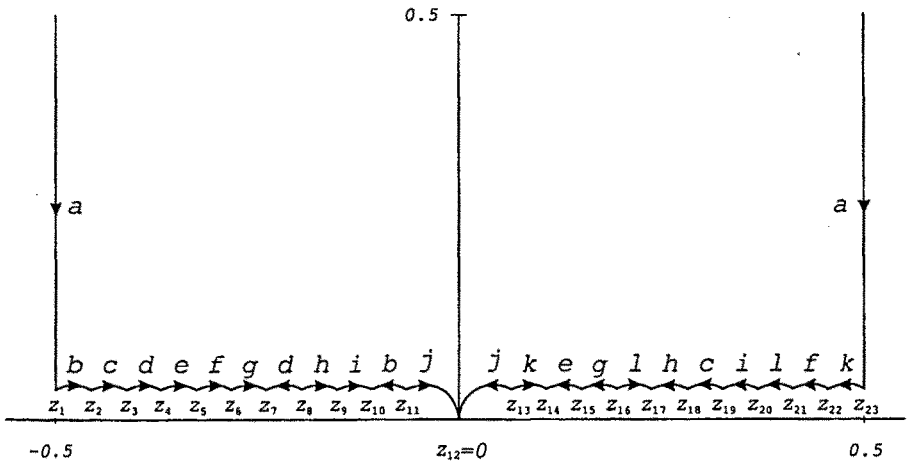

Figura 3.8: Domini fonamental de $X(1,23)$.

Taula 3.3 *Cicles de la corba de Shimura* $X(1,23)$ *i presentació del grup* $\Gamma(1,23)/\pm\mathrm{Id}$.

k	$n_k(1,23)$	$e_k(1,23)$	cicles d'ordre k
∞	2	2	$\{0\},\{\infty\}$
2	0	0	
3	0	0	
1	22	7	$\{z_1,z_{23},z_{13},z_{11}\}$, $\{z_2,z_{10},z_{19}\}$, $\{z_3,z_8,z_{18}\}$, $\{z_4,z_{15},z_7\}$, $\{z_{22},z_{14},z_5\}$, $\{z_{21},z_{16},z_6\}$, $\{z_{20},z_9,z_{17}\}$

generadors	relacions
$T,\gamma_1,\gamma_2,\gamma_3,\gamma_4,\gamma_5,\gamma_7,$ $\gamma_{-2},\gamma_{-3},\gamma_{-4},\gamma_{-5},\gamma_{-7}$	$\gamma_{-2}\gamma_1\gamma_2^{-1}T=1$, $\gamma_7\gamma_{-3}\gamma_{-2}^{-1}=1$, $\gamma_7\gamma_{-4}\gamma_{-5}^{-1}=1$, $\gamma_{-5}\gamma_4\gamma_3^{-1}=1$, $\gamma_{-7}\gamma_3\gamma_2^{-1}=1$, $\gamma_{-7}\gamma_4\gamma_5^{-1}=1$, $\gamma_5\gamma_{-4}\gamma_{-3}^{-1}=1$

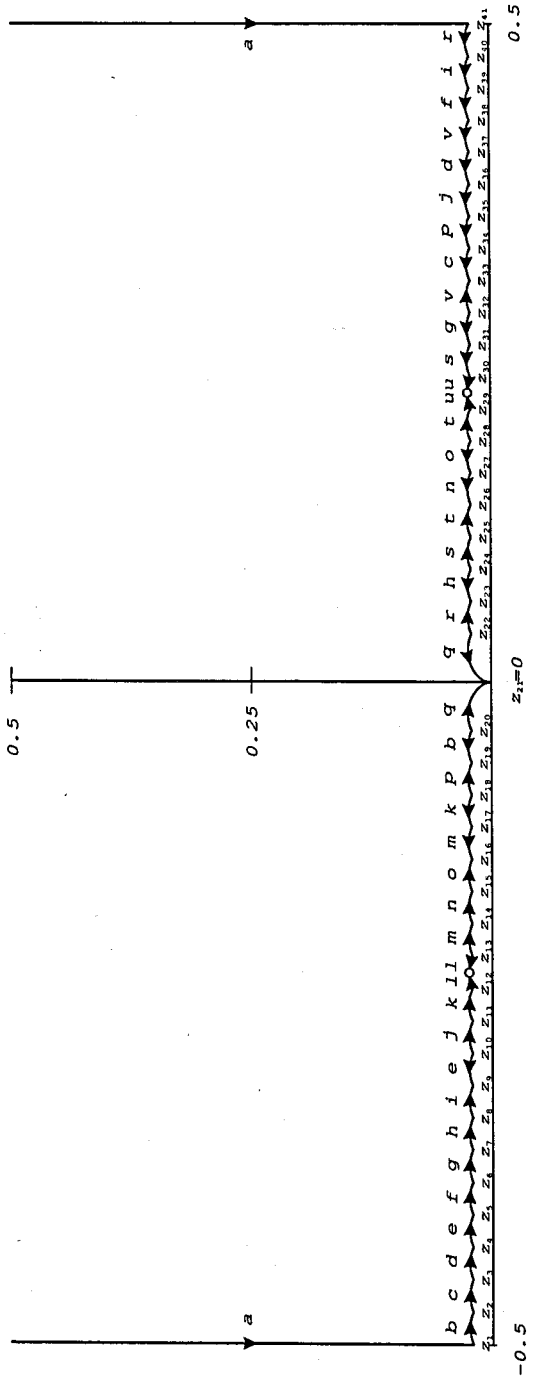

Figura 3.9: Domini fonamental de $X(1, 41)$.

Taula 3.4 *Cicles de la corba de Shimura* $X(1,41)$ *i presentació del grup* $\Gamma(1,41)/\pm\mathrm{Id}$.

k	$n_k(1,41)$	$e_k(1,41)$	cicles d'ordre k
∞	2	2	$\{0\}$, $\{\infty\}$
2	2	2	$\{w_{2,1}\}=\{\frac{-9}{41}+\frac{1}{41}i\}$, $\{w_{2,2}\}=\{\frac{9}{41}+\frac{1}{41}i\}$
3	0	0	
1	40	13	$\{z_1,z_{20},z_{22},z_{41}\}$, $\{z_2,z_{34},z_{19}\}$, $\{z_3,z_{37},z_{33}\}$, $\{z_4,z_{10},z_{36}\}$, $\{z_5,z_{39},z_9\}$, $\{z_6,z_{32},z_{38}\}$, $\{z_7,z_{24},z_{31}\}$, $\{z_8,z_{40},z_{23}\}$, $\{z_{11},z_{18},z_{35}\}$, $\{z_{12},z_{13},z_{17}\}$, $\{z_{14},z_{27},z_{16}\}$, $\{z_{15},z_{28},z_{26}\}$, $\{z_{25},z_{29},z_{30}\}$.

generadors	$T,\gamma_1,\gamma_9,\gamma_{-9},$ $\gamma_2,\gamma_3,\gamma_4,\gamma_5,\gamma_6,\gamma_{11},\gamma_{12},\gamma_{13},\gamma_{16},$ $\gamma_{-2},\gamma_{-3},\gamma_{-4},\gamma_{-5},\gamma_{-6},\gamma_{-11},\gamma_{-12},\gamma_{-13},\gamma_{-16}.$
relacions	$\gamma_9^2=\gamma_{-9}^2=1,\ T^{-1}\gamma_2\gamma_1\gamma_2^{-1}=1,$ $\gamma_{-2}\gamma_3^{-1}\gamma_{-13}^{-1}=1,\ \gamma_{13}\gamma_{-12}^{-1}\gamma_{-10}^{-1}=1,\ \gamma_{16}\gamma_{-11}\gamma_{12}^{-1}=1,$ $\gamma_{-12}\gamma_{13}^{-1}\gamma_{-16}=1,\ \gamma_{16}^{-1}\gamma_{12}\gamma_{-11}^{-1}=1,\ \gamma_{11}\gamma_4\gamma_{-3}^{-1}=1,$ $\gamma_3\gamma_{-2}^{-1}\gamma_{-13}=1,\ \gamma_{11}^{-1}\gamma_{-3}\gamma_4^{-1}=1,\ \gamma_{-4}\gamma_5\gamma_{-9}=1,$ $\gamma_{-5}\gamma_6^{-1}\gamma_{-6}^{-1}=1,\ \gamma_6\gamma_{-5}^{-1}\gamma_{-6}=1,\ \gamma_{-4}^{-1}\gamma_9\gamma_5=1.$

Capítol 4

Formes quadràtiques enteres

En aquest capítol incloem definicions i resultats referents a formes quadràtiques. En alguns casos ha calgut generalitzar definicions conegudes per a les formes binàries, ternàries o quaternàries a altres graus, com per exemple el concepte de nivell definit per a una forma ternària (cf. [Ogg69] i [Leh92]) o la propietat de K-forma aplicada a les formes quaternàries (cf. [Bra24]). En general, ens restringirem a formes quadràtiques regulars.

Siguin K un cos de característica $\neq 2$ i $R \subseteq K$ un subanell. En general, K serà un cos de nombres totalment real o algun dels seus localitzats. En particular, ens interessarà el cas $R = \mathcal{O}_K$, l'anell d'enters de K.

4.1 Introducció

Una forma quadràtica f de n variables sobre K és un polinomi homogeni $f \in K[X_1, \ldots, X_n]$ de grau 2. Es pot escriure com

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j, \qquad \text{on } a_{ij} = a_{ji},\ a_{ij} \in K.$$

Sobre un K-espai vectorial V de dimensió n, tota forma quadràtica f defineix una estructura d'espai quadràtic. Com a referències per a l'estudi de les formes quadràtiques, citem [Gau1801], [Sie44], [Jon67], [Ser73] i [Kit93].

4.1.1 Definicions generals

4.1.1 Definició. Una matriu simètrica $A = (a_{ij}) \in \mathrm{M}(n, R)$ és una matriu parella si $2|a_{ii}$ per a tot $1 \leq i \leq n$. □

4.1.2 Definicions. La matriu simètrica $A(f) = (a_{ij})$ s'anomena matriu associada a f. Així,

$$f(X_1, \ldots, X_n) = \begin{pmatrix} X_1 & \cdots & X_n \end{pmatrix} A(f) \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

De fet, és la matriu de la forma f, fixada una base de V. Si la forma f té coeficients en un anell $R \subseteq K$, la matriu $A(f)$ té les entrades a $R[\frac{1}{2}]$. Podem associar a f una altra matriu amb les entrades a R; n'hi ha prou amb posar $A_2(f) := 2A(f)$. Anomenem matriu parella associada a f la matriu $A_2(f)$. Tenim que

$$f(X_1, \ldots, X_n) = \frac{1}{2}\begin{pmatrix} X_1 & \cdots & X_n \end{pmatrix} A_2(f) \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

El determinant de la forma quadràtica f, denotat per $\det_1(f)$, és igual al determinant de la matriu associada $A(f)$. Si $\det_1(f) = 0$, es diu que la forma f és singular; altrament, es diu que és regular. Anomenem determinant parell de f, denotat per $\det_2(f)$, el determinant de la matriu parella. Així,

$$\begin{aligned} \det_1(f) &:= \det A(f), \\ \det_2(f) &:= \det A_2(f). \end{aligned}$$

Observem que tenim la relació $\det_2(f) = 2^n \det_1(f)$. Si f té coeficients a R, aleshores $\det_2(f) \in R$; en canvi, $\det_1(f) \in R[\frac{1}{2}]$. □

D'ara en endavant, tractarem només formes quadràtiques regulars.

4.1.3 Definició. El K-discriminant de la forma quadràtica f, denotat per $\mathrm{disc}_K(f)$, és la classe del determinant $\det_1(f)$ a K^*/K^{*2}. □

Observem que per a les formes quadràtiques d'un nombre parell de variables és igual definir el K-discriminant a partir de $\det_1(f)$ o de $\det_2(f)$. De la naturalesa dels determinants i el discriminant en depenen, en bona part, les propietats de les formes quadràtiques.

Per mitjà d'un canvi de variables R-lineal, $X_i = \sum_{j=1}^{n} c_{ij}Y_j$ amb $c_{ij} \in R$, per a $1 \leq i \leq n$, s'obté una forma quadràtica f'. Posant $C = (c_{ij})$, tenim la relació de matrius $A(f') = C^t A(f)C$. En particular, considerant determinants, tenim que $\det A(f') = \det A(f)(\det C)^2$; és a dir, $\det_1(f') = \det_1(f)(\det C)^2$. En canvi, és clar que els K-discriminants són iguals, $\mathrm{disc}_K(f') = \mathrm{disc}_K(f)$.

Per exemple, sigui $f(X,Y) = X^2 + XY - Y^2$. Fent el canvi $X = X - Y$, $Y = 2Y$, obtenim la forma diagonal $f'(X,Y) = X^2 - 5Y^2$. Tenim que $\det_1(f) = -\frac{5}{4}$, $\det_2(f) = -5$, $\det_1(f') = -5$, $\det_2(f') = -20$ i $\det C = 2$.

4.1.4 Definició. L'adjunta $\mathrm{ad}(f)$ d'una forma quadràtica f és la forma quadràtica que té per matriu associada la matriu adjunta de $A(f)$; és a dir, $A(\mathrm{ad}(f)) = \mathrm{ad}(A(f)) := \det A(f) \cdot A(f)^{-1}$. □

4.1.5 Lema. *Sigui A una matriu parella de $\mathrm{M}(2k,R)$, $k \in \mathbb{N}$. Aleshores, $\mathrm{ad}(A)$ és també una matriu parella.*

DEMOSTRACIÓ: Sigui $\mathrm{ad}(A) = (A_{ij})$. Per a cada i, $1 \leq i \leq 2k$, A_{ii} correspon al determinant d'una matriu de mida $r = 2k - 1$, parella. Provarem que cada un d'aquests determinants és múltiple de 2. Per definició, $A_{ii} = \sum_\sigma \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{r\sigma(r)}$, on σ recorre el grup simètric sobre r elements. Com que A és simètrica, els sumands per a σ i σ^{-1} són els mateixos. Per a cada parella $\sigma \neq \sigma^{-1}$, és a dir, $\sigma^2 \neq 1$, tindrem dos sumands iguals. Com que r és senar, cada permutació σ tal que $\sigma^2 = 1$ té almenys un punt fix; per tant, cadascun d'aquests sumands conté almenys un element de la diagonal, a_{jj}, que és múltiple de 2. □

4.1.6 Lema. *Sigui f una forma quadràtica regular de n variables de coeficients a R.*

(i) *La forma quadràtica* $\mathrm{ad}(f)$ *té coeficients a* $R\left[\frac{1}{2^{n-1}}\right]$.

(ii) $\det_1(\mathrm{ad}(f)) = (\det_1(f))^{n-1}$.

(iii) *La matriu* $\mathrm{ad}(A_2(f))$ *té entrades enteres, però pot no ser parella.*

(iv) *Les adjuntes de les matrius associades a f satisfan la relació*

$$\mathrm{ad}(A_2(f)) = 2^{n-1}\,\mathrm{ad}(A(f)).$$

(v) *Si n és parell, aplicant el lema anterior, tenim la relació*

$$\mathrm{ad}(A_2(f)) = A_2(2^{n-2}\,\mathrm{ad}(f)).$$ □

4.1.2 Formes quadràtiques sobre $\mathbb{Z}$

Ens restringim, a partir d'ara, a les formes quadràtiques de coeficients a $\mathbb{Z}$.

4.1.7 Definicions. El contingut d'una forma quadràtica f de coeficients a $\mathbb{Z}$ és el màxim comú divisor, de signe positiu, dels seus coeficients. El denotem per $\text{cont}(f)$. Una forma quadràtica f de coeficients a $\mathbb{Z}$ és primitiva si $\text{cont}(f) = 1$. Sobre les entrades de la matriu $A(f)$, equival a demanar que $\text{mcd}\{a_{ii}, 2a_{ij} \mid i, j, = 1, \ldots, n, i \neq j\} = 1$. □

4.1.8 Definició. Sigui f una forma quadràtica de n variables de coeficients a $\mathbb{Z}$. La forma polar de f, denotada per $\text{pol}(f)$, s'obté a partir de la forma $\text{ad}(f)$, multiplicant-la per 2^{n-1} i dividint-la pel màxim comú divisor, amb signe positiu, dels coeficients obtinguts; és a dir,

$$\text{pol}(f) := \frac{2^{n-1}\,\text{ad}(f)}{\text{cont}(2^{n-1}\,\text{ad}(f))}.\square$$

A partir de la forma adjunta, la forma polar queda determinada per les condicions de tenir els coeficients a $\mathbb{Z}$ i ser primitiva. Per a construir-la, es pot utilitzar tant la matriu $\text{ad}(A(f))$ com la matriu $\text{ad}(A_2(f))$, independentment de si n és o no parell.

4.1.9 Lema. *Sigui f una forma quadràtica de n variables, de coeficients a $\mathbb{Z}$. Posem $m = \text{cont}(f)$ i considerem $f' := \frac{1}{m}f$. Aleshores,*

(i) *f' és una forma primitiva.*

(ii) $\det_1(f) = m^n \det_1(f')$, $\det_2(f) = m^n \det_2(f')$.

(iii) $\text{ad}(f) = \text{ad}(mf') = m^{n-1}\,\text{ad}(f')$.

(iv) $\text{pol}(f) = \text{pol}(f')$. □

4.1.10 Proposició. *Sigui f una forma quadràtica de n variables sobre $\mathbb{Z}$ i sigui $N \in \mathbb{N}$. Són equivalents:*

(a) *N és l'enter positiu més petit tal que $NA_2(f)^{-1}$ és la matriu parella associada a una forma de coeficients enters.*

(b) *N és l'enter positiu més petit tal que $N\frac{1}{4}A(f)^{-1}$ és la matriu associada a una forma de coeficients enters.*

(c) *N satisfà que* $NA_2(f)^{-1} = (-1)^s A_2(\mathrm{pol}(f))$, *on* $s = 0$ *si* $\det_1(f) > 0$ *i* $s = 1$ *si* $\det_1(f) < 0$.

(d) *N satisfà que* $N\frac{1}{4}A(f)^{-1} = (-1)^s A(\mathrm{pol}(f))$, *on* $s = 0$ *si* $\det_1(f) > 0$ *i* $s = 1$ *si* $\det_1(f)f < 0$.

(e) $N = \dfrac{2^{n+1}|\det_1(f)|}{\mathrm{cont}(2^{n-1}\,\mathrm{ad}(f))}$.

El nombre N s'anomena el nivell de la forma quadràtica f i es denota per $\mathrm{N}(f)$. □

DEMOSTRACIÓ: Per a veure l'equivalència entre (a) i (b) i l'equivalència entre (c) i (d), només cal utilitzar la relació entre les matrius associades a una forma quadràtica qualsevol, $A_2(f) = 2A(f)$, $A_2(f)^{-1} = \frac{1}{2}A(f)^{-1}$.

L'equivalència entre (a) i (c), o bé entre (b) i (d), s'obté a partir de la definició de la forma polar, construïda a partir de la forma adjunta, determinada per les condicions que tingui coeficients enters i sigui primitiva, amb el signe que li correspon a partir de la forma adjunta. La condició de ser primitiva és precisament equivalent al fet que sigui l'enter més petit possible.

Finalment, vegem l'equivalència entre (d) i (e). Desenvolupem

$$\begin{aligned} N\tfrac{1}{4}A(f)^{-1} &= N\frac{1}{4}\frac{A(\mathrm{ad}(f))}{\det A(f)} = \\ &= N\frac{1}{4}\frac{m}{2^{n-1}\det A(f)}\frac{2^{n-1}A(\mathrm{ad}(f))}{m} = \\ &= N\frac{m}{2^{n+1}\det A(f)}A(\mathrm{pol}(f)), \end{aligned}$$

on $m = \mathrm{cont}(2^{n-1}\,\mathrm{ad}(f))$. Així, $N\frac{1}{4}A(f)^{-1} = \pm A(\mathrm{pol}(f))$ si, i només si, $N = \dfrac{2^{n+1}|\det(f)|}{\mathrm{mcd}(2^{n-1}\,\mathrm{ad}(f))}$. □

4.1.11 Remarca. La condició (a) és la definició que dóna Ogg [Ogg69] per a les formes definides positives d'un nombre parell de variables, a partir de la matriu parella. La condició (e) generalitza un càlcul de Lehman [Leh92] per a formes ternàries definides positives. □

4.1.12 Proposició. *Sigui f una forma quadràtica de n variables i coeficients enters. Aleshores,*

(i) $|\det_2(\mathrm{pol}(f))| = \dfrac{\mathrm{N}(f)^n}{|\det_2(f)|}$.

(ii) *Se satisfan les relacions* $\mathrm{N}(f)|2\det_2(f)$ *i* $\det_2(f)|\mathrm{N}(f)^n$*; per tant,* $\mathrm{N}(f)$ *i* $\det_2(f)$ *tenen els mateixos factors primers, excepte potser el* 2.

