Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Enters algebraics i treballs de Kummer sobre l'Últim Teorema de Fermat

Autor: Cèlia Cortés Roca

Director: Dr. Luís Dieulefait
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 27 de juny de 2018

Abstract

Fermat's Last Theorem asserts that the equation $x^n + y^n = x^n$ has not non-zero integral solutions x, y, z for $n \geq 3$. In this project we study the Kummer's proof of the first case of the Theorem along with developing the basic tools of the algebraic number theory. This first case is that the exponent n in the equation is a so-called regular prime and n does not divide any of x, y, z.

Resum

L'últim teorema de Fermat afirma que l'equació $x^n + y^n = x^n$ no té cap solució entera per $n \geq 3$ amb x, y, z diferents de zero. En aquest treball estudiem la demostració del primer cas del Teorema feta per Ernst Kummer juntament amb el desenvolupament de les eines bàsiques de la teoria algebraica de nombres. Aquest primer cas consisteix en que l'exponent de l'equació és un nombre p primer regular i p no divideix cap x, y, z.

2010 Mathematics Subject Classification. 11R04, 11R18, 11R27, 11R29

Agraïments

Principalment voldria agrair al meu tutor, Dr. Luís Dieulefait, pels seus consells, ajuda i sobretot motivació a l'hora de realitzar aquest treball. M'agradaria estendre aquest agraïment a tot el professorat que m'ha acompanyat durant aquests anys de formació i aprenentatge. No m'agradaria deixar-me l'Eduard Soto, que tot i que l'he conegut tard, m'ha ajudat i m'ha donat suport de cara a la finalització d'aquest treball.

D'altra banda també m'agradaria donar les gràcies a la meva família i amics per la paciència, recolzament i suport durant aquests mesos.

Índex

1 Introducció

Context històric

Els orígens de l'Últim Teorema de Fermat provenen dels pitagòrics, ja que aquests van demostrar que l'equació $x^2 + y^2 = z^2$ té infinites solucions enteres. Cap a l'any 1637, Pierre de Fermat va escriure al marge d'un llibre, del qual copiava l'Aritmètica de Diofant, el següent enunciat:

És impossible que un cub sigui la suma de dos cubs, que una potència quarta sigui la suma de dues potències quartes, i en general, que qualsevol nombre que sigui una potència superior a dos, sigui la suma de dues potències del mateix valor. He descobert una demostració veritablement meravellosa d'aquesta proposició, però aquest marge és massa estret perquè hi càpiga.

Més concretament va afirmar que l'equació

$$x^n + y^n = z^n \tag{1.1}$$

no té solucions enteres diferents de zero per $n \geq 3$. Tot i dir que tenia la demostració completa, Fermat només deixà constància de la demostració per n=4.

L'afirmació de Fermat va esdevenir un repte des del moment en el que es va plantejar. Durant els segles XVIII, XIX i XX molts matemàtics van enfrontar-se amb aquest problema, demostrant tant per un cert exponent, com casos més generals. Finalment, l'any 1995 Andrew Wiles va publicar un article de 96 pàgines demostrant el Teorema de Taniyama-Shimura que enllaça formes modulars i corbes el·líptiques. Combinant aquest Teorema amb representacions de Galois s'obté la demostració de l'Últim Teorema de Fermat i, finalment un dels problemes més famosos de la història de les matemàtiques queda tancat.

El primer resultat important va ser quan Leonard Euler va demostrar el cas $n = 3$ cap a l'any 1735. El segon gran pas el va fer Sophie Germain (1776-1831), una de les úniques dones que feien recerca matemàtica en aquell temps. Dins de la seva obra, va trobar convenient dividir el problema en dos casos:

1. Cap de les x, y, z és divisible per n.
2. Només un x, y, z és divisible per n.

Sophie Germain va demostrar el primer cas per tot $p < 100$. El dia 1 de març del 1847 Gabriel Lamé (1796-1870), es va adreçar a l'Acadèmia de Ciències de Paris i va anunciar la demostració completa de l'Últim Teorema de Fermat. Va presentar un esbós d'una demostració que introduïa les arrels complexes de la unitat i factoritzava l'equació (1.1) en els termes lineals $x^n + y^n = (x + y)(x + \zeta y) \dots (x + \zeta^{n-1} y)$, on $\zeta = e^{2\pi i/n}$ representa arrel n-èsima de la unitat amb n senar. No obstant, la seva demostració utilitzava un sèrie de detalls que no havia contemplat; la factorització fallava en alguns anells d'enters de cossos ciclotòmics i, a més a més faltava un control exhaustiu de les unitats en el seu treball. De fet Lamé havia ignorat en

la seva demostració que 3 anys abans, el matemàtic Ernst Kummer, havia provat que per $n = 23$ la factorització a l'anell ciclotòmic p-èsim no és única, i per tant la demostració de Lamé era incorrecta. A l'estiu del 1847 va començar a idear la seva pròpia demostració per certs exponents n, resolent les dificultats de la factorització única introduint la teoria dels "nombres complexos ideals". En retrospectiva podem veure aquesta teoria com la introducció d'aquests "nombres ideals"fora de l'anell d'enters $\mathbb{Z}[\zeta]$ per utilitzar-los com a factors quan factoritzem elements de $\mathbb{Z}[\zeta]$. Finalment, l'any 1850, Kummer va presentar la demostració dels dos casos de l'Últim Teorema de Fermat per certs exponents primers, els quals va anomenar *primers regulars*.

Kummer va afirmar que els primers regulars són infinits, fet que encara no s'ha demostrat; però el que si s'ha demostrat és la infinitud dels primers irregulars. Així doncs la demostració de Kummer va tenir un paper molt important, atès que va canviar el focus de les demostracions que havien fet fins aquell moment i, d'altra banda, va donar aire fresc als matemàtics posteriors.

El projecte

La motivació principal d'aquest treball és veure com va sorgir la teoria algebraica de nombres mitjançant la demostració de l'Últim Teorema de Fermat. Més concretament, ens centrem en el treball fet per Ernst Kummer, que, com hem dit anteriorment, és un matemàtic del segle XIX que va demostrar el Teorema per uns certs primers anomenats primers regulars. Durant aquest transcurs, es va trobar amb certes dificultats; la factorització en irreductibles dels elements dels anells d'enters i el control de les unitats. El mètode que va seguir va ser expressar l'equació (1.1) amb nombres complexos

$$z^n = (x + y)(x + \zeta y) \dots (x + \zeta^{n-1} y)$$

on $\zeta = e^{2\pi n/2}$ expressa l'arrel n-èsima de la unitat.

Per aquest motiu, l'objectiu principal d'aquest treball és desenvolupar la teoria necessària dels anells d'enters per poder estudiar la factorització en aquests i el comportament de les seves unitats. Amb aquests coneixements, podrem centrarnos en els anells d'enters dels cossos ciclotòmics, estudiant les seves propietats i l'estructura de les seves unitats, per, finalment, poder demostrar el primer cas de l'Últim Teorema de Fermat, seguint els passos de Kummer.

Pel que fa a la metodologia, aquest treball s'ha basat en la recerca bibliogràfica i posterior descripció dels conceptes de manera comprensiva per a tota persona amb coneixements d'estructures algebraiques. Per aquest fet també he desenvolupat conceptes adquirits a les assignatures d'Estructures Algebraiques i Equacions Algebraiques.

Estructura de la Memòria

Aquesta memòria consta de tres blocs importants. El primer bloc és una introducció de la teoria necessària d'anells d'enters algebraics, estudiant la factorització d'aquests i, per últim, presentar l'enunciat de dos teoremes molt importants de la teoria algebraica de nombres; el teorema de les unitats de Dirichlet i el teorema de finitud del grup de classes. El segon bloc és l'estudi dels cossos ciclotòmics, presentant propietats de l'anell d'enters ciclòtomic $\mathbb{Z}[\zeta]$ i l'estudi de les seves unitats. Finalment, el darrer bloc consta de la demostració del teorema.

