Capítol II

Corbes el·líptiques amb multiplicació complexa i teoria de cossos de classes

A. Travesa

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

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

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

Comencem l'exposició amb l'estudi dels conceptes que apareixen a l'enunciat. A la secció primera, recordem les propietats principals dels ordres dels cossos quadràtics, dels seus ideals, dels grups de classes, i la relació d'aquests conceptes amb les formes quadràtiques binàries enteres. A la secció segona, repassem la definició i les propietats de la funció j per a relacionar-la amb les corbes el·líptiques amb multiplicació complexa. A la secció tercera, introduïm els polinomis modulars, establim les congruències

Amb suport parcial de DGES, PB96-0166.

de Kronecker i relacionem els polinomis modulars amb les isogènies cícliques entre corbes el·líptiques. A la secció quarta, recordem algunes qüestions relatives a la teoria de cossos de classes; essencialment, el teorema de densitat de Txebotarev, la caracterització de les inclusions entre extensions de Galois de cossos de nombres en funció dels primers que hi descomponen completament, i la definició i les propietats bàsiques del cos de classes associat a un ordre d'un cos quadràtic.

La demostració del **teorema 0.1** ocupa tota la secció cinquena. A la secció sisena, enunciem algunes conseqüències del teorema i alguns altres resultats relacionats, especialment, amb la llei de reciprocitat. I, finalment, a la secció setena, estudiem l'equació de les classes i la factorització dels polinomis modulars; hi incloem la discussió d'una afirmació errònea de [**Cox 87**].

§1. Ordres i ideals dels cossos quadràtics imaginaris

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

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

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

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

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

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

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

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

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

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

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

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

Un ordre $\mathcal{O} \subseteq K$ no és, en general, un subanell íntegrament tancat de K; de fet, i per definició, només és íntegrament tancat l'ordre màxim. En particular, els ordres no són anells de Dedekind i no disposem, a priori, d'una

bona teoria multiplicativa d'ideals; per exemple, no podem suposar que disposem de factorització única dels ideals com a producte d'ideals primers. Però ens interessa parlar dels ordres dels cossos quadràtics i dels seus grups de classes d'ideals. A fi de posar en evidència algunes particularitats dels ordres i dels ideals, començarem amb un exemple.

1.4. Exemple. Considerem el cos quadràtic $K := \mathbb{Q}(\sqrt{-3})$; el seu ordre màxim és $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-3})/2]$, de discriminant -3. D'altra banda, l'anell $\mathcal{O} := \mathbb{Z}[\sqrt{-3}]$ és l'ordre de K de discriminant -12; el conductor de $\mathcal{O}_K$ en $\mathcal{O}$ és 2. Considerem el $\mathcal{O}$-ideal $\mathfrak{a} \subseteq \mathcal{O}$ generat per 2 i $1+\sqrt{-3}$. Les igualtats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A fi d'aplicar la teoria de cossos de classes, cal relacionar els $\mathcal{O}$-ideals fraccionaris propis de K amb els $\mathcal{O}_K$-ideals fraccionaris de K, on $\mathcal{O}_K$ és

l'ordre màxim d'un cos quadràtic imaginari K; per a això, i per a obtenir la finitud del grup de classes d'ideals, per exemple, és útil relacionar-los amb les formes quadràtiques binàries enteres.

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

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

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

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

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

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

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

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

més a més, si $m \in \mathbb{Z}$ és un nombre enter no nul i $\mathfrak{a} \subseteq \mathcal{O}_K$ és un $\mathcal{O}_K$-ideal enter no nul, es diu que $\mathfrak{a}$ és primer amb m si $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$.

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

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

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

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

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

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

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

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

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

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

La relació entre els $\mathcal{O}$-ideals enters primers amb el conductor de $\mathcal{O}$ i

els ideals de $\mathcal{O}_K$ és donada en la proposició següent.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§2. Corbes el·líptiques i multiplicacions complexes

Recordem que una $\mathbb{Z}$-xarxa de $\mathbb{C}$ és, per definició, un subgrup additiu $L \subseteq \mathbb{C}$ generat per una $\mathbb{R}$-base de $\mathbb{C}$. En altres paraules, una xarxa és un subgrup $L \subseteq \mathbb{C}$ de la forma $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, on $\omega_1, \omega_2 \in \mathbb{C}$ són $\mathbb{R}$-linealment independents. En particular, una xarxa és un grup abelià lliure de dimensió 2. Per exemple, tot ordre $\mathcal{O}$ d'un cos quadràtic imaginari K i tot $\mathcal{O}$-ideal fraccionari de K són xarxes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) *$\alpha L \subseteq L$.*

(c) *Existeix un ordre $\mathcal{O}$ en un cos quadràtic imaginari K tal que $\alpha \in \mathcal{O}$ i L és una xarxa homotètica a un $\mathcal{O}$-ideal fraccionari propi de K.*

A més a més, en aquest cas, la funció $\wp(\alpha z; L)$ es pot escriure en la forma

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

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

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

Aquest teorema ens diu que l'anell de multiplicadors d'una xarxa $L \subseteq \mathbb{C}$, $\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$, o equivalentment, l'anell d'endomorfismes

de la corba el·líptica $\mathbb{C}/L$, és, o bé $\mathbb{Z}$, o bé un ordre $\mathcal{O} \subseteq K$ d'un cert cos quadràtic imaginari K. A més a més, en aquest cas, existeix un nombre complex no nul $\lambda \in \mathbb{C}$ tal que $\lambda L \subseteq K$ i λL és un $\mathcal{O}$-ideal fraccionari propi de K.

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

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

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

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

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

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

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

2.18. Teorema.

(a) *La funció* $j : \mathbb{H} \longrightarrow \mathbb{C}$ *és una funció holomorfa.*

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

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

(d) *Per a* $\tau \in \mathbb{H}$, *és* $j'(\tau) \neq 0$, *excepte per als casos*

(d1) $\tau = \gamma i$, $\gamma \in \mathbf{SL}(2,\mathbb{Z})$, *en què* $j'(\tau) = 0$, *però* $j''(\tau) \neq 0$;

(d2) $\tau = \gamma\rho$, $\rho = \dfrac{-1+\sqrt{-3}}{2}$, *i* $\gamma \in \mathbf{SL}(2,\mathbb{Z})$, *en què és* $j'(\tau) = j''(\tau) = 0$, *però* $j'''(\tau) \neq 0$. □

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

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

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

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

Considerem les sèries de potències de q

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

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

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

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

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

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

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

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

Si ara tenim en compte els valors de la funció zeta

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

obtenim que

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

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

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

2.23. Proposició. *Siguin $f : \mathbb{H} \longrightarrow \mathbb{C}$ una funció modular holomorfa en $\mathbb{H}$ i $f(q) := \sum_{n\geq n_0} c_n q^n$, $n_0 \geq 0$, la seva q-expansió, i posem $C := \sum_{n\geq n_0} \mathbb{Z}c_n \subseteq \mathbb{C}$.*

Llavors, $f(q) \in C[j(q)]$; és a dir, $f(q)$ és un polinomi en $j(q)$ de coeficients en el grup abelià generat pels coeficients c_n. □

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

§3. Els polinomis modulars

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

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

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

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

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

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

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

Si transposem totes les matrius, obtenim el resultat següent.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ara, de la definició dels polinomis modulars, obtenim que

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.20. Corol·lari. *Siguin $\mathbb{C}/L$, $\mathbb{C}/L'$ corbes el·líptiques complexes. Existeix*

alguna isogènia $\mathbb{C}/L' \to \mathbb{C}/L$ *cíclica de grau* $n \geq 1$ *si, i només si,* $j(L')$ *és una arrel del polinomi* $\Phi_n(X, j(L)) \in \mathbb{C}[X]$. $\square$

§4. Teoria de cossos de classes

En aquesta secció, enunciarem alguns conceptes i alguns resultats de teoria de cossos de classes que utilitzarem a la prova del **teorema 0.1**. Començarem pel teorema de densitat de Txebotarev.