(iii) *Per a* $n = 2$, $\mathrm{N}(f) = |\det_2(f)|$ *si, i només si, la forma* f *és primitiva.*

(iv) $\mathrm{N}(\mathrm{pol}(f))|\mathrm{N}(f)$. *La igualtat es dóna si, i només si, la forma* f *és primitiva.*

DEMOSTRACIÓ: L'apartat (i) es dedueix de 4.1.10(c), en considerar determinants.

Provem (ii). Com que $\det_2(\mathrm{pol}(f))$ és enter, la segona relació de divisibilitat es dedueix directament de (i). Per a veure que $\mathrm{N}(f)|2\det_2(f)$, podem utilitzar també 4.1.10(c). Així,

$$\pm A_2(\mathrm{pol}(f)) = \mathrm{N}(f)A_2^{-1}(f) = \frac{\mathrm{N}(f)}{\det_2 A(f)}\,\mathrm{ad}(A_2(f)).$$

D'una banda, la matriu $\mathrm{ad}(A_2(f))$ té entrades enteres i correspon a una forma quadràtica de coeficients enters, i $\det_2(f)$ és un nombre enter. D'altra banda, $\pm A_2(\mathrm{pol}(f)) = \pm 2A(\mathrm{pol}(f))$ i $\mathrm{pol}(f)$ és una forma primitiva. Així, $2\det_2(f)/\mathrm{N}(f)$ és un enter, la qual cosa ens dóna la primera relació de divisibilitat.

Per a veure (iii), suposem $\det_2(f) > 0$, per tal de fixar el signe de la igualtat. Si utilitzem de nou 4.1.10(c), tenim que $A_2(\mathrm{pol}(f)) = \dfrac{\mathrm{N}(f)}{\det_2 A(f)}\,\mathrm{ad}(A_2(f))$. Per a les formes binàries se satisfà que $\mathrm{ad}\,A_2(f)) = A_2(\mathrm{ad}(f))$. Així, per a $n = 2$, tenim que $\mathrm{N}(f) = \det_2(f)$ si, i només si, la forma polar de f i la forma adjunta de f coincideixen, la qual cosa és equivalent al fet que la forma f sigui primitiva (cf. 4.1.15).

Finalment, vegem (iv). Podem suposar $\det_1(f) > 0$ per a simplificar notació, ja que les condicions de divisibilitat no depenen del signe. Si apliquem 4.1.10(b) i (d), tenim que

$$\mathrm{N}(\mathrm{pol}(f))\frac{1}{4}A(\mathrm{pol}(f))^{-1} = \mathrm{N}(\mathrm{pol}(f))\frac{1}{4}(\mathrm{N}(f)\frac{1}{4}A(f)^{-1})^{-1} = \frac{\mathrm{N}(\mathrm{pol}(f))}{\mathrm{N}(f)}A(f)$$

és la matriu d'una forma de coeficients enters primitiva. Com que la forma f té els coeficients a $\mathbb{Z}$, deduïm la relació de divisibilitat. A més, la igualtat correspon al fet que el resultat sigui la matriu $A(f)$, la qual cosa passa si, i només si, la forma f és primitiva. □

4.1.13 Remarca. Els resultats d'aquesta subsecció s'estenen fàcilment a formes quadràtiques sobre un domini R d'ideals principals.

4.1.3 Formes binàries, ternàries i quaternàries

En particular, estem interessats en les formes quadràtiques de $n = 2$, 3 o bé 4 variables, anomenades binàries, ternàries o bé quaternàries, respectivament. Precisem tot seguit algunes notacions, resultats i exemples.

4.1.14 Cas binari. Considerem una forma quadràtica binària de coeficients enters $f(X,Y) = aX^2 + bXY + cY^2$, que s'escriu $f = (a,b,c)$. Tenim que

$$A(f) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}, \qquad A_2(f) = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix},$$

$$A(\mathrm{ad}(f)) = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}, \quad \mathrm{ad}(A_2(f)) = \begin{pmatrix} 2c & -b \\ -b & 2a \end{pmatrix}.$$

4.1.15 Proposició. *Per a qualsevol forma quadràtica binària f sobre $\mathbb{Z}$, se satisfan les propietats:*

(i) $\det_1(f) = \det_1(\mathrm{ad}(f)) = ac - b^2/4$.

(ii) $\det_2(f) = \det_2(\mathrm{ad}(f)) = 4ac - b^2$, $-\det_2(f) \equiv 0, 1 \mod 4$.

(iii) $\mathrm{disc}_{\mathbb{Q}}(f) = \mathrm{disc}_{\mathbb{Q}}(\mathrm{ad}(f)) = 4ac - b^2$.

(iv) $\mathrm{ad}(A_2(f)) = A_2(\mathrm{ad}(f))$.

(v) $\mathrm{cont}(f) = \mathrm{cont}(\mathrm{ad}(f))$.

(vi) $\mathrm{pol}(f) = \dfrac{1}{\mathrm{cont}(f)}\mathrm{ad}(f) = \dfrac{1}{\mathrm{cont}(f)}(c, -b, a)$.

(vii) *f és primitiva si, i només si,* $\mathrm{pol}(f) = \mathrm{ad}(f)$.

(viii) $\mathrm{N}(f) = \dfrac{4|\det_1(f_2)|}{\mathrm{cont}(f_2)} = \dfrac{|\det_2(f_2)|}{\mathrm{cont}(f_2)}$. □

4.1.16 Cas ternari. Considerem una forma quadràtica ternària

$$f(X,Y,Z) = aX^2 + bY^2 + cZ^2 + a'YZ + b'XZ + c'XY, \quad a,b,c,a',b',c' \in \mathbb{Z}.$$

També s'utilitza la notació (cf. [Gau1801])

$$f = \begin{pmatrix} a & b & c \\ a'/2 & b'/2 & c'/2 \end{pmatrix}.$$

Tenim que

$$A(f) = \begin{pmatrix} a & c'/2 & b'/2 \\ c'/2 & b & a'/2 \\ b'/2 & a'/2 & c \end{pmatrix}, \quad A_2(f) = \begin{pmatrix} 2a & c' & b' \\ c' & 2b & a' \\ b' & a' & 2c \end{pmatrix},$$

$$\det_1(f) = abc + \tfrac{1}{4}(a'b'c' + a(a')^2 + b(b')^2 + c(c')^2).$$

4.1.17 Exemple. Considerem una forma ternària concreta:

$$f = X^2 + Y^2 - XZ, \qquad \mathrm{ad}(f) = -\tfrac{1}{4}Y^2 + Z^2 + XZ,$$

$$f = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1/2 & 0 \end{pmatrix}, \qquad \mathrm{ad}(f) = \begin{pmatrix} 0 & -1/4 & 1 \\ 0 & 1/2 & 0 \end{pmatrix},$$

$$A(f) = \begin{pmatrix} 1 & 0 & -1/2 \\ 0 & 1 & 0 \\ -1/2 & 0 & 0 \end{pmatrix}, \quad A(\mathrm{ad}(f)) = \begin{pmatrix} 0 & 0 & 1/2 \\ 0 & -1/4 & 0 \\ 1/2 & 0 & 1 \end{pmatrix}.$$

No té sentit pensar en la matriu parella associada a $\mathrm{ad}(f)$, perquè aquesta no té coeficients enters. Notem que, si considerem la matriu parella de f, la seva matriu adjunta no és una matriu parella:

$$A_2(f) = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad \mathrm{ad}(A_2(f)) = \begin{pmatrix} 0 & 0 & 2 \\ 0 & -1 & 0 \\ 2 & 0 & 4 \end{pmatrix}.$$

En aquest exemple tenim:

(i) $\det_1(f) = -\frac{1}{4}$, $\det_2(f) = -2$ i $\mathrm{disc}_{\mathbb{Q}}(f) = -1$.

(ii) $\det_1(\mathrm{ad}(f)) = \frac{1}{16}$ i $\mathrm{disc}_{\mathbb{Q}}(\mathrm{ad}(f)) = 1$.

(iii) $\mathrm{ad}(A_2(f)) = 2^2 A(\mathrm{ad}(f))$.

(iv) $\mathrm{pol}(f) = -Y^2 + 4Z^2 + 4XZ$.

(v) $\mathrm{N}(f) = 2^2$. □

4.1.18 Cas quaternari. Considerem una forma quadràtica quaternària de coeficients enters

$$f(X,Y,Z,T) = aX^2+bY^2+cZ^2+dT^2+b'XY+c'XZ+d'XT+d''YZ+ \\ +c''YT+b''ZT.$$

S'utilitza també la notació (cf. [Bra24])

$$\begin{array}{|ccc|}\hline & b' & c' & d' \\ a & b & c & d \\ & b'' & c'' & d'' \\ \hline\end{array}.$$

Tenim que

$$A(f) = \begin{pmatrix} a & b'/2 & c'/2 & d'/2 \\ b'/2 & b & d''/2 & c''/2 \\ c'/2 & d''/2 & c & b''/2 \\ d'/2 & c''/2 & b''/2 & d \end{pmatrix}, \quad A_2(f) = \begin{pmatrix} 2a & b' & c' & d' \\ b' & 2b & d'' & c'' \\ c' & d'' & 2c & b'' \\ d' & c'' & b'' & 2d \end{pmatrix}.$$

4.1.19 Exemple. Considerem una forma quaternària concreta:

$$\begin{aligned} f(X,Y,Z,T) &= X^2-2Y^2+T^2+XZ-2YT \\ \mathrm{ad}(f)(X,Y,Z,T) &= -\tfrac{1}{4}Y^2-3Z^2+\tfrac{1}{2}T^2+3XZ-\tfrac{1}{2}YT, \end{aligned}$$

$$f = \begin{array}{|cccc|}\hline & 0 & 1/2 & 0 \\ 1 & -2 & 0 & 1 \\ & 0 & -1 & 0 \\ \hline\end{array}, \qquad \mathrm{ad}(f) = \begin{array}{|cccc|}\hline & 0 & 3/2 & 0 \\ 0 & -1/4 & -3 & 1/2 \\ & 0 & -1/4 & 0 \\ \hline\end{array},$$

$$A(f) = \begin{pmatrix} 1 & 0 & 1/2 & 0 \\ 0 & -2 & 0 & -1 \\ 1/2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \quad A_2(f) = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & -4 & 0 & -2 \\ 1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 2 \end{pmatrix},$$

$$A(\mathrm{ad}(f)) = \begin{pmatrix} 0 & 0 & 3/2 & 0 \\ 0 & -1/4 & 0 & -1/4 \\ 3/2 & 0 & -3 & 0 \\ 0 & -1/4 & 0 & 1/2 \end{pmatrix},$$

$$\mathrm{ad}(A_2(f)) = \begin{pmatrix} 0 & 0 & 12 & 0 \\ 0 & -2 & 0 & -2 \\ 12 & 0 & -24 & 0 \\ 0 & -2 & 0 & 4 \end{pmatrix}.$$

En aquest cas tenim que:

(i) $\det_1(f) = \frac{3}{4}$, $\det_2(f) = 12$ i $\mathrm{disc}_{\mathbb{Q}}(f) = 3$.

(ii) $\det_1(\mathrm{ad}(f)) = \frac{3^3}{4^3}$ i $\mathrm{disc}_{\mathbb{Q}}(\mathrm{ad}(f)) = 3$.

(iii) $\mathrm{ad}(A_2(f)) = 2^3 A(\mathrm{ad}(f))$ és una matriu parella; de fet, més concretament, $\mathrm{ad}(A_2(f)) = A_2(2^2\,\mathrm{ad}(f))$.

(iv) $\mathrm{pol}(f) = -Y^2 - 12Z^2 + 2T^2 + 12XZ - 2YT$.

(v) $\mathrm{N}(f) = 12$. □

4.2 Representació de formes per formes

En aquesta secció precisem les definicions referents a la representació de nombres i formes quadràtiques per formes quadràtiques que utilitzarem en els capítols posteriors. Hi ha nombroses referències on es poden consultar els resultats clàssics, referits majoritàriament a la representació de nombres per formes i a l'equivalència de formes. Citem, per exemple, [Sie35], [BS66], [Ser73], i [Are87].

4.2.1 Definició. Siguin f i g formes quadràtiques sobre un anell R de n i r variables, respectivament, amb $r \leq n$. Es diu que f representa g sobre R si existeix una matriu $P \in \mathrm{M}(n \times r, R)$ de rang r tal que $P^t A(f) P = A(g)$. Ho denotem per $f \xrightarrow{R} g$. □

En particular, per al cas de $r = 1$, una forma f representa un element $\alpha \in R$, sobre R, si existeixen elements $\alpha_1, \ldots, \alpha_n \in R$ no tots nuls, tals que $f(\alpha_1, \ldots, \alpha_n) = \alpha$; és a dir, existeix una matriu $P = (\alpha_i) \in \mathrm{M}(n \times 1, R)$, de rang 1, tal que $P^t A(f) P = \alpha$. Ho denotem per $f \xrightarrow{R} \alpha$.

4.2.2 Definició. Es diu que una forma quadràtica f és R-isòtropa si representa el 0 sobre R. En cas contrari, es diu que la forma quadràtica és R-anisòtropa. □

Si R és un anell i K és el cos de fraccions de R, una forma quadràtica és isòtropa sobre R si, i només si, ho és sobre K. Destaquem el resultat següent sobre la relació entre formes isòtropes i la representació d'un element qualsevol.

4.2.3 Proposició. *Sigui f una forma quadràtica sobre K regular. Si f és K-isòtropa, aleshores f representa qualsevol element $\alpha \in K$.*

4.2.4 Definició. Sigui $\Gamma \subseteq \mathrm{GL}(n,R)$ un grup de matrius. Dues formes quadràtiques f i g direm que són Γ-equivalents si existeix una matriu $\gamma \in \Gamma$ tal que $A(g) = \gamma^t A(f)\gamma$. Ho denotem per $f \overset{\Gamma}{\sim} f'$. Per alleugerir la notació, si $\Gamma = \mathrm{GL}(n,R)$, ho denotem, també, per $f \overset{R}{\sim} f'$. □

4.2.5 Remarca. Siguin f i g dues formes quadràtiques sobre R del mateix nombre de variables. Sigui $\Gamma \subseteq \mathrm{GL}(n,R)$. És clar que, amb les definicions anteriors, es té que:

(i) Si $f \overset{\Gamma}{\to} g$, aleshores $f \overset{K}{\sim} g$.

(ii) $f \overset{\Gamma}{\sim} g$ si, i només si, $f \overset{\Gamma}{\to} g$ i $g \overset{\Gamma}{\to} f$.

(iii) Si $f \overset{\Gamma}{\sim} g$, aleshores $\operatorname{rang} A(f) = \operatorname{rang} A(g)$. □

Sigui $f \overset{\Gamma}{\sim} f'$, donada per $\gamma \in \Gamma$. Si $\Gamma = \mathrm{GL}(n,K)$, aleshores γ representa un canvi de variables K-lineal invertible, per la qual cosa es parla també d'equivalència racional sobre K. Si $\Gamma \subseteq \mathrm{GL}(n,\mathbb{Z})$, se satisfà $\det\gamma = \pm 1$. Si $\det\gamma = 1$, l'equivalència es diu que és pròpia; per al cas $\det\gamma = -1$, es diu que és impròpia.

4.2.6 Remarca. Sigui f una forma quadràtica binària sobre $\mathbb{Z}$. Aleshores, les formes f i $\mathrm{ad}(f)$ són sempre $\mathrm{SL}(2,\mathbb{Z})$-equivalents. Només cal considerar $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, que és un dels generadors estàndards del grup $\mathrm{SL}(2,\mathbb{Z})$. □

4.2.7 Remarca. Siguin f i f' dues formes quadràtiques de n variables regulars sobre R.

Si $f \overset{\Gamma}{\sim} f'$, aleshores:

(i) $\det_1(f') = \det_1(f)(\det\gamma)^2$, on $\gamma \in \Gamma$ és tal que $A(f') = \gamma^t A(f)\gamma$.

(ii) $\mathrm{disc}_K(f') = \mathrm{disc}_K(f)$.

(iii) $\det_1(f') = \det_1(f)$, si $R = \mathbb{Z}$.

Si $f \overset{R}{\to} f'$, aleshores:

(i) $\det_1(f') = \det_1(f)(\det\gamma)^2$, on $\gamma \in \Gamma$ és tal que $A(f') = \gamma^t A(f)\gamma$.

(ii) $\mathrm{disc}_K(f') = \mathrm{disc}_K(f)$.

(iii) $\det_1(f) | \det_1(f')$, si $R = \mathbb{Z}$. □

D'entrada, això ja indica que, si K és un cos de nombres, el nombre de classes de K-equivalència de formes quadràtiques és infinit. Per aquest motiu, s'estudien les classes de K-equivalència per a un determinant fixat.

4.2.8 Exemple. Sigui la forma quadràtica binària $f(X,Y) = X^2 + XY - Y^2$. Considerant la matriu $\gamma = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$, obtenim la forma diagonal $f'(X,Y) = X'^2 - 5Y'^2$. Tenim que $\det\gamma = 2$; per tant, $\gamma \in \mathrm{GL}(2,\mathbb{Q})$, però $\gamma \notin \mathrm{GL}(2,\mathbb{Z})$. Així, $f \overset{\mathbb{Z}}{\to} f'$ i $f \overset{\mathbb{Q}}{\sim} f'$, és a dir, f i f' són $\mathbb{Q}$-equivalents, però no són $\mathbb{Z}$-equivalents. □

4.2.9 Notació. Sigui f una forma quadràtica de coeficients enters. Denotem, com és habitual, $\varepsilon_p(f)$ l'invariant de Hasse-Witt local de f. Posem:

$$S_1(f) := \{p : f_p \text{ és } \mathbb{Q}_p\text{-anisòtropa}\},$$
$$S_2(f) := \{v : \varepsilon_v(f_v) = -1\}. \square$$

4.2.10 Lema. *Siguin f i f' dues formes quadràtiques de coeficients enters. Si $f \overset{\mathbb{Q}}{\sim} f'$, aleshores $S_1(f) = S_1(f')$ i $S_2(f) = S_2(f')$.* □

4.2.11 Cas binari-ternari. Siguin f_3 i f_2 una forma quadràtica ternària i una de binària, respectivament, sobre $\mathbb{Z}$. Si $f_3 \overset{\mathbb{Z}}{\to} f_2$, aleshores $\mathrm{ad}(f_3) \overset{\mathbb{Z}}{\to} \det_1(f_2)$. Aquesta representació s'obté a partir dels menors de la matriu P de la representació de f_2 per f_3. S'anomena la representació adjunta de $f_3 \overset{\mathbb{Z}}{\to} f_2$.

A la inversa, totes les representacions d'un nombre d per una forma ternària f_3 provenen d'una representació d'una forma binària f_2' amb $\det_1(f_2') = d$ per una forma ternària f_3' amb $\mathrm{ad}(f_3') = f_3$. A més, aquestes representacions caracteritzen la classe d'equivalència de les formes binàries (cf. [Gau1801]). La construcció de la representació adjunta justifica la definició de representació primitiva d'una forma quadràtica per una altra, que donarem tot seguit. □

4.2.12 Definició. Suposem que R és un domini d'ideals principals. Siguin f i g formes quadràtiques sobre R de n i r variables, respectivament, amb $r \leq n$, tal que f representa g sobre R amb matriu P; és a dir, $P \in \mathrm{M}(n \times r, R)$ satisfà que $P^t A(f) P = A(g)$. Diem que la representació donada per P és

primitiva si el màxim comú divisor dels menors $r \times r$ de la matriu P és 1. Diem que f representa primitivament g sobre R si existeix almenys una representació primitiva P de g per f.