2 Preliminars

2.1 Nocions bàsiques d'anells i cossos

En aquest treball considerem el terme *Anell* com un anell commutatiu amb l'element identitat $1 \neq 0$. Direm que l'anell A és un domini d'integritat si no té divisors de zero (és a dir, $\forall a, b \in A$ si $ab = 0$ aleshores $a = 0$ o $b = 0$). D'altra banda considerem que un anell A és un *Cos* Si $1 \neq 0$ i si tots els elements diferents de zero son unitats.

Definició 2.1. *Sigui A un anell i sigui $u \in A$, direm que u és una unitat si existeix un element $v \in A$ tal que $uv = 1$.*

2.2 Grups abelians finitament generats

Definició 2.2. *Sigui A un anell, un A-mòdul de M és un grup abelià $(M,+)$ amb una funció $\alpha : R \times M \longrightarrow M$, $\alpha(r, m) = rm$ que satisfà:*

a) $(r+s)m = rm+sm$,

a) $r(m+n) = rm+rn$,

c) $r(sm) = (rs)m$,

d) $1m = m$,

per tot $r, s \in A$ i $m, n \in M$

Veiem que si A és un cos K, aleshores un A-mòdul és un espai vectorial sobre K. A continuació introduirem unes definicions bàsiques indispensables alhora d'estudiar grups abelians finitament generats, un concepte que utilitzarem força al llarg d'aquest treball.

Definició 2.3. *Direm que G és un grup abelià finitament generat si G és finitament generat com a $\mathbb{Z}$-mòdul, de manera que existeixen $g_1, ..., g_n \in G$ tal que per tot $g \in G$*

$$g = m_1 g_1 + ... + m_n g_n$$

amb $m_i \in \mathbb{Z}$.

Definició 2.4. *Sigui G un grup abelià finitament generat. Direm que $g_1, ..., g_n \in G$ són linealment independents si qualsevol equació*

$$m_1 g_1 + ... + m_n g_n = 0$$

amb $m_i \in \mathbb{Z}$ implica que $m_1 = ... = m_n = 0$.

Definició 2.5. *Sigui G un grup abelià finitament generat. Direm que $\{g_1, ..., g_n\}$ és una $\mathbb{Z}$-base de G si generen G i són linealment independents. En aquest cas direm que G és un grup abelià lliure de rang n.*

Definició 2.6. *Una matriu quadrada sobre $\mathbb{Z}$ és unimodular si el seu determinant és ± 1.*

Lema 2.7. *Sigui G un grup abelià lliure de rang n i sigui $\{x_1, ..., x_n\}$ una $\mathbb{Z}$-base. Suposem que $A = (a_{ij})$ és una matriu quadrada $n \times n$ amb coeficients enters. Aleshores els elements*

$$y_i = \sum_{j=1}^{n} a_{ij} x_j$$

formen una base de G si i només si $A = (a_{ij})$ és unimodular.

Demostració. Per un cantó, si $\{y_1, ..., y_n\}$ és una $\mathbb{Z}$-base de G, aleshores existeixen b_{ij} enters tal que

$$x_i = \sum_{j=1}^{n} b_{ij} y_j.$$

D'aquesta manera, si considerem $B = (b_{ij})$, aleshores $AB = I_n$ on I_n és la matriu identitat. Per tant $\det(A)\det(B) = 1$ i A és unimodular.

Suposem ara que A és unimodular. Com $\det(A) \neq 0$, clarament els elements $y_1, ..., y_n$ són linealment independents. A causa de ser unimodular

$$A^{-1} = \frac{A^*}{\det(A)} = \pm A^*$$

on A^* és la transposada de la matriu adjunta i aquesta té coeficients enters. Fixant $B := A^{-1} = (b_{ij})$ obtenim $x_i = \sum_{j=1}^{n} b_{ij} y_j$. Així doncs $y_1, ..., y_n$ generen G i per tant formen una $\mathbb{Z}$-base. □

Teorema 2.8. *Tot subgrup H d'un grup abelià G lliure de rang n és un grup lliure de rang $s \leq n$. A més, existeix una $\mathbb{Z}$-base $\{u_1, ..., u_n\}$ de G i $\alpha_1, ..., \alpha_n \in \mathbb{Z}$ tal que $\alpha_1 u_1, ..., \alpha_s u_s$ és una $\mathbb{Z}$-base de H.*

La demostració d'aquest teorema es pot trobar al llibre [5] a les pàgines 29 i 30.

A continuació donarem una proposició vista a Estructures Algebraiques que utilitzarem per demostrar el següent Teorema.

Proposició 2.9. *Tot grup abelià finitament generat és producte directe d'un grup abelià finit i un grup lliure.*

Teorema 2.10. *Sigui G un grup abelià lliure de rang n i H un subgrup de G. Aleshores G/H és finit, si i només si, G i H tenen els mateixos rangs. En aquest cas, si G i H tenen com a $\mathbb{Z}$-bases $\{x_1, ..., x_n\}$ i $\{y_1, ..., y_n\}$ respectivament amb $y_i = \sum_{j=1}^{n} a_{ij} x_j$, aleshores*

$$|G/H| = |det(a_{ij})|.$$

Demostració. Sigui H un subgrup de G de rang s, utilitzant el Teorema 2.8 escollim $\mathbb{Z}$-bases $u_1, ..., u_n$ de G i $v_1, ..., v_s$ de H tal que $v_i = \alpha_i u_i$ per $1 \leq i \leq s$. Per la Proposició 2.9 G/H és el producte de grups cíclics finits d'ordres $\alpha_1, ..., \alpha_s$ i $n - s$ grups cíclics infinits. Per tant $|G/H|$ és finit si i només si $n = s$ i en aquest cas

$$|G/H| = \alpha_1 \dots \alpha_n.$$

Si $\{x_1, ..., x_n\}$ i $\{y_1, ..., y_n\}$ són $\mathbb{Z}$-bases de G i H respectivament, tal que $y_i = \sum_{j=1}^{n} a_{ij} x_j$, aleshores tenim

$$u_i = \sum_{j=1}^{n} b_{ij} x_j$$

$$v_i = \sum_{j=1}^{n} c_{ij} u_j$$

$$y_i = \sum_{j=1}^{n} d_{ij} v_j$$

on les matrius $B := (b_{ij})$ i $D := (d_{ij})$ són unimodulars pel Lema 2.7 i

$$C = (c_{ij}) = \begin{pmatrix} \alpha_1 & 0 & 0 & ... & 0 \\ 0 & \alpha_2 & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & \alpha_n \end{pmatrix}.$$

Clarament si $A = (a_{ij})$ es compleix $A = BCD$, i per tant, $\det(A) = \det(B)\det(C)\det(D)$. Així doncs

$$|\det(A)| = |\pm 1||\det(c)||\pm 1| = |\alpha_1 \dots \alpha_n| = |G/H|$$

com volíem demostrar. □

3 Enters algebraics

3.1 Anell d'enters algebraics

En aquesta secció introduirem el concepte d'enter algebraic i veurem que el conjunt d'aquests forma un subanell de $\mathbb{C}$. Abans però recordarem les nocions bàsiques dels nombres algebraics.

Definició 3.1. *Un nombre $\alpha \in \mathbb{C}$ és algebraic si existeix un polinomi no nul $f(x)$ amb coeficients racionals tal que $f(\alpha) = 0$. El conjunt dels nombres algebraics el denotem com $\overline{\mathbb{Q}}$.*

Definició 3.2. *Direm que K és un cos de nombres si és una extensió finita sobre $\mathbb{Q}$.*

Tot cos algebraic de nombres K el podem expressar com $\mathbb{Q}(\theta)$, on θ és un nombre algebraic, ja que totes les extensions de $\mathbb{Q}$ són separables. (Pel teorema de l'element primitiu).

Definició 3.3. *Un enter algebraic és un element $\alpha \in \mathbb{C}$ tal que α satisfà la següent equació:*

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$$

Amb $n \geq 1$ i $c_1, ..., c_n \in \mathbb{Z}$. El conjunt d'enters algebraics l'anomenarem $\overline{\mathbb{Z}}$.

Proposició 3.4. $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

Demostració. Sigui $\alpha \in \mathbb{Z}$, com α és arrel del polinomi $f(x) = x - \alpha$, aleshores $\alpha \in \overline{\mathbb{Z}}$, per tant $\alpha \in \mathbb{Q} \cap \overline{\mathbb{Z}}$.