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

$$\delta(\mathcal{S}) := \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} \mathrm{N}(\mathfrak{p})^{-s}}{-\log(s-1)}.$$

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

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

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

(c) *Si* $\delta(\mathcal{S})$ *existeix, llavors* $0 \leq \delta(\mathcal{S}) \leq 1$.

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

(e) *Si* $\mathcal{S}$ *és finit, llavors* $\delta(\mathcal{S}) = 0$.

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

(g) *Sigui* $\mathcal{P}_{K,1}$ *el conjunt dels ideals primers* $\mathfrak{p} \subseteq \mathcal{O}_K$ *tals que* $\mathrm{N}(\mathfrak{p})$ *és primer. Llavors, si* $\delta(\mathcal{S})$ *existeix, també existeix* $\delta(\mathcal{S} \cap \mathcal{P}_{K,1})$ *i* $\delta(\mathcal{S}) = \delta(\mathcal{S} \cap \mathcal{P}_{K,1})$. $\square$

Sigui, ara, $L|K$ una extensió de Galois, no necessàriament abeliana, de cossos de nombres. Donat $\mathfrak{p} \in \mathcal{P}_K$ tal que $\mathfrak{p}$ és no ramificat en l'extensió

$L|K$, els símbols d'Artin $\left(\frac{L|K}{\mathfrak{P}}\right)$, associats a tots els ideals primers $\mathfrak{P}$ de L que divideixen $\mathfrak{p}$, formen una classe de conjugació en $\mathrm{Gal}(L|K)$. Per tant, podem definir el símbol d'Artin $\left(\frac{L|K}{\mathfrak{p}}\right)$ com aquesta classe de conjugació.

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

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

té densitat de Dirichlet

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

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

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

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

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

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

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

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

(b) *$L = M$ si, i només si, existeixen conjunts finits $\mathcal{T}_1, \mathcal{T}_2 \subseteq \mathcal{P}_K$ tals que $\mathcal{S}_{M|K} \cup \mathcal{T}_1 = \mathcal{S}_{L|K} \cup \mathcal{T}_2$.*

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

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

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

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

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

Notem que si $M|K$ és de Galois, llavors $\tilde{\mathcal{S}}_{M|K} := \mathcal{S}_{M|K}$; així, qualsevol de les dues afirmacions d'aquesta proposició implica el teorema anterior.

Per a acabar aquesta secció, introduirem el concepte i les propietats més generals dels cossos de classes dels ordres dels cossos quadràtics imaginaris. Siguin, doncs, K, un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ l'ordre de conductor f de K.

En el **teorema 1.24**, hem establert que el grup de classes d'ideals de l'ordre $\mathcal{O}$ es pot escriure en la forma

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

on $\mathbf{P}_{K,\mathbb{Z}}(f)$ és el subgrup de $\mathbf{I}_K(f)$ generat pels $\mathcal{O}_K$-ideals enters principals de la forma $\alpha\mathcal{O}_K$, on $\alpha \in \mathcal{O}_K$ és tal que $\alpha \equiv a \pmod f$, per a algun nombre enter $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a, f) = 1$.

Si denotem per $\mathbf{P}_{K,1}(f)$ el subgrup principal de congruència per al mòdul f; és a dir, el subgrup de $\mathbf{I}_K(f)$ generat pels $\mathcal{O}_K$-ideals enters principals de la forma $\alpha\mathcal{O}_K$, on $\alpha \in \mathcal{O}_K$ és tal que $\alpha \equiv 1 \pmod f$, és immediat

que $\mathbf{P}_{K,1}(f) \subseteq \mathbf{P}_{K,\mathbb{Z}}(f) \subseteq \mathbf{I}_K(f)$, de manera que hi ha exactament un cos de classes per al subgrup $\mathbf{P}_{K,\mathbb{Z}}(f)$; aquest cos s'anomena el cos de classes de l'ordre $\mathcal{O}$. Si denotem per L aquest cos de classes, se satisfà que l'extensió $L|K$ és abeliana i que $\mathrm{Gal}(L|K) \simeq \mathbf{Cl}(\mathcal{O})$, l'isomorfisme donat pel símbol d'Artin.

Notem que, en particular, d'aquesta manera també obtenim la finitud del grup de classes $\mathbf{Cl}(\mathcal{O})$, ja que el grup quocient $\dfrac{\mathbf{I}_K(f)}{\mathbf{P}_{K,1}(f)}$ és finit. De fet, se satisfà el resultat següent.

4.8. Proposició. *Sigui L el cos de classes d'un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K. Llavors, l'extensió $L|\mathbb{Q}$ és de Galois, i el grup de Galois $\mathrm{Gal}(L|\mathbb{Q})$ és el producte semidirecte de $\mathrm{Gal}(L|K) \simeq \mathbf{Cl}(\mathcal{O})$ per un grup cíclic d'ordre 2, on l'element no trivial de C_2 actua en $\mathrm{Gal}(L|K)$ en la forma $\sigma \mapsto \sigma^{-1}$.* □

Recordem que un grup s'anomena diedral generalitzat si és extensió d'un grup cíclic d'ordre 2 per un grup abelià, no necessàriament cíclic. Com a conseqüència, disposem de la noció d'extensió diedral generalitzada.

4.9. Teorema. *Sigui K un cos quadràtic imaginari. Una extensió abeliana $L|K$ és diedral generalitzada sobre $\mathbb{Q}$ si, i només si, L és subcòs del cos de classes d'algun ordre de K.* □

4.10. Observació. Donat un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K, el cos de classes de l'ordre $\mathcal{O}$ duu associat un conductor en el sentit de la teoria de cossos de classes; aquest conductor, $\mathfrak{f}(L|K)$ coincideix, gairebé sempre, amb el conductor f de l'ordre $\mathcal{O}$; però hi ha alguns casos en què això no és així. Més concretament:

$$\mathfrak{f}(L|K) = \begin{cases} \mathcal{O}_K, & \text{si } f = 2,3, \text{ i } K = \mathbb{Q}(\sqrt{-3}); \\ \mathcal{O}_K, & \text{si } f = 2, \text{ i } K = \mathbb{Q}(\sqrt{-1}); \\ \dfrac{f}{2}\mathcal{O}_K, & \text{si } f = 2f',\ f' \text{ senar,} \\ & \text{i 2 descompon completament en } \mathcal{O}_K; \\ f\mathcal{O}_K, & \text{altrament.} \end{cases}$$

§5. Demostració del teorema

Recordem l'enunciat del teorema que volem provar.

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

Demostració. Començarem per veure que $j(\mathfrak{a})$ és un enter algebraic.

• Afirmem que existeix un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, primitiu de $\mathcal{O}$ i tal que $m := \mathrm{N}(\alpha)$ no és un quadrat (cf. la **definició 1.27**).