En particular, si f és una forma quadràtica sobre R i $\alpha \in R$, $f(\alpha_1, \ldots, \alpha_n) = \alpha$ és una representació primitiva de α per la forma quadràtica f sobre R si, i només si, $\mathrm{mcd}(\alpha_1, \ldots, \alpha_n) = 1$. □

4.2.13 Exemple. Considerem la forma quadràtica $f(X,Y,Z) = -aX^2 - bY^2 + abZ^2$, $a, b \in \mathbb{Z}$. És clar que la forma f representa primitivament les formes binàries diagonals $g_1(X,Y) = -aX^2 - bY^2$, $g_2(X,Y) = -bX^2 + abY^2$, $g_3(X,Y) = -aX^2 + abY^2$. Representa també primitivament altres formes binàries no diagonals, com ara $g_4(X,Y) = (a(b-1), 2ab, b(a-1))$ i $g_5(X,Y) = (-a-b+9ab, -4b+6ab, -4b+ab)$. La matriu $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \\ 3 & 1 \end{smallmatrix}\right)$ és una representació no primitiva de $g_6(X,Y) = (-a+9ab, 6ab, -4b+ab)$ per f. Aquestes representacions donen explícitament representacions $\mathrm{ad}(f) \xrightarrow{R} d_i$, amb $d_i = \det_1 g_i$. Per exemple, si $a = p$ i $b = -1$, a partir de la representació de g_5 obtenim una representació primitiva del nombre $p(p-29)$ per $\mathrm{ad}(f) = -pX^2 + p^2Y^2 - pZ^2$, donada per $(5,1,2)$. □

4.2.14 Notació. Siguin f i g formes quadràtiques sobre R. A partir de les definicions sobre representació de formes quadràtiques, considerem els conjunts següents:

$$\mathcal{R}(f,g;R) = \{P : P \in \mathrm{M}_{n\times r}(R), \mathrm{rang} P = r, P^tA(f)P = A(g)\},$$

$$\mathcal{R}^*(f,g;R) = \{P : P \in \mathcal{R}(f,g;R),\ P \text{ primitiva}\},\ \text{si } R \text{ és DIP},$$

$$\mathcal{D}(f;R) = \{\alpha \in R : \mathcal{R}(f,\alpha;R) \neq \emptyset\}.$$

Sigui $\Gamma \subseteq \mathrm{GL}(n,\mathbb{R})$. Per a una forma quadràtica f de n variables sobre R , el grup de Γ-isotropia de f és

$$\mathbf{O}(f;\Gamma) := \{\gamma \in \Gamma : \gamma^t A(f)\gamma = A(f)\}.$$

Si $R \subseteq \mathbb{R}$, posem $\mathbf{O}^+(f;\Gamma) = \{\gamma \in \mathbf{O}(f;\Gamma) \mid \det\gamma > 0\}$. □

Notem que en el cas de $R = \mathbb{Z}$, tenim que $\mathbf{O}^+(f;\Gamma) \subseteq \mathrm{SL}(n,\mathbb{Z})$, on n és el nombre de variables de f. Siguin $\alpha \in \mathcal{D}(f;R)$ i $(\alpha_1, \ldots, \alpha_n)$ una representació de α per f sobre R. Si $\gamma \in \mathbf{O}^+(f;\Gamma)$, aleshores $(\alpha'_1, \ldots, \alpha'_n) = \gamma^{-1}(\alpha_1, \ldots, \alpha_n)$ també és una representació de α per f sobre R. Això dóna peu a definir la relació d'equivalència següent.

4.2.15 Definició. Dues representacions $P, P' \in \mathcal{R}(f, g; R)$ direm que són Γ-equivalents si existeix $\gamma \in \mathbf{O}(f, \Gamma)$ tal que $P = \gamma P'$. En particular, dues representacions $(\alpha_1, \ldots, \alpha_n), (\alpha'_1, \ldots, \alpha'_n)$ pertanyents a $\mathcal{R}(f, \alpha; R)$ són Γ-equivalents si, i només si, existeix $\gamma \in \mathbf{O}(f, \Gamma)$ tal que $(\alpha_1, \ldots, \alpha_n) = \gamma(\alpha'_1, \ldots, \alpha'_n)$. □

4.2.16 Remarca. (i) Si $f \overset{\mathrm{SL}(n,R)}{\sim} f'$, aleshores $\mathcal{D}(f; R) = \mathcal{D}(f'; R)$.

(ii) $\alpha \in \mathcal{D}(f; K)$ si, i només si, $\alpha\beta^2 \in \mathcal{D}(f; K)$. Així, per al cas d'un cos, és suficient estudiar les representacions dels elements de K^*/K^{*2}. □

El resultat següent, degut essencialment a Hermite, cf. [Jon67], permet definir, de forma recurrent, el concepte de forma $\mathrm{SL}(n, \mathbb{Z})$-reduïda per a formes quadràtiques de n variables.

4.2.17 Teorema. *Sigui g una forma quadràtica regular de n variables de coeficients a $\mathbb{Q}$. Suposem que g és anisòtropa sobre $\mathbb{Z}$. Aleshores, existeix una forma $f = \sum c_{ij} X_i X_j$ que és $\mathrm{SL}(n, \mathbb{Z})$-equivalent a g i satisfà que*

(i) $0 < |c_{11}| \leq \left(\frac{4}{3}\right)^{(n-1)/2} \sqrt[n]{|\det_1(f)|}$,

(ii) $|c_{11}| \geq 2|c_{1j}|$, *per a* $j > 1$,

(iii) $c_{11} f - (c_{11} X_1 + c_{12} X_2 + \cdots + c_{1n} X_n)^2 = f_1$,

on f_1 és una forma quadràtica de $n-1$ variables que satisfà, amb n canviat per $n-1$, les condicions imposades a f. El determinant de f_1 és $c_{11}^{n-2} \det_2(f)$. □

4.2.18 Definició. Una forma quadràtica s'anomena forma $\mathrm{SL}(n, \mathbb{Z})$-reduïda si satisfà les condicions (i),(ii) i (iii) de la proposició anterior. □

Fixades dues formes quadràtiques de n variables sobre R, f, g, i un subgrup $\Gamma \subseteq \mathrm{GL}(n, \mathbb{R})$, podem considerar el conjunt de Γ-classes de representacions. Habitualment hom pensa, de manera implícita, en $\Gamma = \mathrm{SL}(n, \mathbb{Z})$, però en el capítol 7 obtindrem resultats en aquest sentit més ampli.

4.3 Formes quadràtiques de 1a i 2a espècie

En aquesta secció presentem una altra manera de treballar amb formes quadràtiques, assignant a cada forma una espècie. Introduïm també els conceptes de forma recíproca i de K-forma. D'aquesta manera generalitzem conceptes considerats per Brandt [Bra24] per a formes quadràtiques quaternàries. Durant tota la secció ens referirem a formes quadràtiques racionals, és a dir, a formes quadràtiques sobre $\mathbb{Q}$.

4.3.1 Definició. Anomenem forma quadràtica d'espècie σ, amb $\sigma = 1, 2$, la parella $(f, (c_{ij}))$, on f és una forma quadràtica de coeficients a $\mathbb{Q}$ que s'escriu

$$f = \frac{1}{\sigma} \sum_{i,j} c_{ij} X_i X_j.$$

Si $\sigma = 1$, es diu que $(f, (c_{ij}))$ és de primera espècie; si $\sigma = 2$, es diu que $(f, (c_{ij}))$ és de segona espècie. □

4.3.2 Remarca. Sigui $(f, (c_{ij}))$ una forma d'espècie σ. La relació entre les dues matrius associades a f i les dues espècies està donada per:

(a) Fixada la forma f, tenim que $(c_{ij}) = \begin{cases} A(f) & \text{si } \sigma = 1, \\ A_2(f) & \text{si } \sigma = 2. \end{cases}$

(b) Fixada la matriu $(c_{ij}) = A(g)$, tenim que $g = \begin{cases} f & \text{si } \sigma = 1, \\ 2f & \text{si } \sigma = 2. \end{cases}$ □

4.3.3 Lema. *Se satisfà:*

(i) $A(2f) = A_2(f)$.

(ii) $\mathrm{ad}(2f) = 2^{n-1} \mathrm{ad}(f)$.

(iii) $\mathrm{pol}(2f) = \mathrm{pol}(f)$.

DEMOSTRACIÓ: L'apartat (i) és trivial.

Calculem la matriu adjunta a partir de la relació de (i). Com que $\mathrm{ad}(A_2(f)) = 2^{n-1} \mathrm{ad}(A(f))$, la igualtat que s'obté sobre les formes quadràtiques és directament (ii).

Per a veure (iii), recordem que la forma $\mathrm{pol}(f)$ és una forma múltiple de la forma adjunta, determinada per les propietats de tenir coeficients enters i ser primitiva. Per (ii), les formes adjuntes de f i $2f$ són l'una múltiple de l'altra; per tant, la polar que els correspon és la mateixa. □

Els coeficients de la forma s'anomenen coeficients centrals si acompanyen els termes X_i^2 i coeficients laterals si acompanyen els termes mixtos X_iX_j. Per a una forma $(f,(c_{ij}))$, els coeficients centrals són $a_{ii} = \dfrac{1}{\sigma}c_{ii}$ i els coeficients laterals són $2a_{ij} = \dfrac{2}{\sigma}c_{ij}$, $i \neq j$.

Donada una parella $(f,(c_{ij}))$ d'espècie σ, considerem els determinants:

$$\det(c_{ij}) \quad \text{i} \quad \Delta(f) := \det\left(\frac{\partial^2 f}{\partial X_i \partial X_j}\right).$$

4.3.4 Lema. *Se satisfà:*

(i) $\det(c_{ij}) = \det(\sigma A(f)) = \det_\sigma(f) = \det_1(\sigma f)$.

(ii) $\left(\dfrac{\partial^2 f}{\partial X_i \partial X_j}\right) = A_2(f)$.

(iii) $\Delta(f) = \det_2(f) = \det_1(2f)$.

DEMOSTRACIÓ: Si $(f,(c_{ij}))$ és de primera espècie, tenim $(c_{ij}) = A(f)$; per tant, $\det(c_{ij}) = \det A(f) = \det_1(f)$. Si $(f,(c_{ij}))$ és de segona espècie, tenim $(c_{ij}) = A_2(f)$; per tant, $\det(c_{ij}) = \det A_2(f) = \det 2A(f) = \det_1 2f$. En ambdós casos el determinant coincideix amb $\det(\sigma A(f))$. Això demostra (i).

Per a provar (ii), calculem

$$\frac{\partial^2 f}{\partial X_i \partial X_j} = \frac{1}{\sigma}\frac{\partial}{\partial X_i}\left(2c_{jj}X_j + \sum_{k\neq j} c_{kj}X_k\right) = \begin{cases} \dfrac{1}{\sigma}c_{ij} = a_{ij} & \text{si } i \neq j, \\ \dfrac{2}{\sigma}c_{ii} = 2a_{ii} & \text{si } i = j. \end{cases}$$

Per tant, de forma independent a l'espècie obtenim la igualtat de matrius $\left(\dfrac{\partial^2 f}{\partial X_i \partial X_j}\right) = A_2(f)$.

L'apartat (iii) és conseqüència directa de (ii). □

A partir dels lemes i la remarca anteriors podem observar que el fet de treballar amb les dues espècies és equivalent a treballar amb les dues matrius associades a f, o amb les dues formes f i $2f$.

4.3.5 Definició. Suposem que f és una forma quadràtica tal que $\det_\sigma(f)$ és un quadrat perfecte. Posem $\mathrm{d}_\sigma(f) = +\sqrt{\det_\sigma(f)}$ si la forma quadràtica és definida positiva i $\mathrm{d}_\sigma(f) = -\sqrt{\det_\sigma(f)}$ si la forma quadràtica és indefinida; no considerarem formes quadràtiques definides negatives. □

4.3.6 Remarca. Observem que, si n és parell, $\mathrm{d}_2(f) = 2^{n/2}\,\mathrm{d}_1(f)$, ja que $\det_2(f) = 2^n \det_1(f)$. Així, si n és parell, és indiferent demanar la condició que el determinant sigui un quadrat en una o altra espècie. Si n és senar, cal fixar en quina espècie exigim la condició; no es pot treballar de la mateixa manera en f o $2f$, ni simultàniament en les dues matrius associades. En aquests casos, especialment quan $n = 3$, ens restringirem a la primera espècie. □

A continuació definim el concepte de forma σ-recíproca per a formes quadràtiques f de n variables tals que $\det_\sigma(f)$ sigui un quadrat perfecte. Per a n parell, considerarem $\sigma = 1, 2$, i veurem la relació que hi ha entre les dues formes recíproques associades; per a n senar fixem $\sigma = 1$.

4.3.7 Definició. Sigui $f = \frac{1}{\sigma}\sum_{i,j} c_{ij}X_iX_j$ una forma quadràtica d'espècie σ, de coeficients a $\mathbb{Q}$, tal que $\det_\sigma(f)$ sigui un quadrat perfecte. La forma quadràtica

$$\mathrm{rec}_\sigma(f) = \frac{1}{\sigma}\sum_{i,j} t_{ij}X_iX_j, \quad \text{on } t_{ij} = \frac{1}{d_\sigma(f)}\,\frac{\partial \det_\sigma(f)}{\partial c_{ij}},$$

s'anomena la forma σ-recíproca de f. □

La proposició següent relaciona la forma σ-recíproca amb la forma adjunta.

4.3.8 Proposició. *Sigui f una forma quadràtica sobre $\mathbb{Q}$ de n variables tal que $\det_\sigma(f)$ sigui un quadrat perfecte. Aleshores,*

$$\text{(i)}\ \left(\frac{\partial \det_\sigma(f)}{\partial c_{ij}}\right) = A(\mathrm{ad}(\sigma f)) = \begin{cases} \mathrm{ad}(A(f)) & \text{si } \sigma = 1, \\ \mathrm{ad}(A_2(f)) & \text{si } \sigma = 2. \end{cases}$$

$$\text{(ii)}\quad \mathrm{rec}_\sigma(f) = \begin{cases} \dfrac{1}{\mathrm{d}_1}\,\mathrm{ad}(f) & si\ \sigma = 1, \\ \dfrac{1}{\mathrm{d}_2}\,\mathrm{ad}(2f) & si\ \sigma = 2. \end{cases}$$

$$\text{(iii)}\quad A(\mathrm{rec}_\sigma(f)) = \begin{cases} \dfrac{1}{\mathrm{d}_1}\,\mathrm{ad}(A(f)) & si\ \sigma = 1, \\ \dfrac{1}{\mathrm{d}_2}\,\mathrm{ad}(A(2f)) = \dfrac{1}{\mathrm{d}_2}\,\mathrm{ad}(A_2(f)) & si\ \sigma = 2. \end{cases}$$

(iv) $\det(\mathrm{rec}_\sigma(f)) = (\mathrm{d}_\sigma(f))^{n-2}$. *En particular, tenim que* $\det(\mathrm{rec}_\sigma(f)) = \det_\sigma(f)$ *per a* $n = 4$.

DEMOSTRACIÓ: Posem $B = (b_{ij}) = \left(\dfrac{\partial \det_\sigma(f)}{\partial c_{ij}}\right)$. Calculem b_{ij}.

Si desenvolupem el determinant $\det_\sigma(f) = \det(c_{ij})$ per la fila i, obtenim que:

$$\det(c_{ij}) = (-1)^{i+1}c_{i1}C_{i1} + \cdots + (-1)^{i+j}c_{ij}C_{ij} + \cdots + (-1)^{i+n}c_{in}C_{in},$$

on C_{ij} denota el menor obtingut en suprimir la fila i i la columna j. Per a obtenir b_{ij}, derivem l'expressió anterior respecte de c_{ij}; obtenim que $b_{ij} = (-1)^{i+j}C_{ij}$, que és justament l'adjunt a c_{ij} en el sentit habitual. Així, tenim les igualtats de matrius $(b_{ij}) = \mathrm{ad}(c_{ij}) = \mathrm{ad}(A(\sigma f))$. Finalment, recordem que $\mathrm{ad}(A(\sigma f)) = A(\mathrm{ad}(\sigma f))$. En particular, per a cada espècie σ s'obtenen les matrius indicades; per a $\sigma = 2$, apliquem 4.3.3(ii). Això demostra (i).

Els apartats (ii) i (iii) són conseqüència de (i), afegint el factor $\dfrac{1}{\mathrm{d}_\sigma(f)}$ per tal d'obtenir la forma σ-recíproca. L'apartat (ii) expressa el resultat per a les formes, i l'apartat (iii), per a les matrius associades a les formes.

Per a veure (iv), desenvolupem

$$\det_1(\mathrm{rec}_\sigma(f)) = \frac{1}{\mathrm{d}_\sigma^n}\det_1 \mathrm{ad}(\sigma f) = \frac{1}{\mathrm{d}_\sigma^n}\det_1(\sigma f)^{n-1} = \frac{1}{\mathrm{d}_\sigma^n}(\mathrm{d}_\sigma^2)^{n-1} = \mathrm{d}_\sigma^{n-2}\,.\ \square$$

Obtenim directament el corol·lari següent, per a les formes d'un nombre parell de variables.

4.3.9 Corol·lari. *Sigui* f *una forma quadràtica sobre* $\mathbb{Q}$ *d'un nombre parell de variables* n, *tal que* $\det_1(f)$ *sigui un quadrat perfecte. Aleshores,* $\mathrm{rec}_2(f) = 2^{n/2-1}\,\mathrm{rec}_1(f)$.

DEMOSTRACIÓ: S'obté directament a partir de l'apartat (ii) de la proposició anterior, utilitzant la relació entre les matrius adjuntes de f i $2f$, explicitada en 4.3.3 i la relació entre $\mathrm{d}_1(f)$ i $\mathrm{d}_2(f)$ de la remarca anterior. Notem que la condició n parell és necessària perquè $\mathrm{d}_1(f)$ i $\mathrm{d}_2(f)$ tinguin sentit simultàniament. □

Per a les formes quadràtiques binàries, les dues formes recíproques associades coincideixen, per la qual cosa el valor de σ és indiferent. Per a les ternàries, hem fixat $\sigma = 1$. Per a les formes quadràtiques quaternàries, tenim que $\mathrm{rec}_2(f) = 2\,\mathrm{rec}_1(f)$, i cal especificar en quina espècie es treballa. En general, mantindrem, doncs, la notació amb subíndex σ per tal d'evitar imprecisions.

4.3.10 Definició. Sigui f una forma quadràtica de coeficients a $\mathbb{Z}$ i $\det_\sigma(f)$ igual a un quadrat. Es diu que f és una K_σ-forma si $\mathrm{rec}_\sigma(f)$ també és de coeficients enters. □

El resultat següent relaciona la forma recíproca amb la forma polar definida en la primera secció i dóna condicions necessàries i/o suficients per a que una forma sigui K_σ-forma.

4.3.11 Lema. *Sigui f una forma quadràtica de n variables de coeficients enters tal que $\det_\sigma(f)$ sigui un quadrat. Aleshores, f és una K_σ-forma si, i només si, $\mathrm{rec}_\sigma(f) = \lambda\,\mathrm{pol}(f)$, per a algun $\lambda \in \mathbb{Z}$.*

DEMOSTRACIÓ: D'una banda, la forma polar es defineix a partir de la forma adjunta, multiplicant-la per un factor de manera que s'obtingui una forma de coeficients enters i primitiva. D'altra banda, per la proposició 4.3.8 (ii), la forma recíproca és també un múltiple de la forma adjunta, $\mathrm{rec}_\sigma(f) = \dfrac{1}{d_\sigma}\,\mathrm{ad}(\sigma f)$. El fet de ser una K_σ-forma correspon, per definició, al fet que $\mathrm{rec}_\sigma(f)$ tingui coeficients enters.

Atès que tant la forma σ-recíproca com la forma polar provenen de la forma adjunta, que les dues formes són de coeficients enters i que la forma polar és primitiva, obtenim la relació

$$\mathrm{rec}_\sigma(f) = \lambda\,\mathrm{pol}(f) \qquad \text{per a cert } \lambda \in \mathbb{Z}.$$

A la inversa, si tenim aquesta relació, forçosament f és una K_σ-forma, ja que la forma σ-recíproca té coeficients enters en ser un múltiple enter de la forma polar. □

4.3.12 Proposició. *Sigui f una forma quadràtica de n variables de coeficients enters tal que $\det_\sigma(f)$ sigui un quadrat. Sigui $\mathrm{N}(f)$ el seu nivell. Aleshores:*

(i) *f és una K_1-forma si, i només si, $4\,\mathrm{d}_1(f)$ és enter i $\mathrm{N}(f)|4\,\mathrm{d}_1(f)$.*

(ii) *f és una K_2-forma si, i només si, $\mathrm{N}(f)|2\,\mathrm{d}_2(f)$.*

(iii) *$\mathrm{N}(f) = 4\,\mathrm{d}_1(f)$ si, i només si, $\mathrm{pol}(f) = \pm\,\mathrm{rec}_1(f)$.*

(iv) *$\mathrm{N}(f) = 2\,\mathrm{d}_2(f)$ si, i només si, $\mathrm{pol}(f) = \pm\,\mathrm{rec}_2(f)$. En aquest cas, $4|\,\mathrm{N}(f)$.*

(v) *Suposem que n és parell. Si f és una K_1-forma, aleshores f és una K_2-forma.*

(vi) *Si $n = 2$, aleshores f és una K_1-forma si, i només si, f és una K_2-forma.*

(vii) *Si $n = 4$, aleshores f és una K_1-forma si, i només si, $\mathrm{N}(f)|\,\mathrm{d}_2(f)$.*

DEMOSTRACIÓ: Utilitzem 4.3.8 per a la relació entre les matrius associades a la forma recíproca i a la forma adjunta. Explicitem la relació, donada a 4.1.10, entre les matrius associades a la forma polar i a la forma adjunta en funció del nivell de f:

$$A(\mathrm{pol}(f)) = \frac{\mathrm{N}(f)}{4\det_1(f)} A(\mathrm{ad}(f)), \qquad A_2(\mathrm{pol}(f)) = \frac{\mathrm{N}(f)}{\det_2(f)}\,\mathrm{ad}(A_2(f)).$$

Si $\sigma = 1$, com que $\det_1(f) = \mathrm{d}_1^2(f)$, pel lema anterior tenim que f és una K_1-forma si, i només si, existeix $\lambda \in \mathbb{Z}$ tal que

$$\frac{1}{\mathrm{d}_1(f)}\,\mathrm{ad}(f) = \lambda \frac{\mathrm{N}(f)}{4\,\mathrm{d}_1^2(f)}\,\mathrm{ad}(f).$$

Això és clarament equivalent al fet que $4\,\mathrm{d}_1(f) \in \mathbb{Z}$ i $\mathrm{N}(f)|4\,\mathrm{d}_1(f)$ i, per tant, demostra (i).