Per demostrar l'altre inclusió agafem un $r \in \mathbb{Q} \cap \overline{\mathbb{Z}}$, tal que $r = \frac{c}{d}$, amb $c, d \in \mathbb{Z}$, $d \neq 0$ i $(c, d) = 1$. Com $r \in \overline{\mathbb{Z}}$, agafem un polinomi mònic $f(x) = x^n + a_1x^{n-1} + ... + a_n$, $a_i \in \mathbb{Z}, n \geq 1$, tal que $f(r) = 0$, és a dir, $(\frac{c}{d})^n + a_1(\frac{c}{d})^{n-1} + ... + a_n = 0$. Multiplicant per d^n als dos costats, obtenim

$$c^n + a_1c^{n-1}d + ... + a_nd^n = 0$$
$$c^n = -d(a_1c^{n-1} + ... + a_nd^{n-1}).$$

Com que $d|c^n$ i $(c, d) = 1$ aleshores $d = 1$, i per tant $r \in \mathbb{Z}$. Finalment $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

□

Proposició 3.5. *Sigui α un nombre algebraic, aleshores existeix un nombre natural $a \in \mathbb{N}$ tal que $a\alpha \in \overline{\mathbb{Z}}$.*

Demostració. Al ser α és un nombre algebraic, α satisfà

$$c_0\alpha^n + c_1\alpha^{n-1} + ... + c_n = 0$$

amb $c_i \in \mathbb{Q}$ per $i = 0, ..., n$. Sigui d un divisor comú dels coeficients c_i de manera que $c_i = \frac{b_i}{d}$, amb $b_i \in \mathbb{Z}$. Aleshores tenim

$$b_0\alpha^n + b_1\alpha^{n-1} + ... + b_n = 0$$

on podem concloure, sense pèrdua de generalitat, que $b_0 \geq 1$. Multiplicant per b_0^{n-1} a ambdós costats de la igualtat obtenim

$$\begin{aligned} 0 &= b_0^n\alpha^n + b_1^{n-1}\alpha^{n-1} + ... + b_n = \\ &= (b_0\alpha)^n + b_1(b_0\alpha)^{n-1} + ... + b_nb_0^{n-1} \end{aligned}$$

que ens implica que $b_0\alpha \in \overline{\mathbb{Z}}$. □

És conegut que el conjunt de nombres algebraics és un subcòs de $\mathbb{C}$. Així doncs utilitzarem aquest resultat per veure que $\overline{\mathbb{Z}}$ és un subanell de $\overline{\mathbb{Q}}$. Per veure-ho necessitarem un lema previ.

Lema 3.6. *Un nombre complex θ és un enter algebraic si i només si, el grup additiu generat per les potències $1, \theta, \theta^2, ...$ és finitament generat.*

Demostració. Sigui θ un enter algebraic, aleshores per algun $n \geq 1$ tenim

$$\theta^n + a_{n-1}\theta^{n-1} + ... + a_0 = 0 \tag{3.1}$$

on $a_i \in \mathbb{Z}$. Volem veure que cada potència de θ està dins del grup additiu generat per $\{1, \theta, ..., \theta^{n-1}\}$. Anomenarem Γ a aquest grup. Podem veure a (2.1) que $\theta^n \in \Gamma$. Inductivament, suposant que per $m \geq n$, $\theta^m \in \Gamma$, aleshores

$$\theta^{m+1} = \theta^{m+1-n+n} = \theta^{m+1-n}\theta^n = \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - ... - a_0) \in \Gamma$$

i finalment podem observar que totes les potències de θ estan a Γ.

Per veure l'altre implicació, suposarem que totes les potències de θ pertanyen a un grup additiu G finitament generat. El subgrup Γ de G generat per $\{1, \theta, ..., \theta^n\}$ ha de ser finitament generat, ja que qualsevol subgrup d'un grup abelià finitament generat és finitament generat. Suposarem que Γ té com a generadors $v_1, ..., v_n$, on cada v_i és un polinomi en la variable θ amb coeficients enters, així doncs θv_i també és un polinomi. Per tant existeixen b_{ij} enters tal que

$$\theta v_i = \sum_{j=1}^{n} b_{ij}v_j.$$

Igualant totes les equacions a zero obtenim un sistema d'equacions homogeni que té per incògnites v_i, de la següent forma

$$\begin{aligned} (b_{11} - \theta)v_1 + b_{12}v_2 + ... + b_{1n}v_n &= 0 \\ b_{21}v1 + (b_{22} - \theta)v_2 + ... + b_{1n}v_n &= 0 \\ &... \\ b_{n1}v1 + b_{n2}v_2 + ... + (b_{nn} - \theta)v_n &= 0 \end{aligned}$$

Com existeix una solució $v_1, ..., v_n \in \mathbb{C}$ amb algun $v_i \neq 0$, en efecte

$$\begin{vmatrix} b_{11} - \theta & b_{12} & ... & b_{1n} \\ b_{21} & b_{22} - \theta & ... & b_{2n} \\ ... & ... & ... & ... \\ b_{n1} & b_{n2} & ... & b_{nn} - \theta \end{vmatrix} = 0.$$

Desenvolupant-ho podem veure que θ satisfà un polinomi mònic amb coeficients enters. □

Teorema 3.7. *El conjunt d'enters algebraics $\overline{\mathbb{Z}}$ forma un subanell de el cos de nombres algebraics.*

Demostració. Siguin $\theta_1, \theta_2 \in \overline{\mathbb{Z}}$. El nostre objectiu és veure que $\theta_1 + \theta_2$ i $\theta_1\theta_2 \in \overline{\mathbb{Z}}$. Pel Lema 3.6 tenim que totes les potències de θ_1 (resp. θ_2) pertanyen al subgrup additiu finitament generat de $\mathbb{C}$, Γ_{θ_1} (resp. Γ_{θ_1}). A més a més, totes les potències de $\theta_1 + \theta_2$ i $\theta_1\theta_2$ són combinacions lineals enteres d'elements $\theta_1^i\theta_2^j$ que pertanyen a $\Gamma_{\theta_1}\Gamma_{\theta_2} \subseteq \mathbb{C}$. Al ser Γ_{θ_1} i Γ_{θ_2} finitament generats, tenen com a generadors $\Gamma_{\theta_1} = \langle v_1, ..., v_n \rangle$ i $\Gamma_{\theta_2} = \langle w_1, ..., w_m \rangle$; per tant $\Gamma_{\theta_1}\Gamma_{\theta_2}$ és un grup additiu finitament generat i generat per $v_i w_j$ amb $1 \leq i \leq n$, $1 \leq j \leq m$. Així doncs les potències de $\theta_1 + \theta_2$ i $\theta_1\theta_2$ pertanyen a un subgrup additiu de $\mathbb{C}$ finitament generat, i tornant a utilitzar el Lema 3.6, tenim que $\theta_1 + \theta_2$ i $\theta_1\theta_2$ són enters algebraics. Per tant $\overline{\mathbb{Z}}$ és subanell de $\overline{\mathbb{Q}}$. □

Definició 3.8. *L'anell d'enters d'un cos de nombres K el simbolitzem amb $\mathcal{O}_k$ i ve donat per*

$$\mathcal{O}_k = \overline{\mathbb{Z}} \cap K$$

Veiem que $\mathcal{O}_k$ és un anell ja que $\overline{\mathbb{Z}}$ és un subanell de $\mathbb{C}$ i K és un subcòs de $\mathbb{C}$, per tant també un subanell.

Corol·lari 3.9. *Sigui K un cos de nombres, aleshores $K = \mathbb{Q}(\theta)$, per algun $\theta \in \mathcal{O}_k$.*

Demostració. Pel teorema de l'element primitiu tenim que $K = \mathbb{Q}(\phi)$ per algun $\phi \in \overline{\mathbb{Q}}$. A més, per la Proposició 2.7. $\theta = c\phi$ és un enter algebraic per qualsevol $c \in \mathbb{Z}$. Per tant $\mathbb{Q}(\theta) = \mathbb{Q}(\phi)$. □

3.2 Conjugats i discriminants

El conjunt de monomorfismes $\sigma_i : K \longrightarrow \mathbb{C}$ juga un paper fonamental alhora d'estudiar la teoria de l'anell d'enters d'un cos de nombres K. A més, en aquesta secció veurem què són els conjugats d'un element i el discriminant d'una base de K.