En efecte; siguin $\mathcal{O}_K$ l'anell dels enters de K, D el seu discriminant, $\omega_D := \dfrac{D+\sqrt{D}}{2}$, i f el conductor de l'ordre $\mathcal{O}$. Llavors, $\mathcal{O} = \mathbb{Z}\oplus\mathbb{Z}f\omega_D$ (cf. la **proposició 1.2**, (b)); a més a més, $\alpha := f\omega_D \in \mathcal{O}$ és un element primitiu de $\mathcal{O}$, perquè forma part d'una $\mathbb{Z}$-base de $\mathcal{O}$. Finalment, $m := \mathrm{N}(\alpha) = \mathrm{N}(f\omega_D)$ no és un quadrat, ja que, si designem per $x \mapsto x'$ l'automorfisme no trivial de K, el càlcul de la norma de $f\omega_D$ ens proporciona la igualtat

$$\mathrm{N}(f\omega_D) = f^2\omega_D\omega_D' = f^2\frac{D^2-D}{4} = f^2\frac{D(D-1)}{4};$$

i, com que $\mathrm{mcd}(D, D-1) = 1$ i D no és un quadrat, el producte $D(D-1)$ no pot ser un quadrat. •

Sigui, doncs, $\alpha \in \mathcal{O}$, $\alpha \neq 0$, un element primitiu de $\mathcal{O}$ tal que $m := \mathrm{N}(\alpha)$ no és un quadrat.

D'una banda, i com que m no és un quadrat, el polinomi $\Phi_m(X, X) \in \mathbb{Z}[X]$ és de grau > 1 i el seu coeficient dominant és ± 1 (cf. la **proposició 3.13**). D'altra banda, com que $\mathfrak{a}$ és un $\mathcal{O}$-ideal fraccionari propi de K i $\alpha \in \mathcal{O}$ és un element primitiu de $\mathcal{O}$, el grup abelià quocient $\dfrac{\mathfrak{a}}{\alpha\mathfrak{a}}$ és cíclic d'ordre $\mathrm{N}(\alpha) = m$ (cf. el **corol·lari 1.29**). Com que $\mathfrak{a}$ i $\alpha\mathfrak{a}$ són xarxes de $\mathbb{C}$, la **proposició 3.18** ens ensenya que $\Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0$. A més a més, com que $\mathfrak{a}$ i $\alpha\mathfrak{a}$ són dues xarxes homotètiques, el **teorema 2.13** ens diu que és $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$, de manera que $\Phi_m(j(\mathfrak{a}), j(\mathfrak{a})) = 0$ i $j(\mathfrak{a})$ és un enter algebraic.

A continuació, i si L designa el cos de classes de l'ordre $\mathcal{O}$, i $M := K(j(\mathfrak{a}))$, cal veure que $L = M$.

Sigui $\mathcal{S}_{L|\mathbb{Q}}$ el conjunt dels primers de $\mathbb{Z}$ que descomponen completament en L (cf. la **definició 4.5**).

Una de les propietats principals dels cossos de classes dels ordres és que els primers de $\mathbb{Q}$ que hi descomponen completament són, llevat possiblement d'un conjunt finit d'excepcions, els primers representats per la forma nòrmica de l'ordre $\mathcal{O}$; és a dir, llevat d'un conjunt finit (en cada costat), el conjunt $\mathcal{S}_{L|\mathbb{Q}}$ coincideix amb el conjunt

$$\{p \text{ primer de } \mathbb{Z} : \ p = \mathrm{N}(\alpha), \text{ per a algun } \alpha \in \mathcal{O}\}. \tag{1}$$

Com que l'extensió $L|\mathbb{Q}$ és de Galois, i si tenim en compte la **proposició 4.7**, (a), per a demostrar que $M \subseteq L$ és suficient provar que tot element de $\mathcal{S}_{L|\mathbb{Q}}$, llevat potser d'un conjunt finit, pertany a $\mathcal{S}_{M|\mathbb{Q}}$; vegem, doncs, això.

Sigui $p \in \mathcal{S}_{L|\mathbb{Q}}$ qualsevol primer i suposem que p és no ramificat en $M|\mathbb{Q}$; com que la quantitat de primers que ramifiquen en qualsevol extensió és finita, això exclou, com a màxim, una quantitat finita d'elements de $\mathcal{S}_{L|\mathbb{Q}}$.

En virtut de (1), i llevat d'un conjunt finit de primers $p \in \mathcal{S}_{L|\mathbb{Q}}$, existeix $\alpha \in \mathcal{O}$, $\alpha \neq 0$, tal que $p = \mathrm{N}(\alpha)$. Llavors, el grup abelià quocient $\dfrac{\mathfrak{a}}{\alpha\mathfrak{a}}$ és finit d'ordre $p = \mathrm{N}(\alpha)$ i, en conseqüència, és cíclic. Per tant, tenim la igualtat

$$\Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0.$$

Ara, fem servir les congruències de Kronecker (cf. el **teorema 3.16**); existeix $\beta \in \mathcal{O}_M$ tal que

$$(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 = p\beta.$$

Si $\mathfrak{P} \subseteq \mathcal{O}_M$ és un primer de $\mathcal{O}_M$ que divideix p, obtenim que

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}.$$

• Afirmem que:

(i) $\mathcal{O}_K[j(\mathfrak{a})] \subseteq \mathcal{O}_M$ i és un subgrup d'índex finit.

(ii) Si p no divideix l'índex $[\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, la congruència $j(\mathfrak{a})^p \equiv j(\mathfrak{a})$ (mod $\mathfrak{P}$) implica que $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, per a tot element $\alpha \in \mathcal{O}_M$.

En efecte; com que $M = K(j(\mathfrak{a}))$ i $j(\mathfrak{a}) \in \mathcal{O}_M$, és clar que $\mathcal{O}_K[j(\mathfrak{a})] \subseteq \mathcal{O}_M$; i, a més a més, el grup abelià quocient és finit, perquè tots dos són grups abelians lliures de la mateixa dimensió $[M : \mathbb{Q}]$. Això demostra (i).

D'altra banda, com que p descompon completament en L, també descompon completament en K; si $\mathfrak{p} := \mathfrak{P} \cap K$, tenim que $\mathfrak{p}$ és un ideal de $\mathcal{O}_K$ de norma p, de manera que per a tot $\alpha \in \mathcal{O}_K$ és $\alpha^p \equiv \alpha \pmod{\mathfrak{p}}$. I, com que $\mathfrak{P}$ divideix $\mathfrak{p}$, és $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, per a tot $\alpha \in \mathcal{O}_K$. Com que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$, tenim que per a tot element $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$ és $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$.

L'extensió d'aquesta propietat a tot $\mathcal{O}_M$ és immediata a partir del fet que p no divideix $n := [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$. Com que $n\mathcal{O}_M \subseteq \mathcal{O}_K[j(\mathfrak{a})]$, tenim que per a tot $\alpha \in \mathcal{O}_M$ és $n\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$, de manera que $n^p\alpha^p \equiv n\alpha \pmod{\mathfrak{P}}$; i, com que $\mathfrak{P}$ divideix p i p no divideix n, és $n^p \equiv n \pmod{\mathfrak{P}}$; això fa que sigui $n\alpha^p \equiv n\alpha \pmod{\mathfrak{P}}$ i, com que n és invertible mòdul $\mathfrak{P}$, que sigui $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, per a tot $\alpha \in \mathcal{O}_M$, com volíem veure. •

Ara, de (ii) se segueix que, per a tot primer $\mathfrak{P} \subseteq \mathcal{O}_M$ que divideix p, i si $f(\mathfrak{P}|p)$ designa el grau residual, sigui $f(\mathfrak{P}|p) = 1$; i, com que p no ramifica en M, p descompon completament en $\mathcal{O}_M$. Així, obtenim que, llevat d'un conjunt finit, tots els primers de $\mathcal{S}_{L|\mathbb{Q}}$ pertanyen a $\mathcal{S}_{M|\mathbb{Q}}$ i, en conseqüència, és $M \subseteq L$.