Per a $\sigma = 2$, explicitem la matriu de la forma polar en funció de $\mathrm{d}_2(f)$:

$$A(\mathrm{pol}(f)) = \frac{1}{2}A_2(\mathrm{pol}(f)) = \frac{1}{2}\frac{\mathrm{N}(f)}{\det_2(f)}\,\mathrm{ad}(A_2(f)) = \frac{\mathrm{N}(f)}{2\,\mathrm{d}_2^2(f)}\,\mathrm{ad}(A_2(f)).$$

Aplicant de nou el lema anterior, obtenim que f és una K_2-forma si, i només si, $N(f)|2\,d_2(f)$, la qual cosa prova (ii).

De les fórmules anteriors es dedueix que les igualtats $N(f) = 4\,d_1(f)$ i $N(f) = 2\,d_2(f)$ són condicions equivalents a les igualtats $\mathrm{pol}(f) = \pm\,\mathrm{rec}_1(f)$ i $\mathrm{pol}(f) = \pm\,\mathrm{rec}_2(f)$, respectivament. Això prova els apartats (iii) i (iv). Observem que, per 4.1.12, tenim que $2|\,d_2(f)$. Per tant, si $N(f) = 2\,d_2(f)$, obtenim que $4|\,N(f)$.

Si n és parell, obtenim (v) directament, ja que de la igualtat $d_2(f) = 2^{n/2}\,d_1(f)$ es dedueix que $4\,d_1(f)|4\,d_1(f)2^{(n-2)/2} = 2\,d_2(f)$, per a $n \geq 2$.

En el cas binari, tenim que $\mathrm{rec}_1(f) = \mathrm{rec}_2(f)$, per 4.3.9. Per tant, apliquem el lema 4.3.11 i obtenim (vi).

Per al cas de $n = 4$, notem que $4\,d_1(f) = d_2(f)$. Així, si apliquem l'apartat (i), obtenim directament que la condició de K_1-forma equival a $N(f)|\,d_2(f)$. □

4.3.13 Corol·lari. *Sigui f una forma quadràtica de n variables, de coeficients enters i $\det_2(f)$ un quadrat.*

(i) *Si el nivell $N(f)$ és lliure de quadrats, aleshores f és una K_2-forma.*

(ii) *Si $d_2(f)$ és lliure de quadrats, aleshores $d_2(f)|N(f)$. En particular, per a $n = 4$, f és una K_1-forma si, i només si, $N(f) = d_2(f)$.*

DEMOSTRACIÓ: Per a veure (i), apliquem 4.1.12(ii). Tenim que $N(f)|2\,d_2^2(f)$. Amb la hipòtesi de $N(f)$ lliure de quadrats, deduïm que $N(f)|2\,d_2(f)$, la qual cosa equival a ser K_2-forma per la proposició anterior (ii).

Per 4.1.12(ii) sabem que $\det_2(f)|N(f)^n$; per tant, directament $d_2(f)|N(f)^n$. Si $d_2(f)$ és lliure de quadrats, deduïm que $d_2(f)|N(f)$. Per a $n = 4$, junt amb l'apartat (vii) de la proposició anterior, obtenim l'equivalència enunciada a (ii). □

4.3.14 Proposició. *Sigui f una forma quadràtica de coeficients racionals d'un nombre de variables n parell. Sigui $\lambda \in \mathbb{Z}$ i considerem la forma λf. Si f és una K_σ-forma, aleshores λf també és una K_σ-forma.* □

DEMOSTRACIÓ: En primer lloc, notem que cal que n sigui parell perquè $\det_\sigma(\lambda f)$ sigui també un quadrat.

D'una banda, tenim que $\det_\sigma(\lambda f) = \lambda^n \det_\sigma(\lambda f)$; per tant, se satisfà $\mathrm{d}_\sigma(\lambda f) = \lambda^{n/2}\,\mathrm{d}_\sigma(\lambda f)$. D'altra banda, $\mathrm{ad}(\lambda f) = \lambda^{n-1}\,\mathrm{ad}(f)$. Així, tenim les igualtats següents:

$$\mathrm{rec}_\sigma(\lambda f) = \frac{1}{\mathrm{d}_\sigma(\lambda f)}\,\mathrm{ad}(\lambda f) = \lambda^{n-1-n/2}\frac{1}{\mathrm{d}_\sigma(f)}\,\mathrm{ad}(f) = \lambda^{n/2-1}\,\mathrm{rec}_\sigma(f).$$

El resultat es dedueix per la definició de K_σ-forma. □

4.3.15 Remarca. Per a les formes binàries, se satisfà la igualtat $\mathrm{rec}_\sigma(\lambda f) = \mathrm{rec}_\sigma(f)$; per a les quaternàries, $\mathrm{rec}_\sigma(\lambda f) = \lambda\,\mathrm{rec}_\sigma(f)$. És clar que el recíproc de la proposició anterior no és cert. □

4.3.16 Cas binari. Considerem una forma quadràtica binària de coeficients enters, $f = aX^2 + bXY + cY^2$, tal que el seu determinant $\det_1(f) = ac - \frac{1}{4}b^2$ sigui un quadrat; és a dir, $\mathrm{disc}_{\mathbb{Q}}(f) = 1$, la qual cosa equival al fet que la forma f sigui producte de dos factors lineals. En aquest cas, tenim que $2\,\mathrm{d}_1(f) = \mathrm{d}_2(f) = \sqrt{4ac - b^2}$. Per tant,

$$\mathrm{rec}_1(f)(X,Y) = \mathrm{rec}_2(f)(X,Y) = \frac{2}{\sqrt{4ac-b^2}}(cX^2 - bXY + aY^2).$$

Per exemple, sigui $f = X^2 + 4XY + 8Y^2$. Obtenim que $\mathrm{d}_1(f) = 2$, $\mathrm{d}_2(f) = 4$, $\mathrm{ad}(f) = \mathrm{pol}(f) = 8X^2 - 4XY + Y^2$, $\mathrm{rec}_\sigma(f) = 4X^2 - 2XY + \frac{1}{2}Y^2$, i $\mathrm{N}(f) = \det_2(f) = 16$. És clar que f no és una K_σ-forma, per a $\sigma = 1$ ni $\sigma = 2$. □

4.3.17 Cas ternari. En el cas de les formes ternàries, considerem per exemple la forma $f = -245X^2 - 35Y^2 - 422Z^2 + 182YX + 644ZX - 238YZ$. Aleshores tenim que:

(i) $\det_1(f) = 441$, $\mathrm{d}_1(f) = -21$ i $\mathrm{N}(f) = 84$.

(ii) $\mathrm{ad}(f) = 609X^2 + 168YX + 882ZX - 294Y^2 + 294YZ + 294Z^2$.

(iii) $\mathrm{pol}(f) = 29X^2 - 14Y^2 + 14Z^2 + 8XY + 42XZ + 14YZ$.

(iv) $\mathrm{rec}_1(f) = -29X^2 + 14Y^2 - 14Z^2 - 8XY - 42XZ - 14YZ$.

Observem que és K_1-forma. □

4.3.18 Cas quaternari. Considerem la forma quaternària de coeficients enters $f = X^2 - 44Y^2 - 5Z^2 - 131T^2 - 2XZ - XT + 36YZ - 150YT + 61ZT$. Obtenim que:

(i) $\det_1(f) = 225$, $\det_2(f) = 3600$.

(ii) $\mathrm{d}_1(f) = -15$, $\mathrm{d}_2(f) = -60$.

(iii) $\mathrm{N}(f) = 120$.

(iv) $\mathrm{ad}(f) = 330X^2+315XY+270XZ-120XT-\frac{225}{2}Y^2+225YZ+180YT+150Z^2-60ZT$.

(v) $\mathrm{pol}(f) = 44X^2-15Y^2+20Z^2-8T^2+42XY+36XZ-16XT+30YZ+24YT-8ZT$.

(vi) $\mathrm{rec}_1(f) = -22X^2-21XY-18XZ+8XT+\frac{15}{2}Y^2-15YZ-12YT-10Z^2+4ZT+4T^2$.

(vii) $\mathrm{rec}_2(f) = -44X^2-42XY-36XZ+16XT+15Y^2-30YZ-24YT-20Z^2+8ZT+8T^2$.

Observem que f és una K_2-forma, però no és una K_1-forma. □

A continuació introduïm una nova definició, que recupera les *Hauptformen* de Brandt [Bra24]. Ens restringim al cas $\sigma = 1$.

4.3.19 Definició. Una K_1-forma f és principal si representa l'1 sobre $\mathbb{Z}$. □

4.3.20 Proposició. *Siguin f i f' dues formes quadràtiques de coeficients enters, de determinant quadrat. Si f i f' són $\mathbb{Z}$-equivalents, aleshores:*

(i) $\mathrm{d}_\sigma(f) = \mathrm{d}_\sigma(f')$; $\mathrm{N}(f) = \mathrm{N}(f')$.

(ii) $\mathrm{ad}(f) \overset{\mathbb{Z}}{\sim} \mathrm{ad}(f')$; $\mathrm{pol}(f) \overset{\mathbb{Z}}{\sim} \mathrm{pol}(f')$; $\mathrm{rec}(f) \overset{\mathbb{Z}}{\sim} \mathrm{rec}(f')$.

(iii) *f és K_σ-forma si, i només si, f' és K_σ-forma.*

(iv) *f és principal si, i només si, f' és principal.*

DEMOSTRACIÓ: L'apartat (i) és clar, perquè la $\mathbb{Z}$-equivalència dóna igualtat de determinants: $\det_\sigma(f) = \det_1(\sigma f) = \det_1(\sigma f') = \det_\sigma(f')$.

Suposem que la relació entre les matrius de les formes és $A(f') = P^t A(f) P$, amb $P \in \mathrm{GL}(n,\mathbb{Z})$. Fàcilment s'obté $\mathrm{ad}(A(f')) = Q^t \mathrm{ad}(A(f))Q$, amb $Q = (P^t)^{-1}$, que també pertany a $\mathrm{GL}(n,\mathbb{Z})$; per tant, obtenim l'equivalència de les formes adjuntes.

Per a veure la igualtat de nivells, apliquem 4.1.10(e), la igualtat de determinants i l'equivalència d'adjuntes, i notem que els continguts de formes $\mathbb{Z}$-equivalents coincideixen.

Utilitzant la igualtat de nivells i la caracterització del nivell d'una forma donada a 4.1.10(c) o (d), obtenim l'equivalència de les formes polars. L'equivalència de les formes recíproques es prova a partir de la definició de forma σ-recíproca i les igualtats i equivalències anteriors.

Les condicions que el determinant sigui un quadrat i que la forma i la recíproca tinguin coeficients enters es conserven per $\mathbb{Z}$-equivalència; per tant, la condició de K_σ-forma també. Finalment, només cal observar que formes $\mathbb{Z}$-equivalents representen els mateixos nombres sobre $\mathbb{Z}$. □

4.3.21 Lema. *Si f és una forma quaternària principal de coeficients enters, aleshores se satisfà $f(X,Y,Z,T) \overset{\mathbb{Z}}{\sim} X^2 + g(X,Y,Z,T)$, on g és una forma quadràtica quaternària en la qual no apareix el terme en X^2.*

DEMOSTRACIÓ: Per ser f principal, f representa l'1 sobre $\mathbb{Z}$, és a dir, existeixen $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ tals que $f(\alpha_1, \ldots, \alpha_n) = 1$. Notem que les representacions de l'1 sempre són primitives; és a dir, $\mathrm{mcd}(\alpha_1, \ldots, \alpha_n) = 1$. Això ens permet construir $S \in \mathrm{GL}(n, \mathbb{Z})$ de forma que tingui $\alpha_1, \ldots, \alpha_n$ a la primera columna. Aleshores, la matriu $S^t A(f) S$ determina una forma quadràtica f', $\mathbb{Z}$-equivalent a f, que conté el terme X^2. □

4.3.22 Lema. *Sigui f una forma quaternària principal de coeficients enters tal que $f(X,Y,Z,T) = X^2 + g(Y,Z,T)$, amb g forma quadràtica ternària. Aleshores,*

$$\mathrm{rec}_\sigma(f)(X,Y,Z,T) = \mathrm{d}_\sigma(f)X^2 \oplus \mathrm{rec}_\sigma(g)(Y,Z,T).$$

DEMOSTRACIÓ: És clar que $\mathrm{d}_\sigma(f) = \mathrm{d}_\sigma(g)$. És fàcil comprovar que

$$\mathrm{ad}(A(\sigma f)) = \left(\begin{array}{c|c} \det_\sigma(f) & 0 \\ \hline 0 & \mathrm{ad}(A(\sigma g)) \end{array}\right).$$

Si apliquem 4.3.8, es dedueix el resultat. □

4.4 Formes associades a àlgebres

En aquesta secció es presenten generalitats i propietats bàsiques de les K-àlgebres amb estructura d'espai quadràtic. Notem que els resultats es poden

aplicar tant als cossos quadràtics sobre K com a les K-àlgebres de quaternions. Com a referència general de K-àlgebres i ordres es pot veure [Rei75].

Siguin A una K-àlgebra finitament generada, $n = [A : K]$ i B una forma bilineal simètrica:

$$\begin{array}{rccc} B: & A \times A & \longrightarrow & K \\ & (\alpha, \beta) & \mapsto & B(\alpha, \beta). \end{array}$$

Fixada una K-base de A, considerem la forma quadràtica associada, que denotem per f_A. És una forma quadràtica de n variables:

$$\begin{array}{rccc} f_A: & A & \longrightarrow & K \\ & \alpha & \mapsto & f_A(\alpha) = B(\alpha, \alpha). \end{array}$$

L'expressió de la forma quadràtica f_A depèn de la base de A fixada. Si canviem la base, obtenim una forma quadràtica K-equivalent.

Per a obtenir bons resultats, exigim a la forma quadràtica un bon comportament respecte del producte i respecte de l'element unitat, que és l'estructura addicional que té una àlgebra enfront dels espais vectorials. Així, tenim les definicions següents.

4.4.1 Definicions. Una forma quadràtica f_A és unitària si $f_A(1_A) = 1_A$. Una forma quadràtica f_A és multiplicativa si $f_A(\alpha\beta) = f_A(\alpha)f_A(\beta)$, per a $\alpha, \beta \in A$. □

Per a qualsevol forma quadràtica f_A, la forma $\dfrac{1}{f_A(1_A)} f_A$ és una forma unitària. Com a exemple de formes quadràtiques multiplicatives assenyalem les formes nòrmiques, que veurem en els capítols següents. Observem que les dues propietats anteriors no depenen de la base de A en la qual s'expressi la forma quadràtica.

4.4.2 Lema. *Sigui f_A una forma quadràtica unitària de coeficients a K. Aleshores,*

(i) $f_A(\alpha) = \alpha^2$, *per a tot* $\alpha \in K$.

(ii) *Existeixen K-bases de A en les quals f_A representa l'1_A sobre R.*

DEMOSTRACIÓ: L'apartat (i) és una propietat general de formes quadràtiques unitàries.

Per a veure (ii) només cal triar una base respecte de la qual l'1 s'expressi en coordenades a R; per exemple, la base d'un R-ordre. En aquesta base, $f_A(1) = 1$ dóna una representació de l'1 sobre R. □

A partir de la forma f_A obtenim també altres formes quadràtiques. D'una banda, utilitzant l'estructura de A com a K-espai vectorial, ens podem restringir a un subespai A', $[A' : K] = n'$ i considerar la forma quadràtica associada, que tindrà n' variables, les propietats de la qual depenen de les característiques del subespai. En particular, es pot considerar el cas que A' sigui una K-subàlgebra de A.

D'altra banda, podem considerar els R-ordres de A; en aquest cas, obtenim formes quadràtiques de n variables. Sigui $\mathcal{O} \subset A$ un R-ordre de A. Si fixem una R-base $\{v_1, \ldots, v_n\}$ de l'ordre, un element genèric $\omega \in \mathcal{O}$ s'escriu $\omega = X_1v_1 + \ldots + X_nv_n$. Restringint la forma quadràtica f_A als elements de l'ordre, expressats d'aquesta manera, s'obté una forma quadràtica en les variables $X_1, \ldots, X_n$. Denotem per $f_{\mathcal{O},n}$ aquesta forma quadràtica. L'expressió de la forma quadràtica depèn de la base de $\mathcal{O}$ que hem fixat, per la qual cosa la notació anterior podria ser equívoca. Ara bé, pel lema següent, no serà així, si considerem la classe de R-equivalència de formes quadràtiques.

4.4.3 Lema. *Les formes quadràtiques $f_{\mathcal{O},n}$ associades a un R-ordre $\mathcal{O} \subseteq A$ en bases diferents són R-equivalents.*

DEMOSTRACIÓ: Si P és la matriu del canvi de base entre dues bases d'un R-ordre, aleshores $P \in \mathrm{GL}(n, R)$. Per tant, P dóna la R-equivalència de les formes associades. □

Les formes quadràtiques associades als ordres contenen també informació sobre l'àlgebra. En particular, es tenen els resultats següents, que ens seran útils per a tractar les àlgebres de quaternions.

4.4.4 Proposició. *Sigui $\mathcal{O}$ un ordre d'una K-àlgebra A. Fixem bases de $\mathcal{O}$ i de A, i considerem les formes quadràtiques $f_{\mathcal{O},n}$ i f_A. Sigui P la matriu de canvi de la base de $\mathcal{O}$ a la base de A.*

(i) $f_{\mathcal{O},n} \overset{K}{\sim} f_A$. *En particular,* $\mathrm{disc}_K(f_{\mathcal{O},n}) = \mathrm{disc}_K(f_A)$; *concretament* $\det_1(f_{\mathcal{O},n}) = (\det P)^2 \det_1(f_A)$.

(ii) *Si f_A és una forma quadràtica unitària, aleshores $f_{\mathcal{O},n}$ representa l'1 sobre R.*

DEMOSTRACIÓ: La R-base de l'ordre $\mathcal{O}$ és també una K-base de A. Així, la forma $f_{\mathcal{O}}$ és també la forma quadràtica de A, però en una altra base. Per tant, són K-equivalents.

La unitat de l'àlgebra A pertany a $\mathcal{O}$, perquè tot ordre és un subanell. Per ser f_A unitària, tenim precisament que $f_{\mathcal{O},n}(1_A) = 1_A$. La representació és sobre R perquè l'1_A s'expressa en funció de la base de $\mathcal{O}$ amb coeficients a R. □

4.4.5 Corol·lari. *Suposem que K és un cos de nombres totalment real i fixem una immersió de K en $\mathbb{R}$, la qual cosa permet definir la signatura i el caràcter definit o indefinit de les formes quadràtiques amb coeficients a K. Aleshores, per a qualsevol R-ordre $\mathcal{O}$ de A, les formes f_A i $f_{\mathcal{O},n}$ tenen la mateixa signatura i, per tant, el mateix caràcter definit o indefinit.* □

4.4.6 Proposició. *Suposem que la forma f_A és multiplicativa. Siguin $\mathcal{O}$ i $\mathcal{O}'$ dos R-ordres de A conjugats. Aleshores, $f_{\mathcal{O},n} \overset{R}{\sim} f_{\mathcal{O}',n}$.*

DEMOSTRACIÓ: Sigui $\{v_i\}_{i=1,\dots,n}$ una R-base de $\mathcal{O}$. Suposem que $\mathcal{O}' = u^{-1}\mathcal{O}u$. Aleshores, la base conjugada $\{u^{-1}v_iu\}_{i=1,\dots,n}$ és una R-base de $\mathcal{O}'$. Per a qualsevol $\omega \in A$, tenim que $f_A(\omega) = f_A(u^{-1}\omega u)$, per ser una forma quadràtica multiplicativa. D'aquí deduïm que les formes quadràtiques associades als ordres $\mathcal{O}$ i $\mathcal{O}'$, en les bases $\{v_i\}_{i=1,\dots,n}$ i $\{u^{-1}v_iu\}_{i=1,\dots,n}$, respectivament, són exactament la mateixa. Efectivament, és clar que els coeficients centrals coincideixen. Comprovem que els coeficients laterals també coincideixen, usant la forma bilineal associada. Tenim que

$$\begin{aligned} B(v_i + v_j, v_i + v_j) &= f_A(v_i + v_j) = f_A(u^{-1}(v_i + v_j)u) \\ &= B(u^{-1}(v_i + v_j)u, u^{-1}(v_i + v_j)u). \end{aligned}$$

Si ho desenvolupem aplicant la bilinealitat i de nou la multiplicativitat, obtenim que $B(v_i, v_j) = B(u^{-1}v_iu, u^{-1}v_ju)$. Això prova la igualtat de les formes sobre bases conjugades. Ara bé, en un mateix ordre tenim ja R-equivalència de formes, per 4.4.3, per tant, efectivament, les funcions són R-equivalents. □

4.4.7 Proposició. *Siguin $\mathcal{O}' \subseteq \mathcal{O}$ dos ordres de A, amb bases fixades. Posem $r = \det P$, on P és la matriu de les coordenades dels vectors de la base de $\mathcal{O}'$ en funció de la base de $\mathcal{O}$. Aleshores:*

(i) $f_{\mathcal{O},n} \overset{R}{\to} f_{\mathcal{O}',n}$.