Teorema 3.10. *Sigui $K = \mathbb{Q}(\theta)$ un cos de nombres amb $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$. Aleshores hi ha exactament n monomorfismes $\sigma_i : K \longrightarrow \mathbb{C}$ (i=1,...,n) diferents. Els elements $\sigma_i(\theta) = \theta_i \in \mathbb{C}$ són els zeros del polinomi mínim de θ sobre $\mathbb{Q}$.*

Demostració. Siguin $\theta_1, ..., \theta_n$ els diferents zeros del polinomi mínim p sobre θ, aleshores el polinomi mínim de θ_i també és p, ja que aquest ha de dividir p i p és irreductible. Per aquest motiu existeix un únic isomorfisme de cossos $\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta_i)$ tal que $\sigma_i(\theta) = \theta_i$. De fet, si $\alpha \in \mathbb{Q}(\theta)$ aleshores existeix un $r \in \mathbb{Q}[t]$, amb $\partial r < n$, tal que $\alpha = r(\theta)$; i ha de complir

$$\sigma_i(\alpha) = r(\theta_i).$$

Per tant els monomorfismes σ_i queden unívocament determinats per les imatges de θ. Altrament si $\sigma_i : K \longrightarrow \mathbb{C}$ és monomorfisme de cossos, per les propietats d'aquest, σ deixa fixes els elements de $\mathbb{Q}$. Per tant tenim

$$p(\sigma(\theta)) = \sigma(p(\theta)) = \sigma(0) = 0$$

de manera que $\sigma(\theta)$ és una arrel de p, i per aquest motiu un dels θ_i per algun i. Aleshores clarament $\sigma = \sigma_i$. □

Proposició 3.11. *Sigui $\mathcal{O}_k$ l'anell d'enters del cos de nombres K, si $\alpha \in \mathcal{O}_k$ aleshores $\sigma_i(\alpha)$, amb $i = 1, ..., n$, són enters algebraics.*

Demostració. Com α un enter algebraic, existeix un polinomi mònic $p \in \mathbb{Z}[x]$ tal que $p(\alpha) = 0$. Utilitzant que σ_i, $i = 1, ..., n$, és monomorfisme de cossos i deixa fixos els elements de $\mathbb{Q}$, tenim

$$p(\sigma_i(\alpha)) = \sigma_i(p(\alpha)) = \sigma_i(0) = 0.$$

de manera que $\sigma_i(\alpha)$ és un enter algebraic. □

Definició 3.12. *Per cada $\alpha \in K$ definim el "polinomi característic"de α sobre K*

$$f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha)).$$

Teorema 3.13. *Els coeficients del polinomi característic són nombres racionals, per tant $f_\alpha(t) \in \mathbb{Q}[t]$.*

Demostració. Primer de tot observem que, com K és una extensió finita sobre $\mathbb{Q}$, si $\alpha \in K$, aleshores $\alpha = r(\theta)$ per algun $r \in \mathbb{Q}[x]$ amb $\partial r < n$. Així doncs el polinomi característic té la següent forma

$$f_\alpha(x) = \prod_{i=1}^{n}(x - r(\theta_i))$$

on θ_i recorre tots els zeros del polinomi mínim p de θ. Els coeficients de $p(x)$, per definició, són nombres racionals. A més, per les fórmules de Viète, podem veure que els coeficients de $f_\alpha(t)$ són de la forma

$$h(\theta_1, ..., \theta_n)$$

on $h(t_1, ..., t_n) \in \mathbb{Q}[t_1, ..., t_n]$ és un polinomi simètric. Així doncs, aplicant el teorema dels polinomis simètrics, $f_\alpha(t) \in \mathbb{Q}[t]$. □

Definició 3.14. *Sigui K un cos de nombres, α un element de K qualsevol, anomenarem K-conjugats d'α als elements $\sigma_i(\alpha)$ per $i = 1, ..., n$.*

Definició 3.15. *Sigui $K = \mathbb{Q}(\theta)$ un cos algebraic de nombres amb grau d'extensió n, sigui $\{\alpha_1, ..., \alpha_n\}$ una $\mathbb{Q}$-base de K . Definim el discriminant d'aquesta base com*

$$\Delta[\alpha_1, ..., \alpha_n] = \{det[\sigma_i(\alpha_j)]\}^2$$

Proposició 3.16. *Siguin $\{\beta_1, ..., \beta_n\}$ i $\{\alpha_1, ..., \alpha_n\}$ dues $\mathbb{Q}$-bases de K, es compleix*

$$\Delta[\beta_1, ..., \beta_n] = [det(c_{ik})]^2 \Delta[\alpha_1, ..., \alpha_n].$$

on c_{ik} és la matriu de canvi de base de $\{\alpha_1, ..., \alpha_n\}$ a $\{\beta_1, ..., \beta_n\}$ amb coeficients a $\mathbb{Q}$.

Demostració. Sigui $\{\beta_1, ..., \beta_n\}$ i $\{\alpha_1, ..., \alpha_n\}$ bases de K, en efecte, podem escriure $\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_k$. A més, el $det(c_{ik}) \neq 0$ ja que c_{ij} és la matriu canvi de base. Per tant, aplicant que els monomorfismes σ_i deixen fixos els elements de $\mathbb{Q}$ i que el determinant del producte és el producte de determinants, obtenim

$$\Delta[\beta_1, ..., \beta_n] = [det(c_{ik})]^2 \Delta[\alpha_1, ..., \alpha_n].$$

□

Teorema 3.17. *El discriminant de qualsevol base de $K = \mathbb{Q}(\theta)$ és un nombre racional diferent de zero.*

Demostració. Primer de tot fixem una base amb la que puguem treballar bé com ara $\{1, \theta, ..., \theta^{n-1}\}$. Si els conjugats de θ són $\theta_1, ..., \theta_n$, el determinant serà:

$$\Delta[1, \theta, ..., \theta^{n-1}] = (det\theta_i^j)^2 = \begin{vmatrix} 1 & \theta_1 & ... & \theta_1^{n-1} \\ 1 & \theta_2 & ... & \theta_2^{n-1} \\ ... & ... & ... & ... \\ 1 & \theta_n & ... & \theta_n^{n-1} \end{vmatrix}^2$$

Qualsevol determinant de la forma $D = det(t_i^j)$ s'anomena determinant de $Vandermonde$ i el seu valor és

$$D = \prod_{1 \leq i < j \leq n} (t_i - t_j). \tag{3.2}$$

Per tant el valor del discriminant és

$$\Delta = \Delta[1, \theta, ..., \theta^{n-1}] = \left(\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2$$

Sigui ara $p(t_1, ..., t_n) = D^2 \in \mathbb{Q}[X_1, ..., X_n]$, aleshores $p(\theta_1, ..., \theta_n) = \Delta$. Així doncs, pel Teorema dels Polinomis Simètrics, com $p(t_1, ..., t_n)$ és simètric, aleshores Δ és racional. A més com θ_i són diferents dos a dos, $\Delta \neq 0$.

Tot seguit demostrarem que es compleix el resultat per qualsevol base. Sigui $\{\beta_1, ..., \beta_n\}$ una base qualsevol de K de manera que

$$\beta_k = \sum_{i=1}^{n} c_{ik}\theta^{i-1},$$

on $c_{ik} \in \mathbb{Q}$ i $det(c_{ik}) \neq 0$. Hem vist a la Proposició 3.16 que el discriminant de $\{\beta_1, ..., \beta_n\}$ és

$$\Delta[\beta_1, ..., \beta_n] = [det(c_{ik})]^2\Delta$$

en conseqüència $\Delta[\beta_1, ..., \beta_n] \neq 0$ i és racional. En efecte si tots els $\theta_i \in \mathbb{R}$ aleshores $\Delta, \Delta[\beta_1, ..., \beta_n]$ són positius. □

3.3 Bases d'enters

Sigui $K = \mathbb{Q}(\theta)$ un cos de nombres de grau n, sabem que una $\mathbb{Q}$-base de K és $\{1, \theta, ..., \theta^{n-1}\}$. Pel que fa $\mathcal{O}_k$ hem vist que és un anell commutatiu, per tant $(\mathcal{O}_k, +)$ és un grup abelià .