Conèixer aquesta inclusió és important per a la resta de la prova. Efectivament, la inclusió $M = K(j(\mathfrak{a})) \subseteq L$ ens ensenya que el cos de classes L conté l'invariant $j(\mathfrak{a})$; i, com que $\mathfrak{a}$ és qualsevol $\mathcal{O}$-ideal fraccionari propi de K, L conté l'invariant $j(\mathfrak{b})$, per a tots els $\mathcal{O}$-ideals fraccionaris propis $\mathfrak{b}$ de K. Sigui $h := h(\mathcal{O})$ el nombre de classes de l'ordre $\mathcal{O}$, i siguin $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ representants de les classes de $\mathbf{Cl}(\mathcal{O})$. Llavors, $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ són diferents i, per a tot $\mathcal{O}$-ideal fraccionari propi $\mathfrak{b}$ de K, $j(\mathfrak{b})$ és un dels nombres $j(\mathfrak{a}_i)$ (cf. el **teorema 2.13** i el **corol·lari 2.16**). Com a conseqüència,

$$\Delta := \prod_{1 \le i < j \le h} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$$

és un element no nul de $\mathcal{O}_L$.

Ara, per a provar la inclusió contrària, $L \subseteq M$, usarem el criteri que, llevat d'un conjunt finit, $\tilde{\mathcal{S}}_{M|\mathbb{Q}} \subseteq \mathcal{S}_{L|\mathbb{Q}}$, on $\tilde{\mathcal{S}}_{M|\mathbb{Q}}$ és el conjunt dels primers

p de $\mathbb{Q}$ no ramificats en $\mathcal{O}_M$ i que són divisibles per algun primer $\mathfrak{P}$ de M de grau residual 1 (cf. la **proposició 4.7**, (b)).

Sigui, doncs, $p \in \tilde{\mathcal{S}}_{M|\mathbb{Q}}$; és a dir, p és no ramificat en M i existeix algun primer $\mathfrak{P}$ de $\mathcal{O}_M$ que divideix p i tal que $f(\mathfrak{P}|p) = 1$. En particular, com que $K|\mathbb{Q}$ és de Galois, p descompon completament en K i, en conseqüència, $p = \mathrm{N}(\mathfrak{p})$ per a algun ideal primer $\mathfrak{p} \subseteq \mathcal{O}_K$ que divideix p (podem prendre $\mathfrak{p} := \mathfrak{P} \cap K$). Si ens limitem a considerar els ideals p primers amb el conductor $f := [\mathcal{O}_K : \mathcal{O}]$, fet que exclou, com a màxim, una quantitat finita d'ideals primers de $\mathbb{Z}$ i, en conseqüència, un conjunt finit de primers de L, que podríem afegir a $\mathcal{S}_{L|\mathbb{Q}}$, obtenim que $\mathfrak{p} \cap \mathcal{O} \subseteq \mathcal{O}$ és un ideal primer de $\mathcal{O}$ primer amb f i que $\mathrm{N}(\mathfrak{p} \cap \mathcal{O}) = p$.

Ara, si podem demostrar que $\mathfrak{p} \cap \mathcal{O}$ és un ideal principal $\alpha\mathcal{O}$, llavors, $p = \mathrm{N}(\alpha)$ implica que $p \in \mathcal{S}_{L|\mathbb{Q}}$, en virtut del criteri (1) de més amunt, i haurem acabat.

Notem que, de nou, podem excloure de consideració una quantitat finita de primers; en particular, podem suposar que p és coprimer amb Δ. Posem $\mathfrak{a}' := (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. Com que $\mathrm{N}(\mathfrak{p} \cap \mathcal{O}) = p$, el grup abelià quocient $\frac{\mathfrak{a}}{\mathfrak{a}'}$ és cíclic d'ordre p. Per tant, tenim que $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$ (cf. la **proposició 3.18**). De nou, en virtut de la congruència de Kronecker, existeix un polinomi $Q(X, Y) \in \mathbb{Z}[X, Y]$ tal que

$$(j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a})) = 0.$$

Sigui $\tilde{\mathfrak{P}}$ un primer de L que divideix $\mathfrak{P}$. Com que $j(\mathfrak{a}')$ i $j(\mathfrak{a})$ pertanyen a $\mathcal{O}_L$, tenim que $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \tilde{\mathfrak{P}}$; en conseqüència, se satisfà almenys una de les congruències

$$(2) \qquad j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}, \qquad j(\mathfrak{a}') \equiv j(\mathfrak{a})^p \pmod{\tilde{\mathfrak{P}}}.$$

D'altra banda, com que $f(\mathfrak{P}|p) = 1$, tenim que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$; i, com que $\tilde{\mathfrak{P}}$ divideix $\mathfrak{P}$, obtenim que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}$. Ara, com que $\tilde{\mathfrak{P}}$ és de característica residual p, aquesta condició, juntament amb (2), ens ensenyen que $j(\mathfrak{a}') \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{P}}}$.

Si $\mathfrak{a}$ i $\mathfrak{a}'$ definissin classes diferents de $\mathbf{Cl}(\mathcal{O})$, llavors $j(\mathfrak{a}) - j(\mathfrak{a}')$ seria un dels factors de la definició de Δ i p no seria primer amb Δ, com hem suposat; per tant, $\mathfrak{a}$ i $\mathfrak{a}'$ pertanyen a la mateixa classe en $\mathbf{Cl}(\mathcal{O})$; és

a dir, i com que $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$, l'ideal $\mathfrak{p} \cap \mathcal{O}$ és principal. Això acaba la demostració. □

§6. Complements

En aquesta secció, enunciarem dos tipus de resultats que complementen el **teorema 0.1**. D'una banda, proporcionarem la llei de reciprocitat associada al cos de classes d'un ordre d'un cos quadràtic imaginari. D'altra banda, ens ocuparem dels cossos de classes radials de conductors enters dels cossos quadràtics imaginaris.

De manera semblant a com el teorema de Kronecker-Weber ens proporciona generadors de les extensions abelianes maximals de $\mathbb{Q}$ de conductors donats, el **teorema 0.1** ens proporciona un generador del cos de classes d'un ordre $\mathcal{O}$ d'un cos quadràtic imaginari. En el cas particular de l'ordre màxim, aquest cos és el cos de classes de Hilbert; doncs, obtenim el resultat següent.

6.1. Corol·lari. *Siguin K un cos quadràtic imaginari i $\mathcal{O}_K \subseteq K$ l'anell dels enters de K. El cos de classes de Hilbert de K és el cos $K(j(\mathcal{O}_K))$.* □

A més a més, com a conseqüència del **teorema 0.1** i del **teorema 4.9**, obtenim el resultat següent.

6.2. Corol·lari. *Siguin K un cos quadràtic imaginari i $L|K$ una extensió finita. Llavors, $L|K$ és una extensió abeliana i $L|\mathbb{Q}$ és diedral generalitzada si, i només si, existeix un ordre $\mathcal{O} \subseteq K$ tal que $L \subseteq K(j(\mathcal{O}))$.* □

Així com el teorema de Kronecker-Weber ens proporciona la llei de reciprocitat per a les extensions ciclotòmiques de $\mathbb{Q}$, és a dir, l'acció dels Frobenius sobre les arrels de la unitat, també es pot donar l'acció del grup de Galois del cos de classes de l'ordre $\mathcal{O}$ sobre el generador $j(\mathfrak{a})$ de l'extensió $L|K$; és donada per la llei de reciprocitat següent, sobre els generadors diferents $j(\mathfrak{a})$ del cos de classes.