(ii) $\det_1(f_{\mathcal{O}',n}) = r^2 \det_1(f_{\mathcal{O},n})$.

(iii) $\det_1(f_{\mathcal{O}',n}) = \det_1(f_{\mathcal{O},n})$ *si, i només si,* $f_{\mathcal{O},n} \overset{R}{\sim} f_{\mathcal{O}',n}$ *si, i només si,* $\mathcal{O} = \mathcal{O}'$.

DEMOSTRACIÓ: Siguin $\{v_i\}$ i $\{v'_i\}$ R-bases dels ordres $\mathcal{O}$ i $\mathcal{O}'$, respectivament. Tenim que $v'_j = \sum_{i=1}^{n} a_{ij} v_i$, amb $a_{ij} \in R$. Si posem $P = (a_{ij})$, se satisfà $P \in \mathrm{M}(n,R) \cap \mathrm{GL}(n,K)$ i $P^t A(f_{\mathcal{O},n}) P = A(f_{\mathcal{O}',n})$, la qual cosa demostra (i).

En particular, si considerem determinants a la igualtat de matrius, obtenim (ii), amb $r = \det P$.

Finalment, notem que les condicions de (iii) són totes equivalents a $r = \pm 1$, atès que $\mathcal{O}' \subseteq \mathcal{O}$. □

4.5 Ordres quadràtics i formes binàries

En aquesta secció fixem notacions i mostrem la relació entre els cossos quadràtics i les formes quadràtiques binàries, com a introducció als resultats paral·lels que relacionaran les àlgebres de quaternions i les formes quadràtiques ternàries i quaternàries (cf. capítols 5 i 6). Conjuntament, els utilitzarem per a relacionar les immersions de cossos quadràtics en àlgebres de quaternions amb formes quadràtiques (cf. capítol 7). En primer lloc, fem un breu resum de la notació i d'alguns resultats de cossos quadràtics.

Considerem un cos quadràtic $F = \mathbb{Q}(\sqrt{d})$, on $d \in \mathbb{Z}$ és lliure de quadrats. Denotem per Λ_F l'anell d'enters de F. Una $\mathbb{Z}$-base de Λ_F és $\{1, w\}$, on $w = \sqrt{d}$ si $d \equiv 2,3 \mod 4$ i $w = \dfrac{1+\sqrt{d}}{2}$ si $d \equiv 1 \mod 4$. Per a un element $\lambda \in F$, es denoten per λ' el seu conjugat per l'acció del grup de Galois, i per $\mathrm{n}(\lambda)$ i $\mathrm{tr}(\lambda)$ la seva norma i la seva traça, respectivament. Denotem per F_0 els elements de F de traça igual a 0.

Recordem que un ordre Λ de F és un $\mathbb{Z}$-mòdul lliure de rang 2, format per elements enters, i que té associat un discriminant que denotem per D_Λ. Els ordres d'un cos quadràtic, els anomenarem ordres quadràtics. L'anell d'enters Λ_F és l'únic ordre maximal de F. El discriminant fonamental del cos F, que denotem per D_F, és el discriminant de l'ordre maximal, $D_F := D_{\Lambda_F}$. Se satisfà que $D_F = 4d$ si $d \equiv 2,3 \mod 4$ i $D_F = d$ si $d \equiv 1 \mod 4$; així, $F = \mathbb{Q}(\sqrt{D_F})$ i $D_F \equiv 0,1 \mod 4$. Qualsevol altre ordre Λ està contingut en l'ordre maximal i el conductor de Λ és l'índex $[\Lambda_F : \Lambda]$, com a $\mathbb{Z}$-mòduls. De fet, per a cada $m \in \mathbb{N}$, l'ordre quadràtic $\Lambda(d,m) := \mathbb{Z}[1, mw]$ és l'únic ordre de conductor m del cos quadràtic $\mathbb{Q}(\sqrt{d})$, i el seu discriminant és $D_{\Lambda(d,m)} = m^2 D_F$. Així, el conductor determina l'ordre. Observem que l'ordre quadràtic $\mathbb{Z}[1, \sqrt{d}]$ és l'ordre de conductor 1 si $d \equiv 2,3 \mod 4$, i l'ordre de conductor 2 si $d \equiv 1 \mod 4$.

A partir de l'aplicació traça, que tenim definida sobre F, podem definir la forma bilineal simètrica

$$\begin{array}{rccc} B: & F\times F & \longrightarrow & \mathbb{Q} \\ & (\lambda,\mu) & \mapsto & \frac{1}{2}\operatorname{tr}(\lambda\mu'). \end{array}$$

L'espai quadràtic (F,B) és regular i fixem la base $\{1,\sqrt{d}\}$, que és una $\mathbb{Q}$-base ortogonal de (F,B). La forma quadràtica associada a aquesta forma bilineal és justament la forma norma,

$$\begin{array}{ccc} F & \longrightarrow & \mathbb{Q} \\ \lambda & \mapsto & B(\lambda,\lambda)=\frac{1}{2}\operatorname{tr}(\lambda\lambda')=\mathrm{n}(\lambda). \end{array}$$

Aquesta forma quadràtica binària, l'anomenem forma nòrmica de F i la denotem per $n_{F,2}$. Tenim que $n_{F,2}(X,Y)=X^2-dY^2$. Si escollim una altra base de F, la forma quadràtica obtinguda serà $\mathbb{Q}$-equivalent a l'anterior. Algunes de les seves propietats, ben conegudes, es recullen en el lema següent.

4.5.1 Lema. *Sigui $F=\mathbb{Q}(\sqrt{d})$ un cos quadràtic i $n_{F,2}$ la forma nòrmica associada. Aleshores:*

(i) $\operatorname{disc}_{\mathbb{Q}}(n_{F,2})=-d=-D_F$ *a* $\mathbb{Q}^*/\mathbb{Q}^{*2}$;
$\det_1(n_{F,2})=-d$,
$\det_2(n_{F,2})=-4d$.

(ii) $n_{F,2}$ *és definida positiva si F és un cos quadràtic imaginari.*
$n_{F,2}$ *és indefinida si F és un cos quadràtic real.*

(iii) $n_{F,2}$ *és una forma multiplicativa i unitària.*

(iv) $n_{F,2}$ *és de coeficients enters, reduïda i primitiva.*

(v) $\operatorname{ad}(n_{F,2})(X,Y)=\operatorname{pol}(n_{F,2})(X,Y)=-dX^2+Y^2$ *i és* $\mathrm{SL}(2,\mathbb{Z})$*-equivalent a* $n_{F,2}$.

(vi) $\mathrm{N}(n_{F,2})=4d$.

4.5.2 Definició. Sigui Λ un ordre quadràtic. La forma nòrmica associada a Λ, respecte d'una base fixada, és la forma quadràtica binària que s'obté en restringir la norma als elements de l'ordre expressats en aquesta base. □

Notem que, per 4.4.3, les formes nòrmiques que s'obtenen per a un mateix ordre en bases diferents són $\mathrm{SL}(2,\mathbb{Z})$-equivalents. Així, encara que la forma

nòrmica associada a un ordre depèn de la base de l'ordre fixada, podem considerar-la independent si prenem la seva $\mathrm{SL}(2,\mathbb{Z})$-classe d'equivalència. D'altra banda, recordem que les formes nòrmiques dels ordres estan relacionades amb la forma nòrmica associada a l'àlgebra via $\mathbb{Q}$-equivalència, per 4.4.4.

La proposició següent proporciona les formes nòrmiques associades a l'ordre de conductor m respecte d'algunes bases.

4.5.3 Proposició. *Sigui Λ l'ordre de $\mathbb{Q}(\sqrt{d})$ de conductor m.*

(i) *La forma nòrmica de Λ en la base $\{1, mw\}$ és*

$$= \begin{cases} X^2 - dm^2Y^2 & \text{si } d \equiv 2,3 \mod 4, \\ X^2 + mXY + m^2\dfrac{1-d}{4}Y^2 & \text{si } d \equiv 1 \mod 4. \end{cases}$$

$$= \begin{cases} X^2 - \dfrac{D_F}{4}m^2Y^2 & \text{si } D_F \equiv 0 \mod 4, \\ X^2 + mXY + m^2\dfrac{1-D_F}{4}Y^2 & \text{si } D_F \equiv 1 \mod 4. \end{cases}$$

(ii) *La forma nòrmica de Λ en la base $\{1, m\dfrac{D_F+\sqrt{D_F}}{2}\}$ és*

$$\begin{cases} X^2 + 4dmXY + m^2d(4d-1)Y^2 & \text{si } d \equiv 2,3 \mod 4, \\ X^2 + mdXY + m^2d(\dfrac{d-1}{4})Y^2 & \text{si } d \equiv 1 \mod 4. \end{cases}$$

$$= X^2 + mD_FXY + m^2D_F(\frac{D_F-1}{4})Y^2.$$

(iii) *La forma nòrmica de Λ en la base $\{1, \dfrac{D_\Lambda+\sqrt{D_\Lambda}}{2}\}$ és*

$$X^2 + XYD_\Lambda + Y^2(\frac{D_\Lambda^2 - D_\Lambda}{4})$$
$$= X^2 + XYm^2D_F + m^2D_F(\frac{m^2D_F-1}{4})Y^2 =$$

$$= \begin{cases} X^2 + 4m^2dXY + m^2d(4m^2d-1)Y^2 & \text{si } d \equiv 2,3(4) \\ X^2 + m^2dXY + d\dfrac{m^2(m^2d-1)}{4}Y^2 & \text{si } d \equiv 1(4). \end{cases}$$ □

4.5.4 Proposició. *La forma nòrmica reduïda* (cf. [Coh95]) *corresponent a l'ordre* $\Lambda = \Lambda(d, m)$ *és*

$$\begin{cases} X^2 - \frac{D_\Lambda}{4}Y^2 & si\ D_\Lambda \equiv 0 \mod 4, \\ X^2 + XY + \frac{1 - D_\Lambda}{4}Y^2 & si\ D_\Lambda \equiv 1 \mod 4, \end{cases}$$

i s'obté en considerar la base $\begin{cases} \{1, mw\} & si\ d \equiv 2, 3 \mod 4, \\ \{1, -[\frac{m}{2}] + mw\} & si\ d \equiv 1 \mod 4. \end{cases}$

DEMOSTRACIÓ: Considerem la forma nòrmica de Λ respecte de la base habitual, segons l'apartat (i) de la proposició anterior. És clar que per a $d \equiv 2, 3$ mod 4 ja és una forma reduïda. Suposem, doncs, $d \equiv 1 \mod 4$. Tot aplicant l'algoritme clàssic de reducció de formes quadràtiques binàries, ens cal distingir si m és parell o no. Si m és parell, obtenim la mateixa forma que en el cas $d \equiv 2, 3 \mod 4$. Si m és senar, obtenim l'altra expressió. Ambdues possibilitats queden recollides clarament expressant-les respecte D_Λ, ja que $D_\Lambda = m^2 D_F$ és sempre congruent amb 0 o 1 mòdul 4, i estem en el primer cas si, i només si, $d \equiv 2, 3 \mod 4$ o m és parell. El mateix algoritme permet trobar la base corresponent. □

En particular, si considerem l'anell d'enters $\Lambda_F = \Lambda(d, 1)$, utilitzarem la forma nòrmica binària reduïda

$$n_{\Lambda(d,1),2} = \begin{cases} X^2 - dY^2 & \text{si } d \equiv 2, 3 \mod 4, \\ X^2 + XY + \frac{1-d}{4}Y^2 & \text{si } d \equiv 1 \mod 4. \end{cases}$$

$$= \begin{cases} X^2 - \frac{D_F}{4}Y^2 & \text{si } D_F \equiv 0 \mod 4, \\ X^2 + XY + \frac{1 - D_F}{4}Y^2 & \text{si } D_F \equiv 1 \mod 4. \end{cases}$$

Les formes quadràtiques nòrmiques dels ordres contenen informació sobre el cos quadràtic i podríem dir que en certa forma el caracteritzen. Recopilem en el lema següent algunes propietats i relacions entre invariants associats als ordres i a les formes quadràtiques.

4.5.5 Lema. *Sigui* Λ *l'ordre del cos quadràtic* $F = \mathbb{Q}(\sqrt{d})$ *de conductor* m. *Siguin* $n_{\Lambda,2}$ *i* $n_{F,2}$ *les formes nòrmiques associades a l'ordre i al cos quadràtic, respectivament, en certes bases. Aleshores:*

(i) $\mathrm{disc}_{\mathbb{Q}}(n_{\Lambda,2}) = \mathrm{disc}_{\mathbb{Q}}(n_{F,2}) = -d = -D_F$ *a* $\mathbb{Q}^*/\mathbb{Q}^{*2}$;
$\det_1(n_{\Lambda,2}) = -\dfrac{D_\Lambda}{4}$; $\det_2(n_{\Lambda,2}) = -D_\Lambda$

(ii) $n_{\Lambda,2}$ *és definida positiva si* F *és un cos quadràtic imaginari.*
$n_{\Lambda,2}$ *és indefinida si* F *és un cos quadràtic real.*

(iii) $n_{\Lambda,2}$ *és de coeficients enters i unitària.*

(iv) $n_{\Lambda,2}$ *és primitiva i es té la* $\mathrm{SL}(2,\mathbb{Z})$*-equivalència* $n_{\Lambda,2} \sim \mathrm{ad}(n_{\Lambda,2})$.

(v) $\mathrm{N}(n_{\Lambda,2}) = |\det_2(n_{\Lambda,2})| = D_\Lambda$. □

Com a cas particular de 4.4.7 tenim la proposició següent, que la unicitat dels ordres quadràtics i el fet que sigui $R = \mathbb{Z}$ fan que sigui més explícita.

4.5.6 Proposició. *Siguin* $\Lambda' \subset \Lambda$ *dos ordres de* F. *Posem* $r = [\Lambda : \Lambda'] \in \mathbb{Z}$ *l'índex de* Λ' *en* Λ *com a* $\mathbb{Z}$*-mòduls. Aleshores,*

(i) $n_{\Lambda,2} \xrightarrow{\mathbb{Z}} n_{\Lambda',2}$.

(ii) $\det_1(n_{\Lambda',2}) = r^2 \det_1(n_{\Lambda,2})$; $\mathrm{N}(n_{\Lambda',2}) = r^2\,\mathrm{N}(n_{\Lambda,2})$.

(iii) $n_{\Lambda,2} \overset{\mathbb{Z}}{\sim} n_{\Lambda',2}$ *si, i només si,* $\det_1(n_{\Lambda',2}) = \det_1(n_{\Lambda,2})$ *si, i només si,* $\mathrm{N}(n_{\Lambda',2}) = \mathrm{N}(n_{\Lambda,2})$ *si, i només si,* $\Lambda = \Lambda'$. □

Estem interessats en les unitats fonamentals dels cossos quadràtics $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ lliure de quadrats, i els ordres quadràtics $\Lambda(d,m)$. En llenguatge de formes quadràtiques és equivalent a l'estudi de les representacions de ± 1 per la forma nòrmica.

Suposem que F és un cos quadràtic real; és a dir, $d > 0$. Pel teorema de les unitats de Dirichlet, donat un ordre Λ de $\mathbb{Q}(\sqrt{d})$, existeix una unitat $\varepsilon \in \Lambda$ tal que cada unitat de Λ té una expressió única de la forma $\pm\varepsilon^n$. Posant $\varepsilon = a + b\sqrt{d}$, el conjunt d'unitats $\{\varepsilon, -\varepsilon, 1/\varepsilon, -1/\varepsilon\}$ correspon als quatre elements $\pm a \pm b\sqrt{d}$; només l'element amb $a, b > 0$ satisfà que és més gran que 1 i s'anomena unitat fonamental de Λ. De fet, les unitats més grans que 1 són precisament aquelles amb $a + b\sqrt{d}$, $a, b > 0$. La unitat fonamental de l'ordre maximal s'anomena unitat fonamental del cos. En particular, les unitats fonamentals dels ordres quadràtics són potència de la unitat fonamental del cos. La unitat fonamental del cos és la solució, amb els enters positius mínims x i y, de $\mathrm{n}(x + yw) = \pm 1$; és a dir, de $x^2 - dy^2 = \pm 1$ si $d \equiv 2, 3 \mod 4$, o de

$x^2+xy+\frac{1-d}{4}y^2 = \pm 1$ si $d \equiv 1 \mod 4$. En llenguatge de formes quadràtiques nòrmiques, tenim que la unitat fonamental de l'ordre quadràtic $\Lambda(d,m)$ és la representació $(x,y) \in \mathcal{R}(n_{\Lambda(d,m),2}, 1; \mathbb{Z})$ amb x i y enters positius mínims.

Si F és cos quadràtic imaginari, els resultats sobre les unitats són ben concrets. Pel cos quadràtic imaginari $\mathbb{Q}(\iota)$, $\iota^2 = -1$, el grup d'unitats el formen les arrels quartes de la unitat $\{\pm 1, \pm\iota\}$. Per a $\mathbb{Q}(\sqrt{-3})$, el grup d'unitats el formen les arrels sisenes de la unitat $\left\{\left(\frac{1+\sqrt{-3}}{2}\right)^r : r = 0,1,\ldots,5\right\}$. Per a la resta de cossos quadràtics imaginaris, el grup de les unitats és $\{1,-1\}$.

4.5.7 Notació. Sigui $F = \mathbb{Q}(\sqrt{d})$ un cos quadràtic imaginari, on d és lliure de quadrats. Denotem per $h(d)$ el nombre de classes d'ideals de F. Sigui $\Lambda(d,m) \subseteq F$ l'ordre quadràtic de conductor m. Denotem per $h(d,m)$ el nombre de classes d'ideals de $\Lambda(d,m)$, que coincideix amb el nombre de formes quadràtiques binàries definides positives, primitives i reduïdes de discriminant igual a $-D_{\Lambda(d,m)}$. □

4.5.8 Proposició. (cf. [Zag81]) *Sigui $\Lambda(d,m)$ l'ordre quadràtic de conductor $m > 1$ de $F = \mathbb{Q}(\sqrt{d})$, amb d lliure de quadrats, $d < 0$. Sigui D_F el discriminant fonamental de F. Aleshores,*

$$h(d,m) = \frac{mh(d)}{\nu} \prod_{p|m} \left(1 - \left(\frac{D_F}{p}\right) p^{-1}\right),$$

on

$$\nu = \begin{cases} 2 & \text{si } d = -1, m > 1 \\ 3 & \text{si } d = -3, m > 1 \\ 1 & \text{altrament.} \end{cases}$$ □

4.6 Algoritmes

A partir de les definicions i els resultats d'aquest capítol hem programat instruccions per a facilitar el càlcul de les constants i de les formes quadràtiques associades a una forma quadràtica donada. Per a entrar una forma quadràtica f com a argument, utilitzem la matriu associada $A(f)$. Amb la instrucció expf recuperem l'expressió de la forma quadràtica. Algunes de les instruccions funcionen en general per a formes de coeficients reals o, fins i tot, amb paràmetres; notem, però, que no té sentit utilitzar paràmetres quan s'inclou el càlcul d'arrels quadrades, o el del màxim comú divisor o el requeriment que alguns valors siguin enters, com per exemple per a calcular la forma

recíproca. Per tal que totes les instruccions tinguin sentit, ens restringim a formes quadràtiques de coeficients a $\mathbb{Z}$. Per alleugerir, en algunes comandes ens restringim a $n \leq 4$ variables. En general, hem adoptat noms referents a les notacions del capítol.

En primer lloc, la comanda `A2f` dóna la matriu parella i ens permet treballar amb matrius de coeficients enters. Tenim les instruccions següents per a calcular les constants corresponents a una forma quadràtica: `det1f`, `det2f`, `discf`, `contf`, `d1f` i `d2f`, inspirades en les definicions i notacions de les seccions anteriors. Per al càlcul del nivell d'una forma hem programat la instrucció `nivf`.

En relació amb els invariants respecte de relacions d'equivalència, tenim les instruccions: `discpf`, que dóna el discriminant a $\mathbb{Q}_p$; `signf`, que dóna la signatura; `diagf`, que diagonalitza f sobre $\mathbb{Q}$; `Sf`, que dóna la llista de primers crítics; `S1f`, que dóna la llista de primers per als quals f és $\mathbb{Q}$-anisòtropa; `HWinvf`, que dóna l'invariant de Hasse-Witt; i `S2f`, que dóna la llista de primers per als quals l'invariant de Hasse-Witt de f és -1. Per a cercar representacions de nombres enters per formes quadràtiques de 2,3 o bé 4 variables de coeficients enters, hem incorporat la instrucció `FindRepf`.

Calculem les formes quadràtiques associades a partir de les comandes `adf`, `polf`, `rec1f` i `rec2f`, que donen la forma adjunta, la forma polar, la forma 1-recíproca i la forma 2-recíproca, respectivament.