Definició 3.18. *Sigui $\mathcal{O}_k$ l'anell d'enters de K, anomenarem base d'enters de K (o de $\mathcal{O}_k$) a la $\mathbb{Z}$-base de $(\mathcal{O}_k, +)$.*

Hem definit la base d'enters però no és suficient, hem de provar la seva existència. Per fer-ho, veurem que $(\mathcal{O}_k, +)$ és un grup abelià lliure de rang n.

Lema 3.19. *Si $\{\alpha_1, ..., \alpha_n\}$, $\alpha_i \in \mathbb{Z}$, és una base de K, aleshores el discriminant $\Delta[\alpha_1, ..., \alpha_n]$ és un enter diferent de zero.*

Demostració. En primer lloc, pel Teorema 3.17 sabem que el discriminant $\Delta[\alpha_1, ..., \alpha_n] \in \mathbb{Q}\backslash\{0\}$. En segon lloc, com α_i són enters algebraics, per la definició de discriminant i la Proposició 3.11, aleshores $\Delta[\alpha_1, ..., \alpha_n] \in \overline{\mathbb{Z}}$. Per tant utilitzant la Proposició 3.4 el discriminant és un enter diferent de zero. □

Teorema 3.20. *Tot cos de nombres K admet una base d'enters. i el grup $(\mathcal{O}_k, +)$ és un grup abelià lliure de rang igual al grau d'extensió de K.*

Demostració. D'una banda hem vist que $K = \mathbb{Q}(\theta)$, on $\theta \in \mathcal{O}_k$, de manera que $\{1, \theta, ..., \theta^{n-1}\}$ és una $\mathbb{Q}$-base de K formada per enters algebraics. Ara bé, aquest fet no ens implica que $\{1, \theta, ..., \theta^{n-1}\}$ sigui una base d'enters. D'altra banda, hem vist al Lema 3.19., que el discriminant d'una $\mathbb{Q}$-base formada per enters algebraics és enter. Així doncs, seleccionem una $\mathbb{Q}$-base $\{\omega_1, ..., \omega_n\}$ d'enters algebraics tal que el discriminant $|\Delta[\omega_1, ..., \omega_n]|$ sigui mínim. El nostre objectiu és veure que és una base d'enters, per tant una $\mathbb{Z}$-base de $(\mathcal{O}_k, +)$.

Suposem que no fos així, aleshores existeix $\omega \in \mathcal{O}_k$ tal que

$$\omega = a_1\omega_1 + ... + a_n\omega_n$$

amb $a_i \in \mathbb{Q}$, no tots els coeficients a $\mathbb{Z}$. Reordenem de tal manera que $a_1 \notin \mathbb{Z}$. Aleshores $a_1 = a + r$ on $a \in \mathbb{Z}$ i $0 < r < 1$. Definim

$$\begin{aligned} \psi_1 &= \omega - a\omega_1 \\ \psi_i &= \omega_i \qquad\qquad (2 \leq i \leq n) \end{aligned}$$

i tenim que $\{\psi_1, ..., \psi_n\}$ és una $\mathbb{Q}$-base formada per elements enters. En efecte, el determinant del la matriu canvi de base de $\{\omega_1, ..., \omega_n\}$ a $\{\psi_1, ..., \psi_n\}$ és

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & ... & a_n \\ 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 \end{vmatrix} = r$$

per tant, per la Proposició (3.7),

$$\Delta[\psi_1, ..., \psi_n] = r^2 \Delta[\omega_1, ..., \omega_n].$$

Ara bé, el fet que $0 < r < 1$ ens contradiu l'elecció de la base $\{\omega_1, ..., \omega_n\}$, la qual minimitzava el discriminant.

Per tant $\{\omega_1, ..., \omega_n\}$ és una base d'enters, fet que ens implica que $(\mathcal{O}_k, +)$ és un grup abelià lliure de rang n. □

Proposició 3.21. *Siguin $\{\alpha_1, ..., \alpha_n\}$ i $\{\beta_1, ..., \beta_n\}$ dues bases enteres de K, aleshores $\Delta[\alpha_1, ..., \alpha_n] = \Delta[\beta_1, ..., \beta_n]$.*

Demostració. Sigui $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$. Pel Lema 2.7 la matriu de canvi de base $A = (a_{ij})$ és unimodular. Per tant aplicant la Proposició 3.16 es veu directament

$$\Delta[\alpha_1, ..., \alpha_n] = (\pm 1)^2 \Delta[\beta_1, ..., \beta_n] = \Delta[\beta_1, ..., \beta_n].$$

□

Com el discriminant d'una base d'enters és independent de la base que escollim podem dir que aquest és el discriminant de K o $\mathcal{O}_k$. Així doncs al llarg del treball utilitzarem aquest terme com el discriminant de K.

3.4 Normes i traces

Sigui $K = \mathbb{Q}(\theta)$ un cos de nombres amb grau d'extensió n i siguin $\sigma_1, ..., \sigma_n$ els monomorfismes $K \longrightarrow \mathbb{C}$. Per qualsevol $\alpha \in K$ definim la norma com

$$N_k(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

i la traça

$$T_k(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

.

Teorema 3.22. *Sigui K un cos algebraic de nombres de grau n. Siguin $\alpha, \beta \in K$ i $p, q \in \mathbb{Q}$, Aleshores*

$$T(p\alpha + q\beta) = pT(\alpha) + qT(\beta)$$

i

$$N(p\alpha\beta) = p^n N(\alpha)N(\beta)$$

Demostració. Siguin $\sigma_k : K \longrightarrow \mathbb{C}$ (k=1,...,n) els n monomorfismes diferents, per les propietats d'aquests tenim:

$$\begin{aligned} T(p\alpha + q\beta) &= \sum_{k=1}^{n} \sigma_k(p\alpha + q\beta) = \sum_{k=1}^{n} (p\sigma_k(\alpha) + q\sigma_k(\beta)) = \\ &= p\sum_{k=1}^{n} \sigma_k(\alpha) + q\sum_{k=1}^{n} \sigma_k(\beta) = pT(\alpha) + qT(\beta) \end{aligned}$$

$$\begin{aligned} N(p\alpha\beta) &= \prod_{k=1}^{n} \sigma_k(p\alpha\beta) = \prod_{k=1}^{n} p\sigma_k(\alpha)\sigma_k(\beta) = \\ &= p^n \left(\prod_{k=1}^{n} \sigma_k(\alpha)\right)\left(\prod_{k=1}^{n} \sigma_k(\beta)\right) = p^n N(\alpha)N(\beta) \end{aligned}$$

□

Proposició 3.23. *Sigui $\mathcal{O}_k$ l'anell d'enters de un cos de nombres K. Si $\alpha \in \mathcal{O}_k$, aleshores $N(\alpha)$ i $T(\alpha)$ són enteres.*

Demostració. Per la definició de polinomi característic tenim

$$f_\alpha(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = x^n - T(\alpha)x^{n-1} + ... + (-1)^n N(\alpha). \tag{3.3}$$

on la última igualtat ve donada perquè la suma de les arrels d'un polinomi és l'oposat del terme de grau $n-1$ i la multiplicació d'aquestes és el terme independent per les Fórmules de Viète. Per tant, com $\alpha \in \mathcal{O}_k \subseteq K$, la norma i la traça de α són racionals pel Teorema 3.13. D'altra banda, si $\alpha \in \overline{\mathbb{Z}}$, la Proposició 3.11 ens implica que $\sigma_i(\alpha) \in \overline{\mathbb{Z}}$. D'aquesta manera obtenim que $T(\alpha)$ i $N(\alpha)$ pertanyen a $\mathbb{Q} \cap \overline{\mathbb{Z}}$, que per la Proposició 3.4, pertanyen ambdues a $\mathbb{Z}$.