6.3. Teorema. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i L el cos de classes de l'ordre $\mathcal{O}$. Si $\mathfrak{a} \subseteq K$ és un $\mathcal{O}$-ideal fraccionari propi i $\mathfrak{p} \subseteq \mathcal{O}_K$ és un $\mathcal{O}_K$-ideal enter primer, llavors*

$$\left(\frac{L|K}{\mathfrak{p}}\right)(j(\mathfrak{a})) = j((\overline{\mathfrak{p} \cap \mathcal{O}})\mathfrak{a}). \ \square$$

Aquest resultat es pot enunciar, en termes del grup de classes $\mathbf{Cl}(\mathcal{O})$, de la manera següent.

6.4. Corol·lari. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i L el cos de classes de l'ordre $\mathcal{O}$. Donats $\mathcal{O}$-ideals fraccionaris propis $\mathfrak{a}, \mathfrak{b} \subseteq K$, definim $\sigma_{\mathfrak{a}}(j(\mathfrak{b})) := j(\mathfrak{a}^{-1}\mathfrak{b})$. Llavors, $\sigma_{\mathfrak{a}}$ és un element de* $\mathrm{Gal}(L|K)$ *i l'assignació $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ indueix un isomorfisme $\mathbf{Cl}(\mathcal{O}) \xrightarrow{\simeq} \mathrm{Gal}(L|K)$.* $\square$

6.5. Funcions de Weber. Un cop donats els cossos de classes dels ordres dels cossos quadràtics imaginaris, ens podem preguntar pels cossos de classes radials de K de conductor enter.

Donada una xarxa $L \subseteq \mathbb{C}$, la funció de Weber $\tau(z; L)$, associada a la xarxa L, és definida per

$$\tau(z;L) := \begin{cases} \dfrac{g_2(L)^2}{\Delta(L)}\wp(z;L)^2, & \text{si } g_3(L) = 0; \\ \dfrac{g_3(L)}{\Delta(L)}\wp(z;L)^3, & \text{si } g_2(L) = 0; \\ \dfrac{g_2(L)g_3(L)}{\Delta(L)}\wp(z;L) & \text{altrament.} \end{cases}$$

La propietat més important i, d'altra banda, immediata, de les funcions $\tau(z; L)$ de Weber és el seu comportament en les classes d'homotècia de xarxes.

6.6. Lema. *Siguin $L \subseteq \mathbb{C}$ una xarxa i $\lambda \in \mathbb{C}$, $\lambda \neq 0$ un nombre complex no nul, qualssevol. Llavors, $\tau(\lambda z; \lambda L) = \tau(z; L)$, per a tot $z \in \mathbb{C}$.* $\square$

6.7. Teorema. *Siguin K un cos quadràtic imaginari, d_K el discriminant de K, i $N \in \mathbb{Z}$, $N > 0$, un nombre enter. Llavors:*

(a) *El cos* $K(j(\mathcal{O}_K), \tau(1/N; \mathcal{O}_K))$ *és el cos de classes radial per al mòdul* $N\mathcal{O}_K$.

(b) *Si* $\mathcal{O} \subseteq K$ *és l'ordre de* K *de conductor* N *i posem, com abans,* $\omega_K := \dfrac{d_K + \sqrt{d_K}}{2}$, *el cos de classes radial per al mòdul* $N\mathcal{O}_K$ *és el cos* $K(j(\mathcal{O}), \tau(\omega_K; \mathcal{O}_K))$. □

Així, el cos de classes radial de K per al mòdul $N > 0$ és generat, sobre el cos de classes de Hilbert de K, pel valor de la funció de Weber en un punt de N-divisió de la xarxa $\mathcal{O}_K$; o bé, sobre el cos de classes de l'ordre $\mathcal{O}$ de conductor N, pel valor de la funció de Weber en el generador ω_K de l'anell d'enters $\mathcal{O}_K$ de K.

Notem que, en qualsevol cas, obtenim el cos de classes radial de conductor N del cos quadràtic imaginari K en considerar la xarxa $\mathbb{Z} \oplus \mathbb{Z}\omega_K$ i afegir els valors de dues funcions en dos punts; la funció j en un generador de la xarxa i la funció de Weber en un punt de N-divisió (el punt $1/N$), en el primer cas; o bé a l'inrevés, el valor de la funció de Weber en un generador de la xarxa i el de la funció j en un punt de N-divisió de la xarxa $\mathcal{O}_K$ (notem que $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}N\omega_K$), en el segon.

§7. L'equació de les classes

El **teorema 0.1** ens diu que si $\mathcal{O}$ és un ordre d'un cos quadràtic imaginari, el cos de classes de l'ordre $\mathcal{O}$ és $K(j(\mathfrak{a}))$, on $\mathfrak{a}$ és qualsevol $\mathcal{O}$-ideal fraccionari propi de K; així, el teorema ens proporciona un generador del cos. Per exemple, podem prendre $\mathfrak{a} = \mathcal{O}$, de manera que el cos de classes de l'ordre $\mathcal{O}$ és el cos $K(j(\mathcal{O}))$. Es tracta d'estudiar una mica més els nombres algebraics $j(\mathfrak{a})$.

7.1. Lema. *Siguin* K *un cos quadràtic imaginari i* $\mathcal{O} \subseteq K$ *un ordre de* K. *Llavors,* $j(\mathcal{O})$ *és un nombre real.*

Demostració. Com que la conjugació complexa és un automorfisme de $\mathcal{O}$, tenim que $\mathcal{O} \subseteq \mathbb{C}$ és una xarxa invariant per a la conjugació complexa. Ara bé, de les definicions de les funcions $g_2(L)$ i $g_3(L)$ (cf. la **proposició 2.5**),

per a una xarxa arbitrària $L \subseteq \mathbb{C}$, tenim que, si L' denota la xarxa que s'obté de L en aplicar la conjugació complexa, $g_2(L')$ i $g_2(L)$ són nombres complexos conjugats i, anàlogament, $g_3(L')$ i $g_3(L)$ són nombres complexos conjugats; en conseqüència, $j(L')$ i $j(L)$ també són nombres complexos conjugats. Si apliquem això a la xarxa $L = \mathcal{O} = L'$, obtenim que $j(\mathcal{O})$ és invariant per a la conjugació complexa i, en conseqüència, $j(\mathcal{O}) \in \mathbb{R}$. □

A més a més, sabem que $j(\mathcal{O})$ és un nombre enter algebraic; per tant, el seu polinomi minimal sobre $\mathbb{Q}$ és de coeficients enters.

7.2. Definició. Siguin K un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ un ordre qualsevol de K. Sigui $H_{\mathcal{O}}(X) \in \mathbb{Z}[X]$ el polinomi mònic irreductible que té $j(\mathcal{O})$ com a arrel; és a dir, el polinomi minimal de $j(\mathcal{O})$ sobre $\mathbb{Q}$. El polinomi $H_{\mathcal{O}}(X)$, o l'equació $H_{\mathcal{O}}(X) = 0$, s'anomena l'equació de les classes de $\mathcal{O}$. Com que $\mathcal{O} = \mathcal{O}_D$, on D és el discriminant de $\mathcal{O}$, sovint s'escriu $H_D(X)$ en lloc de $H_{\mathcal{O}}(X)$.