Hem implementat també les funcions lògiques `isPrimf`, `isIsotf`, `isK1f` i `isK2f`, les quals responen *true* o *false* segons si una forma satisfà o no les propietats de ser primitiva, isòtropa, K_1-forma i K_2-forma, respectivament.

La generalització de les definicions de la forma recíproca associada a f, per al cas que $|\det_1(f)|$ sigui un quadrat, cf. 5.2, ha donat lloc a les comandes `d1gf`, `d2gf`, `rec1gf`, `rec2gf`, `isK1gf` i `isK2gf`.

Respecte de les formes associades als cossos quadràtics, el paquet `Poincare` conté les instruccions: `fundDiscF`, que dóna el discriminant fonamental del cos; `bnfF`, que dóna la forma nòrmica associada al cos quadràtic; `bnfLatF` i `bnfOrF`, que donen la forma nòrmica associada a una xarxa i a un ordre quadràtic, respectivament, i `redbnfOrF`, que dóna la forma nòrmica reduïda d'un ordre quadràtic.

Capítol 5

Àlgebres de quaternions i formes quadràtiques

En aquest capítol interpretem les $\mathbb{Q}$-àlgebres de quaternions com a espais quadràtics.

Sigui H una $\mathbb{Q}$-àlgebra de quaternions amb una base fixada. Donada una forma bilineal simètrica B definida sobre H,

$$\begin{array}{rccc} B: & H \times H & \longrightarrow & \mathbb{Q} \\ & (\alpha, \beta) & \mapsto & B(\alpha, \beta), \end{array}$$

considerem l'expressió de la forma quadràtica associada, en la base fixada anteriorment, que denotarem per $f_{H,4}$, on el subíndex 4 ens indica que és una forma de quatre variables:

$$\begin{array}{rccc} f_{H,4}: & H & \longrightarrow & \mathbb{Q} \\ & \alpha & \mapsto & f_{H,4}(\alpha) = B(\alpha, \alpha). \end{array}$$

En particular, aplicarem els resultats sobre formes quadràtiques associades a K-àlgebres esmentats en la secció 4.4. La restricció de $f_{H,4}$ al subespai dels quaternions purs H_0 permet definir una forma quadràtica ternària associada a l'àlgebra de quaternions, que denotem per $f_{H,3}$, que tindrà un paper rellevant en els resultats posteriors. Estudiem les formes quadràtiques provinents de la norma i de la traça de les $\mathbb{Q}$-àlgebres de quaternions, que anomenem formes nòrmiques i formes traça, respectivament.

5.1 Formes nòrmiques d'àlgebres de quaternions

5.1.1 Definicions i primeres propietats

Sigui $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ una $\mathbb{Q}$-àlgebra de quaternions, on $a, b \in \mathbb{Z}$, lliures de quadrats. Fixem la base canònica $\{1, i, j, ij\}$ de H.

A partir de l'aplicació traça que tenim definida sobre H, podem definir la forma bilineal simètrica

$$\begin{array}{rccc} B: & H \times H & \longrightarrow & \mathbb{Q} \\ & (\alpha, \beta) & \mapsto & \frac{1}{2}\mathrm{tr}(\alpha\overline{\beta}). \end{array}$$

La forma quadràtica associada a aquesta forma bilineal és justament la forma norma,

$$\begin{array}{ccc} H & \longrightarrow & \mathbb{Q} \\ \alpha & \mapsto & B(\alpha,\alpha) = \frac{1}{2}\mathrm{tr}(\alpha\overline{\alpha}) = \mathrm{n}(\alpha), \end{array}$$

que dóna als espais H i H_0 una estructura natural d'espais quadràtics, (H, B) i $(H_0, B_{|H_0})$, respectivament.

5.1.1 Remarca. Considerem la forma bilineal B restringida a l'espai dels quaternions purs. Per a $u, v \in H_0$ tenim que $B_{|H_0}(u,v) = \frac{1}{2}(u\overline{v} + v\overline{u}) = \frac{-1}{2}(uv + vu)$. Així, u i v són ortogonals a l'espai $(H_0, B_{|H_0})$ si, i només si, u i v anticommuten a H_0. Per tant, $\{i, j, k\}$ és una base ortogonal de H_0. A més, per a $u \in H_0$ tenim que $B(1,u) = 0$; per tant, el subespai $\mathbb{Q}$ (pensat com $\mathbb{Q}\cdot 1$) és ortogonal a H_0. Així, $\{1, i, j, ij\}$ és una base ortogonal de l'espai quadràtic regular (H, B). □

El lema següent dóna una relació explícita entre la forma bilineal associada a la $\mathbb{Q}$-àlgebra de quaternions i el producte quaterniònic, no commutatiu. En particular, es pot utilitzar per a programar el producte quaterniònic.

5.1.2 Lema. *Siguin* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions amb base* $\{1, i, j, ij\}$ *i* B *la forma bilineal associada a* H. *Siguin* $u, v \in H_0$ *i considerem el producte vectorial* $P(u,v)$ *donat pel determinant*

$$P((u_1,u_2,u_3),(u_1,u_2,u_3)) = \begin{vmatrix} -bi & -aj & ij \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix}.$$

Aleshores, $u \cdot v = P(u,v) - B(u,v)$.

DEMOSTRACIÓ: Es comprova sobre els elements de la base i s'estén per bilinealitat de B i P. □

5.1.3 Definició. Anomenem formes nòrmiques associades a la $\mathbb{Q}$-àlgebra de quaternions H les expressions de la forma quadràtica norma sobre H i sobre H_0 en les bases $\{1,i,j,ij\}$ i $\{i,j,ij\}$, respectivament. Les denotem per $n_{H,4}$ i $n_{H,3}$, respectivament. Definim també la forma quadràtica binària associada a H en aquesta base com $n_{H,2}(X,Y) = aX^2 + bY^2$. □

Explícitament, a l'àlgebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, li associem les formes nòrmiques següents, respecte de la base canònica $\{1,i,j,ij\}$:

la forma quaternària	$n_{H,4}(X,Y,Z,T) = X^2 - aY^2 - bZ^2 + abT^2$,
la forma ternària	$n_{H,3}(Y,Z,T) = -aY^2 - bZ^2 + abT^2$,
la forma binària	$n_{H,2}(Y,Z) = aY^2 + bZ^2$.

El subíndex numèric indica el nombre de variables de la forma quadràtica.

5.1.4 Remarca. Sigui V un $\mathbb{Q}$-espai vectorial de dimensió 2 amb estructura d'espai quadràtic donada per la forma quadràtica associada $q(X,Y) = aX^2 + bY^2$. Aleshores, l'àlgebra de Clifford de V és isomorfa a l'àlgebra de quaternions $H = \left(\frac{a,b}{\mathbb{Q}}\right)$. □

5.1.5 Cas no ramificat. Si considerem $H = \left(\frac{1,-1}{\mathbb{Q}}\right)$, obtenim les formes nòrmiques $n_{H,4}(X,Y,Z,T) = X^2 - Y^2 + Z^2 - T^2$, $n_{H,3}(Y,Z,T) = -Y^2 + Z^2 - T^2$ i $n_{H,2}(Y,Z) = Y^2 - Z^2$.

Podem considerar directament l'àlgebra isomorfa $H' = M(2,\mathbb{Q})$. Interpretant la forma quadràtica directament en funció de la norma, obtenim les formes quadràtiques $n_{H',4}(X,Y,Z,T) = XT - YZ$ i $n_{H',3}(Y,Z,T) = -YZ - T^2$ que són $\mathbb{Q}$-equivalents a les dues anteriors, respectivament. Notem que en aquest cas no té sentit la forma binària, ja que no té interpretació en funció de la norma. □

5.1.6 Lema. *Sigui H una $\mathbb{Q}$-àlgebra de quaternions. Tenim les propietats següents.*

(i) *Per a tot $\lambda \in \mathbb{Q}$, $n_{H,4}(\lambda) = \lambda^2$.*

(ii) *Per a tot* $u \in H_0$, $n_{H,4}(u) = n_{H,3}(u) = -u^2$.

(iii) $n_{H,4}$ *és una forma quaternària unitària i multiplicativa.*

(iv) $n_{H,4} \sim < 1 > \oplus\, n_{H,3}$.

(v) *Les formes quadràtiques* $n_{H,4}$, $n_{H,3}$ *i* $n_{H,2}$ *són de coeficients enters.* □

Donat que la norma es conserva per isomorfisme d'àlgebres, tenim el resultat següent, ben conegut, sobre l'equivalència entre isomorfisme de $\mathbb{Q}$-àlgebres i isometria de $\mathbb{Q}$-espais quadràtics.

5.1.7 Proposició. *Siguin* H *i* H' *dues* $\mathbb{Q}$*-àlgebres de quaternions, amb una estructura d'espais quadràtics donada de forma natural per la forma nòrmica associada. Aleshores, són equivalents:*

(i) H *i* H' *són* $\mathbb{Q}$*-àlgebres isomorfes.*

(ii) $(H, n_{H,4})$ *i* $(H', n_{H',4})$ *són* $\mathbb{Q}$*-espais quadràtics isomètrics.*

(iii) $(H_0, t_{H,3})$ *i* $(H'_0, t_{H',3})$ *són* $\mathbb{Q}$*-espais quadràtics isomètrics.* □

Aquestes formes quadràtiques nòrmiques associades a l'àlgebra de quaternions donen molta informació sobre l'àlgebra i, en certa manera, la caracteritzen. Interpretarem alguns invariants i definicions de l'àlgebra de quaternions en funció de les formes quadràtiques.

En primer lloc, llistem algunes propietats d'aquestes formes quadràtiques, determinades bàsicament pels nombres a i b.

5.1.8 Lema. *Siguin* $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i* $n_{H,4}$, $n_{H,3}$ *i* $n_{H,2}$ *les formes nòrmiques associades a* H.

(i) $\mathrm{disc}_{\mathbb{Q}}(n_{H,4}) = \mathrm{disc}_{\mathbb{Q}}(n_{H,3}) = 1 \quad i \quad \mathrm{disc}_{\mathbb{Q}}(n_{H,2}) = ab$.

(ii) *Les formes* $n_{H,4}$ *i* $n_{H,3}$ *tenen el mateix caràcter, definit o indefinit, i no són mai definides negatives.*

(iii) *La forma* $n_{H,4}$ *només pot tenir la signatura* $(4,0)$ *o* $(2,2)$*; la forma* $n_{H,3}$ *només pot tenir la signatura* $(3,0)$ *o* $(1,2)$.

(iv) $\varepsilon_v(n_{H,4}) = \varepsilon_v(n_{H,3}) = (-1,-1)_v(a,b)_v$, *per a qualsevol plaça* v *de* $\mathbb{Q}$.

(v) $n_{H,4} \overset{\mathbb{Z}}{\to} n_{H,3} \overset{\mathbb{Z}}{\to} -n_{H,2}$.

(vi) $n_{H,2}$, $n_{H,3}$ *i* $n_{H,4}$ *són formes* $\mathrm{SL}(n,\mathbb{Z})$*-reduïdes.*

(vii) $n_{H,4}$ *és una forma primitiva; si* $\mathrm{mcd}(a,b) = 1$, *llavors* $n_{H,3}$ *i* $n_{H,2}$ *també són primitives.*

DEMOSTRACIÓ: Els apartats (ii) i (iii) s'obtenen directament en comprovar els possibles signes dels valors de la diagonal de les formes, segons els signes de a i b.

Per a provar (iv), calculem l'invariant de Hasse-Witt d'una forma quadràtica, en funció dels símbols de Hilbert locals (cf. [Ser73]). Per a la forma $n_{H,3}$, obtenim les igualtats següents:

$$\begin{aligned}
\varepsilon_v(n_{H,3}) &= (-a,-b)_v(-a,ab)_v(-b,ab)_v \\
&= (-a,-b)_v(-a,a)_v(-a,b)_v(-b,a)_v(-b,b)_v \\
&= (-a,-b)_v(-a,b)_v(-b,a)_v \\
&= (-a,-1)_v(a,-b)_v \\
&= (-1,-1)_v(a,-1)_v(a,-b)_v \\
&= (-1,-1)_v(a,b)_v.
\end{aligned}$$

Per a la forma $n_{H,4}$, obtenim que $\varepsilon_v(n_{H,4}) = \varepsilon_v(n_{H,3})(1,-a)_v(1,-b)_v(1,ab)_v$ i notem que $(1,\alpha)_v = 1$ per a qualsevol plaça v i qualsevol $\alpha \in \mathbb{Q}$.

Els resultats dels apartats restants s'obtenen fàcilment a partir de les definicions corresponents (cf. cap 4). □

5.1.2 Relacions entre els invariants.

Podem reformular els resultats de la secció anterior, que relacionaven els isomorfismes i les isometries, en la proposició següent.

5.1.9 Proposició. *Siguin* H *i* H' $\mathbb{Q}$*-àlgebres de quaternions i considerem les formes quadràtiques quaternàries, ternàries i binàries associades. Aleshores, són equivalents:*

(i) $H \overset{\mathbb{Q}}{\simeq} H'$.

(ii) $n_{H,4} \overset{\mathbb{Q}}{\sim} n_{H',4}$.

(iii) $n_{H,3} \overset{\mathbb{Q}}{\sim} n_{H',3}$.

A més, $n_{H,2} \overset{\mathbb{Q}}{\sim} n_{H',2}$ *si, i només si,* $H \overset{\mathbb{Q}}{\cong} H'$ *i* $\mathrm{disc}_{\mathbb{Q}}(n_{H,2}) = \mathrm{disc}_{\mathbb{Q}}(n_{H',2})$. □

Com a corol·lari, explicitant les condicions perquè dues formes quadràtiques ternàries siguin equivalents, s'obté de nou la caracterització dels isomorfismes entre àlgebres de quaternions en funció de la igualtat dels discriminants (cf. 1.1.7(ii)).

5.1.10 Corol·lari. *Siguin* H *i* H' $\mathbb{Q}$*-àlgebres de quaternions. Aleshores,*

$$H \overset{\mathbb{Q}}{\cong} H' \Longleftrightarrow D_H = D_{H'}.$$

DEMOSTRACIÓ: Posem $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ i $H' = \left(\frac{a',b'}{\mathbb{Q}}\right)$. Per la proposició anterior, les àlgebres H i H' són $\mathbb{Q}$-isomorfes si les formes ternàries corresponents són $\mathbb{Q}$-equivalents. Ara bé, $n_{H,3} =< -a, -b, ab >$ i $n_{H',3} =< -a', -b', a'b' >$ són $\mathbb{Q}$-equivalents si, i només si, tenen el mateix discriminant sobre $\mathbb{Q}$, el mateix invariant de Hasse-Witt i la mateixa signatura (cf. [Ser73]).

Directament tenim la igualtat de discriminants, ja que $\mathrm{disc}_{\mathbb{Q}}(n_{H,3}) = a^2b^2 = 1 = (a')^2(b')^2 = \mathrm{disc}_{\mathbb{Q}}(n_{H',3})$. Per 5.1.8(ii), una forma nòrmica ternària com les anterior només pot tenir dues signatures possibles, $(3,0)$ i $(1,2)$, segons que el símbol de Hilbert local a l'infinit prengui el valor 1 o -1. Així, la igualtat de signatures es correspon amb la igualtat $(a,b)_\infty = (a',b')_\infty$. Per 5.1.8(iv), la igualtat dels invariants de Hasse-Witt, per a cada plaça finita, és equivalent a la igualtat dels símbols de Hilbert locals $(a,b)_v = (a',b')_v$.

Així, les formes $n_{H,3}$ i $n_{H',3}$ són equivalents sobre $\mathbb{Q}$ si, i només si, els símbols $(a,b)_v = (a',b')_v$ coincideixen en totes les places. Per la definició de discriminant de l'àlgebra de quaternions, això és exactament equivalent a la igualtat de discriminants $D_H = D_{H'}$. □

La proposició següent relaciona l'invariant de Hasse-Witt de les formes quadràtiques nòrmiques amb l'invariant de Hasse de l'àlgebra de quaternions.

5.1.11 Proposició. *Sigui* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i considerem les formes quadràtiques* $n_{H,2}$ *i* $n_{H,3}$*, associades a* H*. Aleshores,*

(i) $\varepsilon_v(n_{H,2}) = \varepsilon\left(\frac{a,b}{\mathbb{Q}}\right)_v$.

$$\text{(ii)}\ \varepsilon_v(n_{H,3}) = \begin{cases} \varepsilon\left(\dfrac{a,b}{\mathbb{Q}}\right)_v & si\ v \neq 2,\infty, \\ -\varepsilon\left(\dfrac{a,b}{\mathbb{Q}}\right)_v & si\ v = 2,\infty. \end{cases}$$

DEMOSTRACIÓ: D'una banda l'invariant de Hasse $\varepsilon\left(\dfrac{a,b}{\mathbb{Q}}\right)_v$ coincideix amb el símbol de Hilbert local $(a,b)_v$. D'altra banda, el símbols de Hasse-Witt de les formes $n_{H,3}$ i $n_{H,2}$ també s'expressen en funció del símbols de Hilbert locals.

Per a la forma $n_{H,2}$ s'obté directament $\varepsilon_v(n_{H,2}) = (a,b)_v$. Això demostra (i).

Per a provar (ii), apliquem la igualtat $\varepsilon_v(n_{H,3}) = (-1,-1)_v(a,b)_v$ (cf. 5.1.8 (v)). Substituint el valor de $(-1,-1)_v$, en funció de v, s'obté el que volíem demostrar. □

És coneguda la caracterització de les àlgebres de quaternions no ramificades en funció de les propietats de les formes quadràtiques nòrmiques associades, que resumim en la proposició següent.

5.1.12 Proposició. *Sigui* $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i siguin* $n_{H,4}$ *i* $n_{H,3}$ *les formes nòrmiques associades. Són equivalents:*

i) $H \simeq \mathrm{M}(2,\mathbb{Q})$.

ii) $n_{H,4}$ *és* $\mathbb{Q}$*-isòtropa.*

iii) $n_{H,3}$ *és* $\mathbb{Q}$*-isòtropa.*

iv) $n_{H,2}$ *represesenta l'1 sobre* $\mathbb{Q}$.

v) $a \in N_{L|\mathbb{Q}}(L)$, *on* $L = \mathbb{Q}(\sqrt{b})$. □

Estenem aquesta proposició a les àlgebres ramificades, de manera que permet caracteritzar el discriminant d'una àlgebra de quaternions a partir de propietats de les formes quadràtiques nòrmiques associades.

Recordem que $S_1(f)$ denota el conjunt de primers p tals que la forma f és $\mathbb{Q}_p$-anisòtropa.

5.1.13 Proposició. *Siguin H una $\mathbb{Q}$-àlgebra de quaternions i p un nombre primer. Són equivalents:*

(i) $p|D_H$.

(ii) $n_{H,4}$ *és anisòtropa a* $\mathbb{Q}_p$.

(iii) $n_{H,3}$ *és anisòtropa a* $\mathbb{Q}_p$.

És a dir, $D_H = \prod_{p\in S_1(n_{H,4})} p = \prod_{p\in S_1(n_{H,3})} p.$

DEMOSTRACIÓ: D'una banda, sabem que per als primers $p \mid D_H$ es té que $(a,b)_p = -1$. D'altra banda, la forma $n_{H,4}$ és $\mathbb{Q}_p$-isòtropa si, i només si, $\varepsilon_p(n_{H,4}) = (-1,-1)_p$, ja que $\mathrm{disc}_{\mathbb{Q}_p}(n_{H,4}) = 1$. Com que per 5.1.8(v) tenim que $\varepsilon_v(n_{H,4}) = (-1,-1)_v(a,b)_v$, el fet de ser anisòtropa sobre $\mathbb{Q}_p$ equival al fet que $(a,b)_p = -1$. Això demostra l'equivalència de (i) i (ii).

Per a la forma ternària $n_{H,3}$, la condició d'isotropia s'expressa també en funció de l'invariant de Hasse-Witt: $\varepsilon_p(n_{H,3}) = (-1, -\mathrm{disc}_{\mathbb{Q}_p}(n_{H,3}))_p$. Tenim també que $\mathrm{disc}_{\mathbb{Q}_p}(n_{H,3}) = 1$. Així, obtenim una condició anàloga al cas anterior. Com que $\varepsilon_p(n_{H,3}) = \varepsilon_p(n_{H,4})$, és clar que (iii) també és equivalent als apartats anteriors. □

La proposició següent relaciona el caràcter definit o indefinit de l'àlgebra amb el caràcter definit o indefinit de les formes associades.