□

Proposició 3.24. *Sigui $\mathcal{O}_k$ l'anell d'enters d'un cos de nombres K i sigui $u \in \mathcal{O}_k$, aleshores u és una unitat si i només si $N(u) = \pm 1$.*

Demostració. Si u és una unitat existeix un $v \in \mathcal{O}_k$ tal que $uv = 1$. Com $1 = N(uv) = N(u)N(v)$ i $N(u), N(v) \in \mathbb{Z}$, per la Proposició 3.23, aleshores $N(u) = \pm 1$.

D'altra banda, si $N(u) = \pm 1$, aleshores

$$\sigma_1(u)\sigma_2(u)\ldots\sigma_n(u) = \pm 1.$$

Suposem sense pèrdua de generalitat que $\sigma_1(u) = u$, de manera que tots els altres $\sigma_i(u)$ són enters algebraics per la Proposició 3.11. Escrivim

$$v = \pm\sigma_2(u)\dots\sigma_n(u) \in \overline{\mathbb{Z}}$$

llavors $uv = 1$, així doncs $v = u^{-1} \in K$. Per tant $v \in K \cap \overline{\mathbb{Z}} = \mathcal{O}_k$ i u és una unitat. $\square$

4 Factorització dels anells d'enters

Al capítol anterior hem vist que el conjunt d'enters algebraics de $\mathcal{O}_k$ d'un cos de nombres K forma un anell. És habitual pensar que un anell d'enters admet factorització única en elements irreductibles, però el fet és que, segons en quins anells ens trobem, aquesta falla. L'objectiu d'aquest capítol és estudiar la factorització en elements irreductibles a l'anell d'enters d'un cos de nombres.

4.1 Falla la factorització única en elements irreductibles

En aquesta secció veurem un cas on podem factoritzar un element en dos productes d'irreductibles diferents. Això si, prèviament necessitem formalitzar un seguit de definicions.

Definició 4.1. *Dos elements $a, b \in A$ són associats si existeix una unitat $u \in A$ tal que $a = ub$ (observem que la relació és simètrica: si $a = ub$, aleshores $b = va$ amb $uv = 1$).*

Definició 4.2. *Direm que dues factoritzacions*

$$a_1 a_2 \dots a_n = b_1 b_2 \dots b_n$$

són equivalents si b_i és associat a un $a_{\pi(i)}$ per alguna permutació $\pi \in S_n$.

Definició 4.3. *Sigui $p \in A$. Direm que p és irreductible si p no és una unitat i si $p = ab$, aleshores a és una unitat o b és una unitat.*

Definició 4.4. *Sigui $p \in A$, direm que p és un element primer si $p|ab$, aleshores $p|a$ o $p|b$ per tot $a, b \in A$.*

Tot cos quadràtic, és a dir cos de nombres tal que $[K : \mathbb{Q}] = 2$, es pot expressar com $K = \mathbb{Q}(\sqrt{d})$ on d és un enter lliure de quadrats. Sigui d un enter lliure de quadrats, si $d \equiv 2, 3 \pmod 4$, aleshores l'anell d'enters de $K = \mathbb{Q}(\sqrt{d})$ és $\mathbb{Z}[\sqrt{d}]$. En cas contrari $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Per simplificar-ho analitzarem un exemple del primer cas.

Exemple 4.5. Suposem que $d = 10$, aleshores l'anell d'enters és $\mathbb{Z}[\sqrt{10}]$. Considerem

$$6 = 2 \times 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right).$$

L'objectiu és provar que tots els factors són irreductibles i que les factoritzacions són realment diferents. Si $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, definim $\overline{\alpha} = a - b\sqrt{d}$ com el seu conjugat complex. Utilitzant la definició de norma que hem vist al capítol anterior

$$= N(\alpha) = \alpha\overline{\alpha} = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2$$

Si $\alpha \in \mathbb{Z}[\sqrt{d}]$, per la Proposició 3.23, sabem que $N(\alpha) \in \mathbb{Z}$.

Lema 4.6. *A* $\mathbb{Z}[\sqrt{10}]$ *les des factoritzacions*

$$6 = 2 \times 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$$

no són equivalents.

Demostració. Si α_1 i α_2 són associats, existeix una unitat u tal que $\alpha_2 = u\alpha_1$. Aleshores

$$N(\alpha_2) = N(u\alpha_1) = N(u)N(\alpha_1) = \pm N(\alpha_1)$$

on la última igualtat ve donada per la Proposició 3.24. Per aquest motiu deduïm que si les dues factoritzacions són equivalents, aleshores les normes dels factors de cada costat han de ser iguals en valor absolut. Malgrat tot a $\mathbb{Z}[\sqrt{10}]$,

$$\begin{aligned} N(2) &= 2^2 = 4 \\ N(3) &= 3^2 = 9 \\ N\left(4 + \sqrt{10}\right) &= 4^2 - 10 \times 1^2 = 6 \\ N\left(4 - \sqrt{10}\right) &= 4^2 - 10 \times 1^2 = 6 \end{aligned}$$

així doncs observem que les normes dels factors són diferents i per tant la factorització no és equivalent. □

A continuació volem comprovar que no podem factoritzar més els factors de l'equació.

Lema 4.7. *Tots els factors de la igualtat*

$$6 = 2 \times 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$$

són irreductibles.

Demostració. En primer lloc volem veure que no existeix cap element $\alpha \in \mathbb{Z}[\sqrt{10}]$ tal que $N(\alpha) = \pm 2$ i $N(\alpha) = \pm 3$. Suposem que existeix $\alpha = a + b\sqrt{10}$ tal que $N(\alpha) = a^2 - 10b^2 = \pm 2$. Aquest fet implica que $a^2 - 10b^2 = 2$ o $a^2 - 10b^2 = -2$. Considerem ara aquestes igualtats mòdul 5 i obtenim $a^2 \equiv 2 \pmod 5$ o $a^2 \equiv 3 \pmod 5$. No obstant ambdós casos són impossibles ja que $a^2 \equiv \pm 1, 0 \pmod 5$. Anàlogament veiem que no existeix cap $\alpha \in \mathbb{Z}[\sqrt{10}]$ amb $N(\alpha) = \pm 3$.

En segon lloc suposem que $2 = \alpha\beta$ amb $\alpha, \beta \in \mathbb{Z}[\sqrt{10}]$. Aleshores $4 = N(2) = N(\alpha)N(\beta)$. Estudiant els possibles valors de α i β observem que si $N(\alpha) = \pm 1$ i $N(\beta) = \pm 4$, aleshores α és una unitat. Anàlogament si $N(\alpha) = \pm 4$ i $N(\beta) = \pm 1$, implica que β és una unitat. Com la norma és entera, la única possibilitat que queda és que $N(\alpha) = N(\beta) = \pm 2$ que pel que hem vist abans, no és possible. Per tant 2 és irreductible. De la mateixa manera, si 3 factoritzés com el producte $\alpha\beta$, cap de les dues unitats, aleshores $N(\alpha) = N(\beta) = \pm 3$, fet que no és possible. Així doncs, 3 també és irreductible.

Finalment, la única forma de factoritzar $4 \pm \sqrt{10}$ sense unitats seria amb el producte d'un element amb norma ± 2 i un element amb norma ± 3 i com hem vist que no pot ser, aleshores tots els elements són irreductibles. □

En definitiva, hem vist que les factoritzacions en elements irreductibles no són equivalents, per tant la factorització en aquest anell no és única.

Cal remarcar també que els factors $2, 3, 4+\sqrt{10}, 4-\sqrt{10}$ són elements irreductibles però no primers. Efectivament $2|(4+\sqrt{10})(4-\sqrt{10})$ però $2 \nmid 4 \pm \sqrt{10}$ atès que $\frac{4\pm\sqrt{10}}{2} = 2 \pm \frac{1}{2}\sqrt{10} \notin \mathbb{Z}[\sqrt{10}]$. Vist d'una altra manera, si $2|(4+\sqrt{10})$, aleshores 2 i $4+\sqrt{10}$ haurien de ser associats ja que els dos són irreductibles, però hem vist que no són associats.