7.3. Proposició. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K, $h := h(\mathcal{O}) := \#\mathbf{Cl}(\mathcal{O})$ el nombre de classes de $\mathcal{O}$, i $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ representants de les classes de $\mathbf{Cl}(\mathcal{O})$. Llavors,*

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)). \; \square$$

7.4. Corol·lari. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i $\mathfrak{a} \subseteq K$ un $\mathcal{O}$-ideal fraccionari propi de $\mathcal{O}$. Llavors, el polinomi minimal de $j(\mathfrak{a})$ sobre $\mathbb{Q}$ és $H_{\mathcal{O}}(X)$.* □

Les equacions de les classes ens permeten factoritzar els polinomis $\Phi_m(X, X)$. Per a això, tenim el resultat següent.

7.5. Lema. *Sigui $m \in \mathbb{Z}$, $m > 1$, i considerem el polinomi $\Phi_m(X, X)$.*

(a) *Si $q(X) \in \mathbb{Z}[X]$ és un polinomi mònic irreductible que divideix el polinomi $\Phi_m(X, X)$, existeixen un cos quadràtic imaginari K i un ordre $\mathcal{O} \subseteq K$ que conté un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, primitiu de norma $\mathrm{N}(\alpha) = m$, tals que $q(X) = H_{\mathcal{O}}(X)$.*

(b) *Recíprocament, si K és un cos quadràtic imaginari i $\mathcal{O} \subseteq K$ és un ordre per al qual existeix un element $\alpha \in \mathcal{O}$, $\alpha \neq 0$, primitiu de norma $\mathrm{N}(\alpha) = m$, llavors $H_{\mathcal{O}}(X)$ és un factor irreductible de $\Phi_m(X, X)$.*

Demostració. Sigui β una arrel de $q(X)$; llavors, és $\Phi_m(\beta, \beta) = 0$. La **proposició 3.18** ens diu que existeixen xarxes $L' \subseteq L \subseteq \mathbb{C}$ tals que $j(L') = j(L) = \beta$ i que el grup abelià quocient L/L' és cíclic d'ordre m; el **teorema 2.13** ens diu, ara, que existeix $\alpha \in \mathbb{C}$, $\alpha \neq 0$, tal que $L' = \alpha L$; en particular, α pertany a l'anell de multiplicadors de la xarxa L, i $\alpha \notin \mathbb{Z}$, perquè L/L' és cíclic. En virtut del **teorema 2.15**, existeix un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K tal que $\alpha \in \mathcal{O}$, i, a més a més, les xarxes $L' \subseteq L$ són homotètiques a $\mathcal{O}$-ideals fraccionaris propis $\mathfrak{a}' \subseteq \mathfrak{a}$ de K; el fet que sigui $j(\mathfrak{a}) = j(L) = \beta$ ens diu que $q(X)$ és el polinomi minimal de $j(\mathfrak{a})$; és a dir, $q(X) = H_{\mathcal{O}}(X)$; això demostra la primera afirmació.

Recíprocament, sigui $\alpha \in \mathcal{O}$, $\alpha \neq 0$, un element primitiu de norma $\mathrm{N}(\alpha) = m$; llavors, $\mathcal{O}/\alpha\mathcal{O}$ és cíclic d'ordre m (cf. el **corol·lari 1.29**) i, en conseqüència, $\Phi_m(j(\mathcal{O}), j(\mathcal{O})) = \Phi_m(j(\alpha\mathcal{O}), j(\mathcal{O})) = 0$ (cf. la **proposició 3.18**). Així, $j(\mathcal{O})$ és una arrel del polinomi $\Phi_m(X, X)$, de manera que $H_{\mathcal{O}}(X) = \mathrm{Irr}(j(\mathcal{O}), K)$ divideix $\Phi_m(X, X)$. □

A fi d'obtenir la factorització completa dels polinomis $\Phi_m(X, X)$, ens cal, encara, obtenir la multiplicitat de les equacions de les classes per a cada ordre $\mathcal{O}$ de cada cos quadràtic imaginari.

7.6. Definició. Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre i $m > 1$ un nombre enter. Escriurem

$$r(\mathcal{O}, m) := \#\frac{\{\alpha \in \mathcal{O} : \alpha \text{ és primitiu i } \mathrm{N}(\alpha) = m\}}{\mathcal{O}^*}.$$

Notem que el conjunt d'unitats de $\mathcal{O}$ és finit i que també ho és el conjunt d'elements de $\mathcal{O}$ de norma donada.

En efecte, les unitats són els elements de norma 1; i els elements de norma $m > 0$ són donats per les solucions (a, b) de l'equació diofantina

$$(a + bf\omega_K)(a + bf\omega'_K) = m,$$

on $x \mapsto x'$ indica la conjugació complexa o, equivalentment, l'automorfisme

no trivial de K. Aquesta equació es pot escriure en la forma

$$\begin{aligned} m &= (a + bf\omega_K)(a + bf\omega'_K) \\ &= a^2 + b^2f^2\omega_K\omega'_K + abf(\omega_K + \omega'_K) \\ &= a^2 + b^2f^2\frac{d_K(d_K-1)}{4} + abfd_K; \end{aligned}$$

és a dir, en la forma

$$4m = (2a + bfd_K)^2 - d_K(bf)^2.$$

Ara, només cal tenir en compte que el discriminant d_K de K és un nombre enter negatiu, de manera que $|b|$ és fitat i, en conseqüència, només pot prendre una quantitat finita de valors enters; i, per tant, a només pot prendre una quantitat finita de valors enters.

7.7. Observació. A més a més, si $r(\mathcal{O}, m) \neq 0$; és a dir, si tenim un element primitiu de norma $m > 1$, ha de ser $b \neq 0$, i la igualtat $4m = (2a + bfd_K)^2 - d_K(bf)^2$ ens diu que el valor del discriminant d_K és fitat. Per tant, obtenim el resultat següent.

7.8. Proposició. *Fixat un nombre $m > 1$, la quantitat d'ordres $\mathcal{O}$ de cossos quadràtics imaginaris tals que $r(\mathcal{O}, m) > 0$ és finita.* □

Finalment, podem enunciar el resultat que ens proporciona la factorització dels polinomis $\Phi_m(X, X)$.

7.9. Teorema. *Sigui $m \in \mathbb{Z}$, $m > 1$. Existeix un nombre complex $c_m \in \mathbb{C}$, $c_m \neq 0$, tal que*

$$\Phi_m(X, X) = c_m \prod_{\mathcal{O}} H_{\mathcal{O}}(X)^{r(\mathcal{O},m)},$$

on $\mathcal{O}$ recorre tots els ordres de tots els cossos quadràtics imaginaris. □

Això no és suficient, encara, per a obtenir l'equació de les classes per a un ordre donat. En efecte; donat l'ordre $\mathcal{O}$ o, equivalentment, el seu discriminant, un element primitiu qualsevol $\alpha \in \mathcal{O}$, $\alpha \neq 0$, ens proporciona un valor $m := \mathrm{N}(\alpha)$ per al qual el polinomi $H_{\mathcal{O}}(X)$ és un divisor irreductible

de $\Phi_m(X,X)$. Però, quin dels divisors irreductibles, si $\Phi_m(X,X)$ en té més d'un?