5.1.14 Proposició. *Siguin H una $\mathbb{Q}$-àlgebra de quaternions i $n_{H,i}$, per a $i = 2,3,4$, les formes nòrmiques associades. Aleshores,*

(i) *H és definida* $\Leftrightarrow$ *$n_{H,4}$ és definida positiva,*
$\Leftrightarrow$ *$n_{H,3}$ és definida positiva,*
$\Leftrightarrow$ *$n_{H,2}$ és definida negativa.*

(ii) *H és indefinida* $\Leftrightarrow$ *$n_{H,4}$ és indefinida,*
$\Leftrightarrow$ *$n_{H,3}$ és indefinida,*
$\Leftrightarrow$ *$n_{H,2}$ és definida positiva o indefinida.*

DEMOSTRACIÓ: Una $\mathbb{Q}$-àlgebra de quaternions H és definida si, i només si, $H \otimes \mathbb{R}$ és un cos, el cos dels quaternions de Hamilton. Si $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, això

està caracteritzat pel valor del símbol de Hilbert sobre $\mathbb{R}$, $(a,b)_\infty = -1$, la qual cosa equival al fet que a i b siguin ambdós negatius. Aquesta mateixa condició determina el caràcter de les formes nòrmiques. □

5.1.3 Les formes nòrmiques i les K_σ-formes

En primer lloc, recollim en els dos lemes següents els càlculs dels determinants, les formes adjuntes, recíproques i polars, i els nivells de les formes nòrmiques associades.

5.1.15 Lema. *Sigui* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions. Considerem la forma nòrmica ternària* $n_{H,3}$ *associada a* H. *Suposem que* H *és indefinida i considerem* $a > 0$. *Aleshores,*

(i) $\det_1(n_{H,3}) = a^2b^2$ *i* $\mathrm{d}_1(n_{H,4}) = -a|b|$.

(ii) $\mathrm{ad}(n_{H,3})(Y,Z,T) = -ab^2Y^2 - a^2bZ^2 + abT^2$; *en particular, se satisfà* $\mathrm{ad}(n_{H,3}) \overset{\mathbb{Q}}{\sim} n_{H,3}$.

(iii) $\mathrm{rec}_1(n_{H,3})(Y,Z,T) = \begin{cases} bY^2 + aZ^2 - T^2 & si\ b > 0, \\ -bY^2 - aZ^2 + T^2 & si\ b \leq 0. \end{cases}$

(iv) $\mathrm{N}(n_{H,3}) = 4a|b|$.

(v) $\mathrm{pol}(n_{H,3})(Y,Z,T) = -bY^2 - aZ^2 + T^2$. □

5.1.16 Lema. *Sigui* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions. Considerem la forma nòrmica quaternària* $n_{H,4}$ *associada a* H. *Suposem que* H *és indefinida i considerem* $a > 0$. *Aleshores,*

(i) $\det_1(n_{H,4}) = a^2b^2$, $\mathrm{d}_1(n_{H,4}) = -a|b|$, $\mathrm{d}_2(n_{H,4}) = -4a|b|$.

(ii) $\mathrm{ad}(n_{H,4})(X,Y,Z,T) = a^2b^2X^2 - ab^2Y^2 - a^2bZ^2 + abT^2$; *en particular,* $\mathrm{ad}(n_{H,4}) \overset{\mathbb{Q}}{\sim} n_{H,4}$.

(iii) $\mathrm{rec}_1(n_{H,4})(X,Y,Z,T) = \begin{cases} -abX^2 + bY^2 + aZ^2 - T^2 & si\ b > 0, \\ abX^2 - bY^2 - aZ^2 + T^2 & si\ b < 0. \end{cases}$
$\mathrm{rec}_2(n_{H,4}) = 2\,\mathrm{rec}_1(n_{H,4})$.
A més, $\mathrm{rec}_1(n_{H,4})(X,Y,Z,T) = \mathrm{d}_1(n_{H,4})X^2 \oplus \mathrm{rec}_1(n_{H,3})(Y,Z,T)$.

(iv) $\mathrm{N}(n_{H,4}) = 4a|b|$.

(v) $\mathrm{pol}(n_{H,4})(X,Y,Z,T) = abX^2 - bY^2 - aZ^2 + T^2$. □

Notem que si les formes fossin definides, canviaria el signe de d_σ i, per tant, el signe de les formes recíproques.

A continuació explicitem la relació entre la signatura de les formes nòrmiques i la de les seves formes adjuntes i recíproques. Notem que el caràcter definit o indefinit es conserva, però hi ha algun canvi en els signes.

5.1.17 Proposició. *Sigui H una $\mathbb{Q}$-àlgebra de quaternions. Tenim les relacions següents.*

(i) $\mathrm{sign}(n_{H,i}) = \mathrm{sign}(\mathrm{ad}(n_{H,i})) = \mathrm{sign}(\mathrm{pol}(n_{H,i}))$, *per a* $i = 3, 4$.

(ii) $\mathrm{sign}(n_{H,4}) = \mathrm{sign}(\mathrm{rec}_\sigma(n_{H,4}))$.

(iii) *La forma* $\mathrm{rec}_1(n_{H,3})$ *té el mateix caràcter, definit o indefinit, que la forma* $n_{H,3}$. *Si* $n_{H,3}$ *és una forma indefinida, de signatura* $(1,2)$, *aleshores* $\mathrm{sign}(\mathrm{rec}_1(n_{H,3})) = (2,1)$.

DEMOSTRACIÓ: A partir dels càlculs explícits de les formes adjuntes d'aquestes formes nòrmiques, és clar que la signatura de l'adjunta coincideix amb la de la forma. Notem que això en general només és cert per a les formes binàries, per a les quals la forma i la seva adjunta són equivalents. Per a qualsevol forma quadràtica, la forma polar s'obté multiplicant la forma adjunta per un nombre racional positiu. Això demostra (i).

Per a estudiar la signatura de la forma recíproca només cal tenir en compte el signe de $\mathrm{d}_1(n_{H,3})$ i $d_\sigma(n_{H,4})$. Aquest signe és positiu si la forma és definida positiva i és negatiu si la forma és indefinida. Observem que, per al cas quaternari, si la signatura és $(2,2)$, en dividir per $d_\sigma(n_{H,4})$ continua sent $(2,2)$. En canvi, si $n_{H,3}$ és indefinida de signatura $(1,2)$, obtenim que $\mathrm{sign}(\mathrm{rec}_1(n_{H,3})) = (2,1)$. □

A partir dels lemes anteriors, utilitzant la caracterització de les K_σ-formes, cf. 4.3.10 i 4.3.12, i el fet que la forma nòrmica és una forma unitària, obtenim el teorema següent.

5.1.18 Teorema. *Siguin* $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions indefinida i* $n_{H,4}$ *i* $n_{H,3}$ *les formes nòrmiques associades. Aleshores,*

(i) $n_{H,4}$ *és una* K_σ*-forma, per a* $\sigma = 1, 2$*; a més, és una forma principal.*

(ii) $n_{H,3}$ *és una* K_1*-forma.* □

5.2 Formes traça d'àlgebres de quaternions

5.2.1 Definició i propietats

Sigui $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ una $\mathbb{Q}$-àlgebra de quaternions, $a, b \in \mathbb{Z}$, lliures de quadrats, amb base $\{1, i, j, ij\}$. Podem associar a H altres formes quadràtiques diferents de les formes nòrmiques, que doten també l'àlgebra de quaternions d'estructura d'espai quadràtic.

Per 1.1.13, la traça indueix una forma bilineal simètrica donada per la traça del producte. Si la normalitzem, obtenim:

$$\begin{array}{rccc} B' : & H \times H & \longrightarrow & \mathbb{Q} \\ & (\alpha, \beta) & \mapsto & \frac{1}{2}\mathrm{tr}(\alpha\beta). \end{array}$$

La forma quadràtica associada és:

$$\begin{array}{ccc} H & \longrightarrow & \mathbb{Q} \\ \alpha & \mapsto & B'(\alpha, \alpha) = \frac{1}{2}\mathrm{tr}(\alpha^2). \end{array}$$

5.2.1 Remarca. Considerem la forma bilineal B' restringida a l'espai dels quaternions purs, $B'_{|H_0}$. Per a $u, v \in H_0$ tenim que $B'_{|H_0}(u, v) = \frac{1}{2}(uv + vu)$. Així, a l'espai $(H_0, B'_{|H_0})$, u i v són ortogonals si, i només si, u i v anticommuten a H_0. Per tant, $\{i, j, k\}$ és una base ortogonal de H_0. Així, $\{1, i, j, k\}$ és una base ortogonal de l'espai quadràtic regular (H, B'). □

5.2.2 Definició. Anomenem formes traça associades a la $\mathbb{Q}$-àlgebra de quaternions H les expressions de la forma quadràtica anterior sobre H i sobre H_0 en les bases $\{1, i, j, ij\}$ i $\{i, j, ij\}$, respectivament. Les denotem per $t_{H,4}$ i $t_{H,3}$, respectivament. □

Explícitament, a l'àlgebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ li associem

la forma quaternària	$t_{H,4}(X, Y, Z, T) = X^2 + aY^2 + bZ^2 - abT^2$,
la forma ternària	$t_{H,3}(Y, Z, T) = aY^2 + bZ^2 - abT^2$.

Hi ha una bona relació entre aquestes formes quadràtiques traça i les formes quadràtiques nòrmiques tractades en la secció anterior; alguns resultats provats per a les formes nòrmiques tenen també el seu anàleg en aquestes noves formes. Ho expressem explícitament en el lema següent.

5.2.3 Lema. *Considerem les formes quadràtiques nòrmiques i traça associades a una àlgebra de quaternions* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$.

(i) *Per a tot* $\lambda \in \mathbb{Q}$, $t_{H,4}(\lambda) = \lambda^2 = n_{H,4}(\lambda)$.

(ii) $t_{H,3}(Y,Z,T) = -n_{H,4}(Y,Z,T)$.

(iii) $t_{H,4}$ *és una forma quadràtica unitària, però no és multiplicativa.*

(iv) $t_{H,4}(X,Y,Z,T) \sim X^2 \oplus t_{H,3}(Y,Z,T)$.

(v) *Les formes quadràtiques* $t_{H,4}$ *i* $t_{H,3}$ *són de coeficients enters.* □

De manera anàloga a la forma nòrmica, obtenim el resultat següent, que dóna una equivalència entre els isomorfismes d'aquestes $\mathbb{Q}$-àlgebres i les isometries d'aquests $\mathbb{Q}$-espais quadràtics.

5.2.4 Proposició. *Siguin* H *i* H' *dues àlgebres de quaternions sobre* $\mathbb{Q}$. *Considerem la seva estructura com a espai quadràtic amb la forma quadràtica donada per la traça. Aleshores, són equivalents:*

(i) H *i* H' *són* $\mathbb{Q}$*-àlgebres isomorfes.*

(ii) $(H, t_{H,4})$ *i* $(H', t_{H',4})$ *són* $\mathbb{Q}$*-espais quadràtics isomètrics.*

(iii) $(H_0, t_{H,3})$ *i* $(H'_0, t_{H',3})$ *són* $\mathbb{Q}$*-espais quadràtics isomètrics.*

DEMOSTRACIÓ: L'isomorfisme de $\mathbb{Q}$-àlgebres de (i) indueix una forma quadràtica en H' a partir de la forma quadràtica traça associada a H. Per 1.1.16(iv), aquesta forma quadràtica induïda coincideix amb la forma traça associada a H'; per tant, obtenim que $(H, t_{H,4})$ i $(H', t_{H',4})$ són $\mathbb{Q}$-espais quadràtics isomètrics.

Per a veure que (ii) implica (iii), de manera anàloga a les formes nòrmiques, s'utilitza el teorema de Witt i el fet que la forma $t_{H,4}(X,Y,Z,T) = X^2 \oplus t_{H,3}(Y,Z,T)$.

Finalment, veurem que (iii) implica (i). Suposem que $(H_0, t_{H,3})$ i $(H'_0, t_{H',3})$ són $\mathbb{Q}$-espais quadràtics isomètrics. Aleshores, és clar que els espais $(H_0, n_{H,3})$ i $(H'_0, n_{H',3})$ també són $\mathbb{Q}$-isomètrics, pel lema 5.2.3(ii). Per a les formes nòrmiques, és conegut que, amb la construcció d'àlgebres de Clifford, aquesta isometria implica que les àlgebres de quaternions H i H' són $\mathbb{Q}$-àlgebres isomorfes. □

5.2.2 Relacions entre els invariants.

A continuació llistem algunes propietats de les formes quadràtiques traça.

5.2.5 Proposició. *Siguin* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i* $t_{H,4}$ *i* $t_{H,3}$ *les formes quadràtiques traça associades a* H.

(i) $\det_1(t_{H,4}) = \det_1(t_{H,3}) = -a^2b^2$, $\operatorname{disc}_{\mathbb{Q}}(t_{H,4}) = \operatorname{disc}_{\mathbb{Q}}(t_{H,3}) = -1$.

(ii) $t_{H,4}$ *és sempre una forma indefinida. Si* H *és definida, té signatura* $(1,3)$*; si* H *és indefinida, té signatura* $(3,1)$.

(iii) $t_{H,3}$ *és una forma indefinida, de signatura* $(2,1)$*, si* H *és indefinida;* $t_{H,3}$ *és una forma definida negativa si* H *és definida; en particular,* $t_{H,3}$ *no pot ser mai definida positiva.*

(iv) $\varepsilon_v(t_{H,4}) = \varepsilon_v(t_{H,3}) = (a,b)_v$*, per a qualsevol plaça* v *de* $\mathbb{Q}$.

(v) $t_{H,4} \xrightarrow{\mathbb{Z}} t_{H,3}$.

(vi) $t_{H,3}$ *i* $t_{H,4}$ *són formes* $\mathrm{SL}(n,\mathbb{Z})$*-reduïdes.*

(vii) $t_{H,4}$ *és un forma primitiva. Si* $\operatorname{mcd}(a,b) = 1$*, llavors* $t_{H,3}$ *també ho és.*

DEMOSTRACIÓ: Aplicant directament la definició de determinant i discriminant, obtenim (i).

Els apartats (ii) i (iii) s'obtenen en comprovar els possibles signes dels valors de la diagonal de les formes, segons els signes de a i b.

Calculem l'invariant de Hasse-Witt, en una plaça v de $\mathbb{Q}$, de la forma $t_{H,3}$,

$$\begin{aligned}\varepsilon_v(t_{H,3}) &= (a,b)_v(a,-ab)_v(b,-ab)_v = \\ &= (a,b)_v(a,-a)_v(a,b)_v(b,a)_v(b,-b)_v = \\ &= (a,b)_v.\end{aligned}$$

Per a la forma $t_{H,4}$, desenvolupant l'invariant de Hasse-Witt local, obtenim que $\varepsilon_v(t_{H,4}) = \varepsilon_v(t_{H,3})(1,a)_v(1,b)_v(1,-ab)_v$. Com en el cas de la forma nòrmica, deduïm (iv), ja que $(1,\alpha)_v = 1$ per a qualsevol plaça v i qualsevol $\alpha \in \mathbb{Q}$.

Per als resultats dels apartats (v), (vi) i (vii) només cal aplicar les definicions corresponents. □

El corol·lari següent mostra la relació entre els invariants de Hasse-Witt de les formes quadràtiques traça, $t_{H,3}$ i $t_{H,4}$, i l'invariant de Hasse de l'àlgebra de quaternions H.

5.2.6 Corol·lari. *Sigui* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i siguin* $t_{H,3}$ *i* $t_{H,4}$ *les formes traça associades. Aleshores, per a tota plaça* v *de* $\mathbb{Q}$*, se satisfà que*

$$\varepsilon_v(t_{H,4}) = \varepsilon_v(t_{H,3}) = \varepsilon\left(\frac{a,b}{\mathbb{Q}}\right)_v.$$

DEMOSTRACIÓ: D'una banda, pel teorema de classificació de les àlgebres de quaternions, l'invariant de Hasse de l'àlgebra $\varepsilon\left(\frac{a,b}{\mathbb{Q}}\right)_v$ coincideix amb el símbol de Hilbert local $(a,b)_v$. D'altra banda, l'invariant de Hasse-Witt de les formes traça també coincideix amb el símbol de Hilbert (cf. lema 5.2.5(iv)). □

El corol·lari següent relaciona directament els invariants de Hasse-Witt de les formes traça amb el discriminant de l'àlgebra de quaternions. Així, tenim una manera de trobar els factors primers del discriminant de la $\mathbb{Q}$-àlgebra de quaternions a partir de les formes traça. Recordem que denotem per $S_2(f)$ el conjunt de primers p tals que l'invariant de Hasse-Witt de la forma f a $\mathbb{Q}_p$ és igual a -1.

5.2.7 Corol·lari. *Sigui* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i siguin* $t_{H,3}$ *i* $t_{H,4}$ *les formes traça associades. Aleshores,*

$$D_H = \prod_{p \in S_2(t_{H,3})} p = \prod_{p \in S_2(t_{H,4})} p. \ \square$$

5.2.3 Les formes traça i les K-formes

A continuació generalitzarem les definicions de forma recíproca i K_σ-forma donades en la secció 4.3, per tal d'aplicar-les a les formes traces.

5.2.8 Definició. Suposem que f és una forma quadràtica de coeficients a $\mathbb{Z}$ tal que $|\det_\sigma(f)|$ és un quadrat perfecte. Posem $\mathrm{d}^+_\sigma(f) = +\sqrt{|\det_\sigma(f)|}$ si la forma quadràtica és definida positiva i $\mathrm{d}^+_\sigma(f) = -\sqrt{|\det_\sigma(f)|}$ si la forma quadràtica és indefinida; no considerarem formes quadràtiques definides negatives. □

5.2.9 Definicions. La forma σ^+-recíproca de f és $\mathrm{rec}^+_\sigma(f) := \dfrac{1}{\mathrm{d}^+_\sigma(f)}\,\mathrm{ad}(f)$. Diem que una forma quadràtica f és una K^+_σ-forma si f i $\mathrm{rec}^+_\sigma(f)$ tenen coeficients enters. Anàlogament, diem que una K^+_1-forma f és principal si representa l'1 sobre $\mathbb{Z}$. □

5.2.10 Remarca. És clar que si f és una K_σ-forma, aleshores f també és una K^+_σ-forma. Així, les definicions anteriors generalitzen les definicions de 4.3. Els resultats obtinguts per a K_σ-formes que només depenen del fet que els coeficients siguin o no enters s'estenen de forma natural a K^+_σ-formes. □

5.2.11 Lema. *Sigui* $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i* $t_{H,3}$ *la forma ternària traça associada. Suposem que* H *és indefinida i considerem* $a > 0$. *Aleshores,*

(i) $\det_1(t_{H,3}) = -a^2b^2$, $\mathrm{d}^+_1(t_{H,4}) = -a|b|$.

(ii) $\mathrm{ad}(t_{H,3})(Y,Z,T) = \mathrm{ad}(n_{H,3})(Y,Z,T) = -ab^2Y^2 - a^2bZ^2 + abT^2$.

(iii) $\mathrm{rec}^+_1(t_{H,3})(Y,Z,T) = \begin{cases} bY^2 + aZ^2 - T^2 & \text{si } b > 0, \\ -bY^2 - aZ^2 + T^2 & \text{si } b < 0. \end{cases}$
De fet, $\mathrm{rec}^+_1(t_{H,3}) = \mathrm{rec}_1(n_{H,3})$.

(iv) $\mathrm{N}(t_{H,3}) = 4a|b|$.

(v) $\mathrm{pol}(t_{H,3})(Y,Z,T) = -bY^2 - aZ^2 + T^2$. □

5.2.12 Lema. *Sigui* $H = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions i* $t_{H,4}$ *la forma quaternària traça associada. Suposem que* H *és indefinida i considerem* $a > 0$. *Aleshores,*

(i) $\det_1(t_{H,4}) = -a^2b^2$, $\mathrm{d}_1^+(t_{H,4}) = -a|b|$ *i* $\mathrm{d}_2^+(t_{H,4}) = -4a|b|$.

(ii) $\mathrm{ad}(t_{H,4})(X,Y,Z,T) = -a^2b^2X^2 - ab^2Y^2 - a^2bZ^2 + abT^2$.

(iii) $\mathrm{rec}_1^+(t_{H,4})(X,Y,Z,T) = \begin{cases} abX^2 + bY^2 + aZ^2 - T^2 & \text{si } b > 0, \\ -abX^2 + bY^2 - aZ^2 + T^2 & \text{si } b < 0. \end{cases}$
$\mathrm{rec}_2^+(t_{H,4}) = 2\,\mathrm{rec}_1^+(t_{H,4})$.
A més, $\mathrm{rec}_1(n_{H,4})(X,Y,Z,T) = \mathrm{d}_1(n_{H,4})X^2 \oplus \mathrm{rec}_1(n_{H,3})(Y,Z,T)$.

(iv) $\mathrm{N}(t_{H,4}) = 4|ab|$.

(v) $\mathrm{pol}(t_{H,4})(X,Y,Z,T) = -abX^2 - bY^2 - aZ^2 + T^2$. □

Dels resultats d'aquests lemes sobre les formes traça, conjuntament amb la generalització dels resultats de la secció 4.3 al cas de les K_σ^+-formes, i el fet que la forma traça és una forma unitària, deduïm el teorema següent.

5.2.13 Teorema. *Siguin* $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ *una àlgebra de quaternions indefinida i* $t_{H,4}$ *i* $t_{H,3}$ *les formes traça associades. Aleshores,*

(i) $t_{H,4}$ *és una* K_σ^+*-forma principal, per a* $\sigma = 1, 2$.