4.2 Nombres ideals de Kummer

A la secció anterior hem vist que no hi ha factorització única en elements irreductibles a tots els anells d'enters. Kummer va intentar resoldre aquest problema incloent-hi els "nombres ideals". La idea era aconseguir la factorització única en elements primers afegint-hi aquest tipus de nombres. Si ens fixem amb l'exemple de l'anterior secció, la idea de Kummer va ser inventar els símbols $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$, $\mathfrak{a}_4$ de manera que

$$\begin{aligned} 2 &= \mathfrak{a}_1 \times \mathfrak{a}_2 \\ 3 &= \mathfrak{a}_3 \times \mathfrak{a}_4 \\ 4+\sqrt{10} &= \mathfrak{a}_1 \times \mathfrak{a}_3 \\ 4-\sqrt{10} &= \mathfrak{a}_2 \times \mathfrak{a}_4. \end{aligned}$$

Aleshores el problema de la factorització única de $6 = 2\times 3 = \left(4+\sqrt{10}\right)\left(4-\sqrt{10}\right)$ s'arregla:

$$(\mathfrak{a}_1 \times \mathfrak{a}_2) \times (\mathfrak{a}_3 \times \mathfrak{a}_4) = (\mathfrak{a}_1 \times \mathfrak{a}_3) \times (\mathfrak{a}_2 \times \mathfrak{a}_4).$$

Ara bé, notem que aquest conjunt de símbols no tenen molt significat en realitat. No obstant, Kummer esperava que aquests símbols es manipulessin de manera que es poguessin obtenir resultats significatius.

Uns anys més tard, Dedekind va reformular la idea de Kummer dels nombres ideals i crea la noció d'ideal d'un anell. Principalment, però, s'interessa pels ideals dels anells d'enters, atès que és on es troba un dels resultats més importants d'aquesta teoria.

5 Ideals

Al capítol anterior hem vist que falla la factorització única en elements irreductibles dels anells d'enters de cossos de nombres. A més a més hem vist com Kummer va intentar solucionar aquest problema treballant amb ideals. En aquest capítol formalitzem aquesta idea i demostrarem que hi ha factorització única en ideals primers a $\mathcal{O}_k$.

Definició 5.1. *Sigui A un anell commutatiu. un subconjunt $I \subset A$ és un ideal de A si satisfà les següents condicions:*

(i) I és un subgrup additiu de A és a dir:

(a) $0 \in I$.

(b) Si $a,b \in I \Rightarrow a+b \in I$ i $a-b \in I$.

(ii) Si $a \in A$ i $b \in I$ aleshores $ab \in I$.

Definició 5.2. *Siguin I, J ideals en un anell commutatiu A, definim el producte $IJ=\{\sum_{i=1}^{n} a_i b_i, n \geq 1, a_i \in I, b_i \in J\}$. Clarament IJ es ideal.*

Definició 5.3. *Direm que un ideal és principal si està generat per un únic element. A més a més, si A és un domini d'integritat, aleshores A és un domini d'ideals principals si tot ideal és principal.*

A l'assignatura d'estructures algebraiques vam veure que tot domini d'ideals principals és un domini de factorització única. D'aquesta manera notem que si falla la factorització única, no tots els ideals són principals. De fet, podem observar que els *nombres ideals complexos* introduïts per Kummer són ideals no principals, atès que no poden estar generats per un únic element.

5.1 Dominis Noetherians

En aquesta secció donem algunes propietats dels Dominis Noetherians que utilitzarem al llarg del capítol.

Definició 5.4. *Un domini D és noetherià si tot ideal de D és finitament generat.*

Definició 5.5. *Condició de cadena ascendent. Donada una cadena ascendent d'ideals:*

$$I_0 \subseteq I_1 \subseteq ... \subseteq I_n \subseteq ... \tag{5.1}$$

aleshores existeix un $N \in \mathbb{N}$ tal que $I_n = I_N$ $\forall n \geq N$.

Definició 5.6. *Condició maximal. Tot conjunt d'ideals no buit admet un element maximal (i.e. un element que no està contingut en cap altre element del conjunt).*

Proposició 5.7. *Les següents condicions són equivalents en un domini d'integritat D:*

a) D és noetherià

b) D satisfà la condició de la cadena ascendent.

c) D satisfà la condició maximal.

Demostració.
a) $\Rightarrow$ *b)*. Considerem una cadena ascendent d'ideals com la (5.1). Sigui $I = \bigcup_{n=1}^{\infty} I_n$, per construcció I és un ideal, i a més finitament generat per ser un ideal d'un domini noetherià. Direm $I = \langle x_1, ..., x_m \rangle$, on cada x_i, amb $i = 1, ..., m$, pertany a algun I_{n_i}. Si fixem $N := \max_{1 \leq i \leq n} n_i$, aleshores tenim $I = I_N$ i ens implica que $I_n = I_N \ \forall n \geq N$.

b) $\Rightarrow$ *c)*. Suposem (b) considerant un conjunt no buit S d'ideals i suposem per contradicció que S no té element maximal. Sigui $I_0 \in S$, com I_0 no és maximal existeix $I_1 \in S$ de manera que $I_0 \subsetneq I_1$. Inductivament, anem trobant $I_n \in S$, que com no és maximal, podem triar un $I_{n+1} \in S$ de tal manera que $I_n \subsetneq I_{n+1}$. Però ara tenim una cadena ascendent que no s'acaba mai, la qual cosa ens contradiu (b).

c) $\Rightarrow$ *a)*. Sigui I qualsevol ideal de D. i sigui S el conjunt de tots els ideals finitament generats continguts en I. Tenim que $\{0\} \in S$, per tant S és un conjunt no buit. D'altra banda, com D satisfà la condició maximal, S té un element maximal J. Si $J \neq I$, agafem un $x \in I \backslash J$. Aleshores $\langle x, J \rangle$ és finitament generat i estrictament més gran que J, que és una contradicció ja que J és l'element maximal. En definitiva $J = I$ i I és finitament generat. □

5.2 Ideals primers i factorització única

Per començar volem generalitzar la idea de nombre primer de $\mathbb{Z}$ a ideals. Com hi ha dues definicions equivalents de nombre primer, una la relacionarem amb ideal maximal i l'altre amb ideal primer. La primera definició és que p és un nombre natural primer si els únics divisors són 1 i ell mateix; i la segona és la que hem vist a la Definició 4.4 d'element primer.

L'objectiu principal d'aquesta secció és demostrar que tot ideal de $\mathcal{O}_k$ és producte d'ideals primers. Per dur-ho necessitarem construir els ideals fraccionaris, que intuïtivament, son com ideals de $\mathcal{O}_k$ on estan permesos els denominadors. A més a més, aquests ideals tenen la propietat de formar un grup abelià multiplicatiu.

Definició 5.8. *Sigui A un anell commutatiu i sigui $\mathfrak{p}$ un ideal propi de A. Direm que $\mathfrak{p}$ és un ideal primer si, per qualsevol $\mathfrak{a}$ i $\mathfrak{b}$ ideals de A amb $\mathfrak{ab} \subseteq \mathfrak{p}$, aleshores $\mathfrak{a} \subseteq \mathfrak{p}$ o $\mathfrak{b} \subseteq \mathfrak{p}$.*

Definició 5.9. *Sigui A un anell commutatiu i sigui $\mathfrak{a}$ un ideal propi de A. Direm que $\mathfrak{p}$ és un ideal maximal si no existeix cap ideal $\mathfrak{b}$ de A tal que $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq A$.*

El lema que enunciarem a continuació, són uns resultats coneguts a estructures algebraiques que utilitzarem al llarg de la secció.

Lema 5.10. *Sigui A un anell i $\mathfrak{a}$ un ideal propi de A. Aleshores:*

a) $\mathfrak{a}$ és maximal, si i només si, $A/\mathfrak{a}$ és un cos.

b) $\mathfrak{a}$ és primer, si i només si, $A/\mathfrak{a}$ és un domini d'integritat.

c) Si A és un domini d'integritat finit, aleshores A és un cos.

d) Si $\mathfrak{a}$ és maximal, aleshores $\mathfrak{a}$ és primer.