A fi de respondre aquesta darrera qüestió, s'introdueix el polinomi $\Phi_{m,1}(X,X)$ com el producte dels factors irreductibles de $\Phi_m(X,X)$ que són de multiplicitat 1; és a dir,

$$\Phi_{m,1}(X,X) := \prod_{r(D,m)=1} H_D(X).$$

Se satisfà la propietat següent.

7.10. Proposició. *Sigui $m > 1$ un nombre enter. Llavors,*

$$\Phi_{m,1}(X,X) = \begin{cases} H_{-4}(X)H_{-8}(X), & \textit{si } m = 2; \\ H_{-m}(X)H_{-4m}(X), & \textit{si } m \equiv 3 \pmod 4 \textit{ i } m \neq 3k^2, \\ & \textit{per a tot } k > 1; \\ H_{-4m}(X), & \textit{si } m > 2 \textit{ i } m \not\equiv 3 \pmod 4, \\ & \textit{o bé } m = 3k^2,\ k > 1. \square \end{cases}$$

El resultat anterior ens permet acabar el càlcul algorítmic de l'equació de les classes $H_D(X)$, per a gairebé tots els discriminants $D < 0$, però no per a tots (cf. [**Cox 89**p. 292–293]).

Comencem per observar que, si posem $f(X) := \Phi_m(X,X)$, llavors $g(X) := \dfrac{f(X)}{\operatorname{mcd}(f(X), f'(X))}$ és el producte de tots els factors irreductibles de $f(X)$, però tots apareixen, en $g(X)$, amb multiplicitat 1; llavors, tenim que $\Phi_{m,1}(X,X) = \dfrac{g(X)}{\operatorname{mcd}(g(X), f'(X))}$. Per tant, el càlcul de $\Phi_{m,1}(X,X)$ a partir del polinomi modular $\Phi_m(X,Y)$ no comporta cap problema.

Però, quin polinomi modular cal considerar? La proposició ens dóna una resposta parcial. Sigui $D < 0$ un discriminant negatiu qualsevol. Suposem, en primer lloc, que $D \equiv 0 \pmod 4$; això és, $D = -4m$, amb $m \geq 1$. Llavors,

$$H_D(X) = \begin{cases} H_{-4}(X) = X - 1728, & \text{si } m = 1, \\ H_{-8}(X) = X - 8000, & \text{si } m = 2, \\ H_{-12}(X) = X - 54000, & \text{si } m = 3, \\ H_{-4m}(X) = \Phi_{m,1}(X,X), & \text{si } m > 3 \text{ i } m \not\equiv 3 \pmod 4, \\ H_{-4m}(X) = \Phi_{m,1}(X,X), & \text{si } m > 3,\ m \equiv 3 \pmod 4 \\ & \text{i } m = 3k^2,\ k > 1. \end{cases}$$

Resten els casos en què és $m > 3$, $m \equiv 3 \pmod 4$, però $m \neq 3k^2$ per a tot nombre enter $k > 1$. En aquests casos, tenim que

$$\Phi_{m,1}(X, X) = H_{-m}(X)H_{-4m}(X) = H_{D/4}(X)H_D(X).$$

Per a distingir quin dels dos factors de $\Phi_{m,1}(X, X)$ és el factor que volem, observem que, si $m \equiv 3 \pmod 8$, la fórmula que relaciona els nombres de classes per a $D = -4m$ i $D = -m$ (cf. el **corol·lari 1.26**) ens diu que $h(-4m) = 3h(-m)$, de manera que els dos factors de $\Phi_{m,1}(X, X)$ són de graus diferents. Però si $m \equiv 7 \pmod 8$, els dos nombres de classes coincideixen, de manera que no podem distingir els factors pel seu grau. En aquest cas, però, se satisfà que

$$H_{-m}(X) = \mathrm{mcd}(\Phi_{m,1}(X, X), \Phi_{(m+1)/4}(X, X)),$$

i això permet acabar el càlcul de $H_D(X)$ en el cas $m > 3$.

Estudiem, ara, el cas en què $D \equiv 1 \pmod 4$; això és, $D = -m$, amb $m \geq 3$, $m \equiv 3 \pmod 4$. Si $m = 3$, tenim que $H_D(X) = H_{-3}(X) = X$; i si $m > 3$, però $m \neq 3k^2$ per a tot nombre enter $k > 1$, tenim que

$$\Phi_{m,1}(X, X) = H_{-m}(X)H_{-4m}(X) = H_D(X)H_{4D}(X),$$

i es distingeix com més amunt.

Però els casos $m = 3k^2$, amb $k > 1$, senar, no són coberts per cap dels casos anteriors.

En efecte; suposem que $D = -3k^2$, amb $k > 1$, senar. Sigui $\alpha \in \mathcal{O} := \mathcal{O}_D$ un element primitiu de norma $\mathrm{N}(\alpha) =: m > 1$, i posem $\alpha = a + b\dfrac{k + k\sqrt{-3}}{2}$. Llavors, tenim que $4\,\mathrm{N}(\alpha) = (2a + kb)^2 + 3k^2b^2$. Si b dóna lloc a una solució α tal que $\alpha \in \mathcal{O}$ és un element primitiu, ha de ser $b \neq 0$. Si, a més a més, suposem que és $2a + kb \neq 0$, i posem $x \in \mathbb{Z}$ tal que $x^2 = 4\,\mathrm{N}(\alpha) - 3k^2b^2 = (2a + kb)^2 \neq 0$, obtenim les quatre solucions

$$(a, b) \in \left\{ \left(\frac{x - kb}{2}, b \right), \left(\frac{-x - kb}{2}, b \right), \left(\frac{-x + kb}{2}, -b \right), \left(\frac{x + kb}{2}, -b \right) \right\},$$

i totes elles donen lloc a valors primitius de α, perquè k és senar. Com que $\#\mathcal{O}_D^* = 2$, perquè $k > 1$, això produeix que $r(\mathcal{O}, m) \geq 2$.

D'altra banda, si existeix algun element $\alpha \in \mathcal{O}$ primitiu de norma $\mathrm{N}(\alpha) = m$, i tal que $b \neq 0$, però $2a + kb = 0$, llavors ha de ser $b = \pm 2$, $a = \mp k$, i $m = 3k^2$. Ara bé, per a $m = 3k^2$, hi ha exactament sis elements primitius de $\mathcal{O}$ de norma m; són els elements

$$\alpha = \pm k\sqrt{-3}, \quad \pm k\frac{3+\sqrt{-3}}{2}, \quad \pm k\frac{-3+\sqrt{-3}}{2};$$

de manera que $r(\mathcal{O}, 3k^2) = 3$.

Com a conseqüència, no hi ha cap valor de m tal que $H_D(X)$ sigui un divisor del polinomi $\Phi_{m,1}(X, X)$.

7.11. Observació. Es pot provar de manera senzilla que, per a $D = -3k^2$, $k > 1$, senar, i $m = \dfrac{3k^2+1}{4}$, és $r(\mathcal{O}, m) = 2$. En efecte; els únics elements de $\mathcal{O}$ de norma $\dfrac{3k^2+1}{4}$ són els $\alpha = a + b\dfrac{k+\sqrt{-3k^2}}{2}$, amb

$$(a,b) \in \left\{ \left(\frac{1-k}{2}, 1\right), \left(\frac{-1-k}{2}, 1\right), \left(\frac{1+k}{2}, -1\right), \left(\frac{-1+k}{2}, -1\right) \right\},$$

i tots ells són primitius. En particular, per a $k > 1$, senar, el polinomi $H_{-3k^2}(X)$ és un factor irreductible de multiplicitat exactament 2 del polinomi $\Phi_{\frac{1+3k^2}{4}}(X, X)$.