(ii) $t_{H,3}$ *és una* K_1^+*-forma.* □

5.3 Correspondència entre àlgebres de quaternions i formes quadràtiques

Recordem que hem assignat a cada $\mathbb{Q}$-àlgebra de quaternions una forma nòrmica (cf. 5.1) i una forma traça (cf. 5.2), de manera que dues formes nòrmiques, o traces, són $\mathbb{Q}$-equivalents si, i només si les $\mathbb{Q}$-àlgebres de quaternions són isomorfes. Així, tenim aplicacions del conjunt de classes d'isomorfisme de $\mathbb{Q}$-àlgebres de quaternions en el de formes quadràtiques sobre $\mathbb{Q}$ de 3 o 4 variables. En aquesta secció, estudiarem els conjunts imatge d'aquestes aplicacions i definirem bijeccions entre aquests conjunts. Les demostracions són constructives i donen de manera explícita l'aplicació inversa.

5.3.1 Notació. D'una banda, considerem el conjunt de les $\mathbb{Q}$-àlgebres de quaternions mòdul $\mathbb{Q}$-isomorfisme, que podem identificar amb $\mathrm{Br}_2(\mathbb{Q})$. D'altra banda, considerem els conjunts de formes quadràtiques enteres regulars

següents:

$$Q_4^+ := \{f : f \text{ forma quaternària no definida negativa, } \det_1(f) = \lambda^2 \text{ a } \mathbb{Q}\},$$

$$Q_4^- := \{f : f \text{ forma quaternària, } \det_1(f) = -\lambda^2 \text{ a } \mathbb{Q}\},$$

$$Q_3^+ := \{f : f \text{ forma ternària, } \det_1(f) = \lambda^2 \text{ a } \mathbb{Q}\},$$

$$Q_3^- := \{f : f \text{ forma ternària, } \det_1(f) = -\lambda^2 \text{ a } \mathbb{Q}\}.$$

Denotem per $\mathcal{C}(Q_i^+)$ i $\mathcal{C}(Q_i^-)$, amb $i = 3, 4$, els conjunts de formes quadràtiques anteriors mòdul la relació de $\mathbb{Q}$-equivalència. Per a una forma quadràtica f, recordem que hem definit els conjunts de places $S_1(f)$ i $S_2(f)$ (cf. secció 4.2). □

En primer lloc, obtenim una bijecció entre els conjunts de formes ternàries i els conjunts de formes quaternàries.

5.3.2 Proposició. *Les aplicacions*

$$\begin{array}{ccc} \mathcal{C}(Q_3^+) & \longrightarrow & \mathcal{C}(Q_4^+), \\ f(Y,Z,T) & \mapsto & X^2 + f(Y,Z,T) \end{array} \qquad \begin{array}{ccc} \mathcal{C}(Q_3^-) & \longrightarrow & \mathcal{C}(Q_4^-), \\ f(Y,Z,T) & \mapsto & X^2 + f(Y,Z,T) \end{array}$$

són bijectives.

DEMOSTRACIÓ: Notem que ambdues aplicacions estan ben definides, ja que una forma i la seva imatge, per a qualsevol de les dues aplicacions, tenen el mateix determinant. A més, és clar que les formes imatge no seran mai definides negatives.

La injectivitat de les dues aplicacions també és clara, utilitzant el teorema de Witt. Vegem l'exhaustivitat per a cada aplicació.

Considerem una forma quadràtica $g \in \mathcal{C}(Q_4^+)$. Provarem que $g \xrightarrow{\mathbb{Q}} 1$. Per ser una forma de quatre variables, tenim que $g \xrightarrow{\mathbb{Q}_p} 1$ per a tota plaça finita p. Si g és una forma indefinida, és clar que $g \xrightarrow{\mathbb{R}} 0$ i, per 4.2.3, tenim que $g \xrightarrow{\mathbb{R}} 1$. Si g és una forma definida positiva, aleshores $g \xrightarrow{\mathbb{R}} 1$ si, i només si, $g(X_1, \ldots, X_4) - X_0^2$ és una forma de cinc variables que representa el 0 sobre $\mathbb{R}$. Ara bé, aquesta forma és indefinida, per ser g definida positiva; per tant, representa el 0. En qualsevol cas, tenim que la forma quadràtica g de quatre variables, regular i no definida negativa, representa el 0 sobre $\mathbb{R}$ i sobre $\mathbb{Q}_p$, per a tot p; per tant, deduïm que $g \xrightarrow{\mathbb{Q}} 1$. Ara bé, si apliquem de nou els

resultats clàssics de representació i equivalència (cf. [Ser73] o bé [BS66]), com que g representa l'1 sobre $\mathbb{Q}$, tenim que g és $\mathbb{Q}$-equivalent a una forma $X^2 + f(Y,Z,T)$. És clar que $\det_1(f) = \det_1(g)$; per tant, $f \in \mathcal{C}(Q_3^+)$. Com que $\det_1(f) > 0$, f no pot ser definida negativa i té el mateix caràcter que g. Això demostra l'exhaustivitat de l'aplicació de $\mathcal{C}(Q_3^+)$ a $\mathcal{C}(Q_4^+)$.

Considerem ara $g \in \mathcal{C}(Q_4^-)$. Notem que g és necessàriament una forma indefinida. El mateix argument anterior prova que g representa l'1 sobre $\mathbb{Q}$; per tant, $g(X,Y,Z,T) \overset{\mathbb{Q}}{\sim} X^2 + f(Y,Z,T)$. És clar que la forma $f \in \mathcal{C}(Q_3^-)$, la qual cosa demostra l'exhaustivitat de l'aplicació de $\mathcal{C}(Q_3^-)$ a $\mathcal{C}(Q_4^-)$. □

A continuació, el teorema següent prova la bijecció entre $\mathrm{Br}_2(\mathbb{Q})$ i els conjunts de formes corresponents, a partir de les propietats de les formes nòrmiques i les formes traça, provades a les seccions anteriors, i els resultats de teoria de representació i equivalència de formes (cf. secció 4.2). Notem que les bijeccions que obtenim en els apartats (i) i (iii) són explícites en els dos sentits. Així, a partir d'una forma quadràtica en les condicions predeterminades construïm explícitament una àlgebra de quaternions que té com a forma nòrmica o bé forma traça una forma equivalent a la donada inicialment. En particular, deduïm una manera de construir àlgebres de quaternions de discriminant predeterminat a partir d'invariants de la forma quadràtica inicial. Això permet una reformulació, en els apartats (ii) i (iv), dels resultats 5.1.13 i 5.2.7.

5.3.3 Teorema. *Considerem els conjunts de classes de formes quadràtiques ternàries i quaternàries anteriors.*

(i) *Les aplicacions*

$$\begin{array}{rcl} \nu_3 : \mathrm{Br}_2(\mathbb{Q}) & \longrightarrow & \mathcal{C}(Q_3^+), \\ H & \mapsto & n_{H,3} \end{array} \qquad \begin{array}{rcl} \nu_4 : \mathrm{Br}_2(\mathbb{Q}) & \longrightarrow & \mathcal{C}(Q_4^+) \\ H & \mapsto & n_{H,4}. \end{array}$$

són bijectives.

(ii) *Si* $f \in Q_3^+$, *aleshores* $\displaystyle\prod_{p \in S_1(f)} p = D_{\nu_3^{-1}(f)}$;
si $f \in Q_4^+$, *aleshores* $\displaystyle\prod_{p \in S_1(f)} p = D_{\nu_4^{-1}(f)}$.

(iii) *Les aplicacions*

$$\begin{array}{rcl} \tau_3 : \mathrm{Br}_2(\mathbb{Q}) & \longrightarrow & \mathcal{C}(Q_3^-), \\ H & \mapsto & t_{H,3} \end{array} \qquad \begin{array}{rcl} \tau_4 : \mathrm{Br}_2(\mathbb{Q}) & \longrightarrow & \mathcal{C}(Q_4^-) \\ H & \mapsto & t_{H,4}. \end{array}$$

són bijectives.

(iv) *Si* $f \in Q_3^-$, *aleshores* $\prod_{p \in S_2(f)} p = D_{\tau_3^{-1}(f)}$;
si $f \in Q_4^-$, *aleshores* $\prod_{p \in S_2(f)} p = D_{\tau_4^{-1}(f)}$.

DEMOSTRACIÓ: En primer lloc, notem que les aplicacions ν_i i τ_i, per a $i = 3, 4$, estan ben definides, ja que si canviem la base de l'àlgebra o tenim un isomorfisme d'àlgebres, les formes obtingudes són $\mathbb{Q}$-equivalents, per 5.1.7 i 5.2.4, respectivament. Dels mateixos resultats deduïm que són aplicacions injectives. Cal veure'n l'exhaustivitat.

Per a veure que ν_3 és exhaustiva, cal veure que, donada una forma quadràtica $f \in Q_3^+$, existeixen $a, b \in \mathbb{Q}$ tals que $f \overset{\mathbb{Q}}{\sim} n_{H,3}$, per a $H = \left(\frac{a,b}{\mathbb{Q}}\right)$. Llevat $\mathbb{Q}$-equivalència, podem suposar que f és diagonal; així, $f(X,Y,Z) = a_1X^2 + a_2Y^2 + a_3Z^2$ amb $a_1a_2a_3 = \lambda^2$, $a_i \in \mathbb{Z}$ lliures de quadrats. Posem $a = -a_1$ i $b = -a_2$; així, obtenim que $ab = a_1a_2 = \frac{a_1a_2}{a_3}a_3$ on $\frac{a_1a_2}{a_3} = \frac{\det_1(f)}{a_3^2} = \left(\frac{\lambda}{a_3}\right)^2 \in \mathbb{Q}^2$. Aleshores tenim que $f(X,Y,Z) \overset{\mathbb{Q}}{\sim} -aX^2 - bY^2 + abZ^2 = n_{H,3}(X,Y,Z)$, per a $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, com volíem veure.

Considerem ara l'aplicació ν_4. És clar que ν_4 s'obté composant ν_3 amb la bijecció de $C(Q_3^+)$ a $C(Q_4^+)$, definida a la proposició 5.3.2 anterior. Per tant, automàticament ν_4 és bijectiva. Això completa la demostració de (i).

L'apartat (ii) és conseqüència directa de (i), tenint en compte la proposició 5.1.7.

La demostració de (iii) és anàloga a la de (i). Per a veure que τ_3 és exhaustiva, cal provar que, donada una forma quadràtica $f \in Q_3^-$, existeixen $a, b \in \mathbb{Q}$ tals que $f \overset{\mathbb{Q}}{\sim} t_{H,3}$, per a $H = \left(\frac{a,b}{\mathbb{Q}}\right)$. Llevat $\mathbb{Q}$-equivalència, podem considerar f diagonal, $f(X,Y,Z) = a_1X^2 + a_2Y^2 + a_3Z^2$ amb $a_1a_2a_3 = \det_1(f)$, $a_i \in \mathbb{Z}$ lliures de quadrats. Ara posem $a = a_1$ i $b = a_2$; per tant, $-ab = -a_1a_2 = -\frac{a_1a_2}{a_3}a_3$, on $-\frac{a_1a_2}{a_3} = -\frac{\det_1(f)}{a_3^2} = \left(\frac{\lambda}{a_3}\right)^2 \in \mathbb{Q}^2$. Aleshores, $f(X,Y,Z) \overset{\mathbb{Q}}{\sim} aX^2 + bY^2 - abZ^2 = t_{H,3}(X,Y,Z)$, per a $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, com volíem veure.

Si utilitzem la proposició 5.3.2 anterior, l'exhaustivitat de τ_4 es dedueix de l'exhaustivitat de τ_3.

Finalment, (iv) es dedueix de (iii) aplicant propietats de la forma traça, cf. 5.2.4. □

Aquesta construcció d'una àlgebra de quaternions de discriminant predeterminat es troba implementada en el paquet `Poincare`. A la secció d'algoritmes comentem les instruccions programades.

5.4 Algoritmes i taules

Les instruccions relatives a aquest capítol fan referència a les formes nòrmiques i les formes traça associades a una àlgebra de quaternions i a la correspondència entre formes quadràtiques i àlgebres de quaternions donada a la secció 5.3.

En primer lloc, obtenim les formes nòrmiques associades a una àlgebra de quaternions $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, directament a partir dels arguments a i b, amb les instruccions `nfH4` i `nfH3`. Per a facilitar l'ús de les constants que porten associades aquestes formes, hem programat també les instruccions `detInfH` i `nivnfH`, que donen el determinant i el nivell de les formes nòrmiques de l'àlgebra, a partir dels arguments a i b.

També tenim instruccions per a calcular altres formes associades a les formes nòrmiques, com `adH3`, `adH4`, `polH3`, `polH4`, `recIH3`, `recIH4` i `rec2H4`.

Per a les formes traça, hem programat les instruccions `tfH4` i `tfH3`. Per a calcular els seus invariants i les formes quadràtiques associades es poden utilitzar les instruccions generals de formes quadràtiques comentades en el capítol 4 o bé la relació entre les formes traça i les formes nòrmiques explicitada en aquest capítol.

Hem implementat explícitament la correspondència entre formes quadràtiques i àlgebres de quaternions de la secció 5.3, utilitzant comandes de formes quadràtiques, comentades ja en el capítol anterior. Un sentit de la correspondència coincideix amb les instruccions `nfH4`, `nfH3`, `tfH4` i `tfH3`. El sentit contrari, és a dir, la determinació d'una àlgebra de quaternions H a partir de formes quadràtiques donades amb certes propietats, es troba implementat en les instruccions `Hnf4`, `Hnf3`, `Htf4` i `Htf3`.

Les taules següents recullen l'expressió explícita de les formes associades a àlgebres de quaternions, definides o bé indefinides, de discriminant $D \leq 100$, i alguns dels seus invariants.

Taula 5.1 *Formes quadràtiques ternàries associades a les $\mathbb{Q}$-àlgebres de quaternions, definides o indefinides, de discriminant $D \leq 100$.*

D	H	$f = n_{H,3} = -t_{H,3}$	$\mathrm{d}_1(f)$	$\mathrm{N}(f)$	$S_1(f)$
1	$(1,-1)$	$-X^2+Y^2-Z^2$	-1	4	$\emptyset$
2	$(-1,-1)$	$X^2+Y^2+Z^2$	1	4	$\{2\}$
3	$(-3,-1)$	$3X^2+Y^2+3Z^2$	3	12	$\{3\}$
5	$(-5,-2)$	$5X^2+2Y^2+10Z^2$	10	40	$\{5\}$
6	$(3,-1)$	$-3X^2+Y^2-3Z^2$	-3	12	$\{2,3\}$
7	$(-7,-1)$	$7X^2+Y^2+7Z^2$	7	28	$\{7\}$
10	$(2,5)$	$-2X^2-5Y^2+10Z^2$	-10	40	$\{2,5\}$
11	$(-11,-1)$	$11X^2+Y^2+11Z^2$	11	44	$\{11\}$
13	$(-13,-2)$	$13X^2+2Y^2+26Z^2$	26	52	$\{13\}$
14	$(7,-1)$	$-7X^2+Y^2+7Z^2$	-7	28	$\{2,7\}$
15	$(3,5)$	$-3X^2-5Y^2+15Z^2$	-15	60	$\{3,5\}$
17	$(-17,-3)$	$17X^2+3Y^2+357Z^2$	357	1428	$\{17\}$
19	$(-19,-1)$	$19X^2+Y^2+19Z^2$	19	76	$\{19\}$
21	$(21,-1)$	$-21X^2+Y^2-21Z^2$	-21	82	$\{3,7\}$
22	$(11,-1)$	$-11X^2+Y^2-11Z^2$	-11	44	$\{2,11\}$
23	$(-23,-1)$	$23X^2+Y^2+23Z^2$	23	92	$\{23\}$
26	$(13,2)$	$-13X^2-2Y^2+26Z^2$	-26	104	$\{2,13\}$
29	$(-29,-2)$	$29X^2+2Y^2+58Z^2$	58	232	$\{29\}$
30	$(-10,-3)$	$10X^2+3Y^2+30Z^2$	30	120	$\{2,3,5\}$
31	$(-31,-1)$	$31X^2+Y^2+31Z^2$	31	124	$\{31\}$
33	$(33,-1)$	$-33X^2+Y^2-33Z^2$	-33	132	$\{3,11\}$
34	$(34,-3)$	$-34X^2+3Y^2-102Z^2$	-102	408	$\{2,17\}$
35	$(7,5)$	$-7X^2-5Y^2+35Z^2$	-35	140	$\{5,7\}$
37	$(-37,-2)$	$37X^2+2Y^2+74Z^2$	74	296	$\{37\}$
38	$(19,-1)$	$-19X^2+Y^2-19Z^2$	-19	76	$\{2,19\}$
39	$(39,-7)$	$-39X^2+7Y^2-273Z^2$	-273	1092	$\{3,13\}$
41	$(-41,-3)$	$41X^2+3Y^2+123Z^2$	123	492	$\{41\}$
42	$(-42,-1)$	$42X^2+Y^2+42Z^2$	42	168	$\{2,3,7\}$
43	$(-43,-1)$	$43X^2+Y^2+43Z^2$	43	172	$\{43\}$
46	$(23,-1)$	$-23X^2+Y^2-23Z^2$	-23	92	$\{2,23\}$
47	$(-47,-1)$	$47X^2+Y^2+47Z^2$	47	188	$\{47\}$

D	H	$f = n_{H,3} = -t_{H,3}$	$\mathrm{d}_1(f)$	$\mathrm{N}(f)$	$S_1(f)$
51	$(3,17)$	$-3X^2 - 17Y^2 + 51Z^2$	-51	204	$\{3,17\}$
53	$(-53,-2)$	$53X^2 + 2Y^2 + 106Z^2$	106	424	$\{53\}$
55	$(-55,-13)$	$55X^2 + 13Y^2 + 715Z^2$	-715	2860	$\{5,11\}$
57	$(57,-1)$	$-57X^2 + Y^2 - 57Z^2$	-57	228	$\{3,19\}$
58	$(29,2)$	$-29X^2 - 2Y^2 + 58Z^2$	-58	232	$\{2,29\}$
59	$(-59,-1)$	$59X^2 + Y^2 + 59Z^2$	59	236	$\{59\}$
61	$(-61,-1)$	$61X^2 + Y^2 + 61Z^2$	61	244	$\{61\}$
62	$(-67,-1)$	$67X^2 + Y^2 + 67Z^2$	-67	268	$\{2,31\}$
65	$(5,13)$	$-5X^2 - 13Y^2 + 65Z^2$	-65	260	$\{5,13\}$
66	$(-66,-1)$	$66X^2 + Y^2 + 66Z^2$	66	264	$\{2,3,11\}$
67	$(-67,-1)$	$67X^2 + Y^2 + 67Z^2$	67	268	$\{67\}$
69	$(69,-1)$	$-69X^2 + Y^2 - 69Z^2$	-69	276	$\{3,23\}$
70	$(-35,-2)$	$35X^2 + 2Y^2 + 70Z^2$	70	280	$\{2,5,7\}$
71	$(-71,-1)$	$71X^2 + Y^2 + 71Z^2$	71	284	$\{71\}$
73	$(-73,-7)$	$73X^2 + Y^2 + 73Z^2$	73	292	$\{73\}$
74	$(37,2)$	$-37X^2 - 2Y^2 + 74Z^2$	-74	296	$\{2,37\}$
77	$(77,-1)$	$-77X^2 + Y^2 - 77Z^2$	-77	308	$\{7,11\}$
78	$(-6,-13)$	$6X^2 + 13Y^2 + 78Z^2$	78	312	$\{2,3,13\}$
79	$(-79,-1)$	$79X^2 + Y^2 + 79Z^2$	79	316	$\{79\}$
82	$(82,-3)$	$-82X^2 + 3Y^2 - 246Z^2$	-246	984	$\{2,41\}$
83	$(-83,-1)$	$83X^2 + Y^2 + 83Z^2$	83	332	$\{83\}$
85	$(5,17)$	$-5X^2 - 17Y^2 + 85Z^2$	-85	340	$\{5,17\}$
86	$(43,-1)$	$-43X^2 + Y^2 - 43Z^2$	-43	172	$\{2,43\}$
87	$(3,29)$	$-3X^2 - 29Y^2 + 87Z^2$	-87	348	$\{3,29\}$
89	$(-89,-3)$	$89X^2 + 3Y^2 + 267Z^2$	267	1068	$\{89\}$
91	$(7,13)$	$-7X^2 - 13Y^2 + 91Z^2$	-91	364	$\{7,13\}$
93	$(93,-1)$	$-93X^2 + Y^2 - 93Z^2$	-93	372	$\{3,31\}$
94	$(47,-1)$	$-47X^2 + Y^2 - 47Z^2$	-47	188	$\{2,47\}$
95	$(95,-7)$	$-95X^2 + 7Y^2 - 665Z^2$	-665	2660	$\{5,19\}$
97	$(-97,-7)$	$97X^2 + 7Y^2 + 679Z^2$	679	2716	$\{97\}$