Anàlogament, els únics elements primitius de $\mathcal{O}$ de norma k^2 són els elements

$$\pm k\frac{1+\sqrt{-3}}{2}, \qquad \pm k\frac{-1+\sqrt{-3}}{2},$$

de manera que $r(\mathcal{O}, k^2) = 2$ i el polinomi $H_{-3k^2}(X)$ és un factor de multiplicitat exactament 2 del polinomi $\Phi_{k^2}(X, X)$; així, $H_{-3k^2}(X)$ és un factor de multiplicitat exactament 2 del polinomi $\mathrm{mcd}(\Phi_{\frac{1+3k^2}{4}}(X, X), \Phi_{k^2}(X, X))$.

En qualsevol cas, el resultat següent ens permet acabar de dissenyar un algoritme per al càlcul de totes les equacions de les classes.

7.12. Proposició. *Siguin $k > 1$ un nombre enter senar, $D := -3k^2$, $d < 0$ un discriminant negatiu qualsevol, i $\mathcal{O} := \mathcal{O}_d$ l'ordre quadràtic de discriminant d. Llavors:*

(a) $r(\mathcal{O}_{-3k^2}, 3k^2) = 3$.

(b) $r(\mathcal{O}_{-12k^2}, 3k^2) = 1$.

(c) *Per a* $d \neq -3, -3k^2, -12k^2$, $r(\mathcal{O}_d, 3k^2)$ *és parell.*

DEMOSTRACIÓ. Considerem l'ordre $\mathcal{O} := \mathcal{O}_d$ de discriminant d, i suposem que $\alpha := a+b\dfrac{d+\sqrt{d}}{2} \in \mathcal{O}$, $a, b \in \mathbb{Z}$, és un element primitiu de norma $\mathrm{N}(\alpha) = 3k^2$. Observem que dir que α és primitiu equival a dir que $\mathrm{mcd}(a, b) = 1$; d'altra banda, si α és primitiu, i com que $3k^2 > 1$, ha de ser $b \neq 0$. L'equació que cal considerar és

$$12k^2 = 4\,\mathrm{N}(\alpha) = (2a + bd)^2 - b^2 d. \tag{1}$$

Suposem, en primer lloc, que l'equació (1) admet alguna solució (primitiva) amb $2a+bd = 0$. Llavors, b divideix $2a$ i, com que $\mathrm{mcd}(a, b) = 1$, és $b = \pm 1, \pm 2$. En el cas $b = \pm 2$, obtenim que $d = -3k^2$; i ja hem vist més amunt que $r(\mathcal{O}_{-3k^2}, 3k^2) = 3$. En el cas $b = \pm 1$, obtenim que $d = -12k^2$; i com que els únics elements primitius de $\mathcal{O}_d$ de norma $-3k^2$ són els elements $\pm k\sqrt{-3}$, resulta que $r(\mathcal{O}_{-12k^2}, 3k^2) = 1$; això demostra (b).

Com a conseqüència, si $d \neq -3k^2, -12k^2$, per a totes les solucions primitives de (1) se satisfà que $2a + bd \neq 0$; posem $x := 2a + bd$. Podem escriure aquella equació en la forma equivalent

$$12k^2 + b^2 d = x^2, \tag{2}$$

on $x = 2a + bd \neq 0$, de manera que $12k^2 + b^2 d$ és un enter quadrat no nul. Observem que, per a $-b$, en lloc de b, els dos valors $\pm x$ no canvien, i podem calcular els corresponents valors de a; obtenim les solucions

$$(a, b) \in \left\{ \left(\frac{x - bd}{2}, b \right) \left(\frac{-x - bd}{2}, b \right) \left(\frac{x + bd}{2}, -b \right) \left(\frac{-x + bd}{2}, -b \right) \right\};$$

de manera equivalent, obtenim que els quatre elements

$$\alpha = \frac{\pm x \pm b\sqrt{d}}{2},$$

son primitius de norma $3k^2$; i tots quatre són diferents.

Ara, raonem de la manera següent: si $d \neq -3k^2, -12k^2$, podem agrupar els elements primitius de norma $-3k^2$ de quatre en quatre; com a conseqüència, si $\#\mathcal{O}_d^* = 2$, obtenim que $r(\mathcal{O}_d, 3k^2)$ és parell. Això només deixa

fora de la discussió els casos dels discriminants $d = -3$ i $d = -4$, a part, és clar, dels casos $d = -3k^2, -12k^2$, exclosos des del començament.

Ara bé, si $d = -4$, l'equació (1) és $12k^2 = (2a - 4b)^2 + 4b^2$ que, en dividir per 4, és equivalent a $3k^2 = (a - 2b)^2 + b^2$; però aquesta equació no té solució, ja que k és senar i, per tant, $3k^2 \equiv 3 \pmod 4$, de manera que $3k^2$ no pot ser la suma de dos quadrats. Així, $r(\mathcal{O}_{-4}, 3k^2) = 0$ que, en particular, és parell. Això acaba la demostració. □

7.13. Observació. Notem que la proposició no diu res del discriminant $d = -3$. En aquest cas, es pot provar que, si $k > 1$ és senar, i divisible per 3 o bé per algun nombre primer $p \equiv -1 \pmod 3$, llavors és $r(\mathcal{O}_{-3}, 3k^2) = 0$. Però si tots els primers p que divideixen k són tals que $p \equiv 1 \pmod 3$, pot ser $r(\mathcal{O}_{-3}, 3k^2) \neq 0$. En qualsevol cas, però, això no priva d'obtenir l'algoritme que se cerca, ja que el factor $H_{-3}(X) = X$ és molt senzill de detectar en $\Phi_{3k^2}(X, X)$.

7.14. Corol·lari. *Siguin $k > 1$ un nombre enter senar i $g_k(X)$ el quocient del polinomi $\Phi_{3k^2}(X, X)$ per la potència de X que el divideix. Llavors, $H_{-3k^2}(X)$ és l'únic factor irreductible de multiplicitat exactament* 3 *del polinomi $g_k(X)$.* □

7.15. Observació. Podem descriure un altre algoritme per al càlcul dels polinomis de les classes, basat en la pròpia definició. De fet, el càlcul dels valors de la funció j és possible a partir, per exemple, del desenvolupament en sèrie (cf. la secció segona). D'altra banda, es pot calcular, via la teoria de la reducció de les formes quadràtiques binàries, representants de les formes primitives de discriminant donat D; això equival a calcular un sistema de representants de les classes dels $\mathcal{O}_D$-ideals fraccionaris propis $\mathfrak{a}$ de K; i els valors de la funció j en els zeros de les formes quadràtiques són les arrels del polinomi de les classes.

Bibliografia

[**Cox 89**] Cox, D. A.: *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989. ISBN: 0-471-50654-0.

[**Ja 73**] Janusz, G. J.: *Algebraic Number Fields*, Academic Press, New York, 1973. ISBN: 0-12-380250-4.

[**La 73**] Lang, S.: *Elliptic Functions*, Addison-Wesley, Reading, MA, 1973. ISBN: 0-201-04162-6.

[**Ne 99**] Neukirch, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999. ISBN: 3-540-65399-6. Traducció de N. Schappacher. Edició original: Algebraische Zahlentheorie, 1992.

[**Se 71**] Serre, J-P.: *Cours d'Arithmètique*, Presses Universitaires de France, Paris, 1977; primera edició, 1970.