Proposició 5.11. *Sigui $\mathcal{O}_k$ l'anell d'enters d'un cos de nombres K. Si $\mathfrak{p}$ és un ideal primer de $\mathcal{O}_k$ diferent de zero, aleshores $\mathcal{O}_k/\mathfrak{p}$ és finit.*

Demostració. Sigui $\mathfrak{p}$ un ideal primer diferent de zero de $\mathcal{O}_k$ i sigui $\alpha \in \mathfrak{p}$ un element diferent de zero. D'una banda la seva norma és

$$N = N(\alpha) = \alpha_1 \dots \alpha_n$$

on α_i són els K-conjugats de α. Com existeix un i tal que $\alpha_i = \alpha$, així doncs $N \in \mathfrak{p}$. A més a més, per la Proposició 3.23, observem que $N \in \mathbb{Z}$.

D'altra banda sabem que $\mathcal{O}_k$ admet una base d'enters, de manera que podem escriure $\mathcal{O}_k = \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n$. A més, com $N \in \mathfrak{p}$, de la definició d'ideal és evident que $N\omega_i \in \mathfrak{p}$ per tot $1 \leq i \leq n$. Aleshores per tot element $a = a_1\omega_1 + ...a_n\omega_n \in \mathcal{O}_k$ existeix $b = b_1\omega_1 + ...b_n\omega_n \in \mathcal{O}_k$ amb $0 \leq b_i \leq N$, de manera que $a \equiv b \ (\mathfrak{p})$. La qual cosa ens implica que hi ha un nombre finit d'elements. Així doncs $\mathcal{O}_k/\mathfrak{p}$ és finit. □

Teorema 5.12. *L'anell d'enters $\mathcal{O}_k$ d'un cos de nombres K té les propietats següents:*

a) És un domini, amb cos de fraccions K,

b) És un domini noetherià,

d) Tot ideal primer diferent de zero és maximal.

Demostració. a) És un domini ja que $\mathcal{O}_k$ és un subanell de K. D'una banda, pel Teorema 3.20, $\mathcal{O}_k$ sabem que admet una base d'enters i d'altra banda, per la Proposició 3.5 sabem que si $k \in K$, existeix un $a \in \mathbb{Z}$ tal que $ak \in \mathcal{O}_k$. Per tant K és el seu cos de fraccions.

b)Volem provar que tot ideal I de $\mathcal{O}_k$ és finitament generat. Al Teorema 3.20, hem vist que $(\mathcal{O}_k, +)$ és un grup abelià lliure de rang n, igual al grau d'extensió de K . Si I és un ideal de $\mathcal{O}_k$, $(I, +)$ és un subgrup de $\mathcal{O}_k$. Per tant aplicant el Teorema 2.8, $(I, +)$ és un grup abelià lliure de rang $s \leq n$. Sigui $\{x_1, ..., x_s\}$ una $\mathbb{Z}$-base de $(I, +)$, clarament $I = \langle x_1, ..., x_s \rangle$. En efecte I és finitament generat.

c)Sigui $\mathfrak{p}$ un ideal primer de $\mathcal{O}_k$, per la Proposició 5.11 $\mathcal{O}_k/\mathfrak{p}$ és un domini d'integritat finit. Per tant un cos pel Lema 5.10 c). Finalment aplicant el Lema 5.10 a) tenim que $\mathfrak{p}$ és maximal. □

Definició 5.13. *Sigui $\mathcal{O}_k$ l'anell d'enters del cos de nombres K. Anomenarem ideals fraccionaris de $\mathcal{O}_k$ als subconjunts $\mathfrak{a} \subseteq K$ de la forma $\mathfrak{a} = c^{-1}\mathfrak{b}$ on $\mathfrak{b}$ és un ideal de $\mathcal{O}_k$ i c és un element de $\mathcal{O}_k$ diferent de zero.*

Notem que els ideals fraccionaris són subconjunts de K, no de $\mathcal{O}_k$.

Definició 5.14. *Sigui $\mathfrak{a}$ un ideal fraccionari de $\mathcal{O}_k$. Direm que $\mathfrak{a} = c^{-1}\mathfrak{b}$ és un ideal fraccionari principal de $\mathcal{O}_k$ si $\mathfrak{b}$ és ideal principal de $\mathcal{O}_k$.*

Definició 5.15. *Siguin $\mathfrak{a}$, $\mathfrak{b}$ ideals de $\mathcal{O}_k$. Direm que $\mathfrak{a}$ divideix $\mathfrak{b}$ (i.e $\mathfrak{a}|\mathfrak{b}$) si existeix un ideal $\mathfrak{c}$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.*

A continuació demostrarem dos teoremes molt importants; primer veurem que el conjunt dels ideals fraccionaris diferents de zero de $\mathcal{O}_k$ formen un grup abelià multiplicatiu i seguidament provarem que tot ideal de $\mathcal{O}_k$ es pot escriure de manera única com a producte d'ideals primers. Demostrarem els dos resultats simultàniament, utilitzant una sèrie de lemes:

Lema 5.16. *Sigui $\mathfrak{a}$ un ideal de $\mathcal{O}_k$ diferent de zero. Aleshores existeixen $\mathfrak{p}_1, ..., \mathfrak{p}_n$ tal que*

$$\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \mathfrak{a} \tag{5.2}$$

.

Demostració. Suposem que no es compleix, aleshores podriem escollir $\mathfrak{a}$ el més gran possible que seguiria sense complir-se (5.2). Hem vist al Teorema 5.12 que $\mathcal{O}_k$ és noetherià, així doncs per la Proposicó 5.7 , podem agafar $\mathfrak{a}$ com l'element maximal que no satisfà (5.2). Clarament $\mathfrak{a}$ no és primer (ja que sinó podríem agafar $\mathfrak{p}_1 = \mathfrak{a}$), per tant existeixen $\mathfrak{b}, \mathfrak{c}$ de $\mathcal{O}_k$ amb $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$, tal que $\mathfrak{b} \nsubseteq \mathfrak{a}$ i $\mathfrak{c} \nsubseteq \mathfrak{a}$. Sigui

$$\mathfrak{a}_1 = \mathfrak{a} + \mathfrak{b}$$
$$\mathfrak{a}_2 = \mathfrak{a} + \mathfrak{c}.$$

Aleshores $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ amb $\mathfrak{a}_1 \supsetneq \mathfrak{a}$ i $\mathfrak{a}_2 \supsetneq \mathfrak{a}$. Com $\mathfrak{a}$ és l'ideal maximal que no satisfà (5.2), existeixen ideals primers $\mathfrak{p}_1, ..., \mathfrak{p}_s, \mathfrak{p}_{s+1}, ..., \mathfrak{p}_r$ tal que

$$\mathfrak{p}_1 \dots \mathfrak{p}_s \subseteq \mathfrak{a}_1$$
$$\mathfrak{p}_{s+1} \dots \mathfrak{p}_r \subseteq \mathfrak{a}_2.$$

De manera que $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$, fet que ens contradiu l'elecció de $\mathfrak{a}$. □

Lema 5.17. *Si $\mathfrak{a}$ és un ideal de $\mathcal{O}_k$, definim*

$$\mathfrak{a}^{-1} = \{\alpha \in K | \alpha\mathfrak{a} \subseteq \mathcal{O}_k\}.$$

Aleshores $\mathfrak{a}^{-1}$ és un ideal fraccionari.

Demostració. Sigui $c \in \mathfrak{a}$ i $\mathfrak{b} = c\mathfrak{a}^{-1}$, l'objectiu és veure que $\mathfrak{b}$ és un ideal de $\mathcal{O}_k$. Clarament $0 \in \mathfrak{b}$. Si $b, b' \in \mathfrak{b}$ necessitem que $b + b' \in \mathfrak{b}$. Tenim $b = c\beta$ i $b' = c\beta'$, amb $\beta, \beta' \in \mathfrak{a}^{-1}$, per tant, $b+b' = c(\beta+\beta')$, de manera que necessitem $\beta+\beta' \in \mathfrak{a}^{-1}$. Clarament $(\beta + \beta')\mathfrak{a} = \beta\mathfrak{a} + \beta'\mathfrak{a} \subseteq (\mathcal{O}_k + \mathcal{O}_k) = \mathcal{O}_k$, que és el que requereix.

Finalment hem de veure que si $b = c\beta \in \mathfrak{b}$, amb $\beta \in \mathfrak{a}^{-1}$, i $r \in \mathcal{O}_k$, aleshores $rb \in \mathfrak{b}$, la qual procedeix de veure que $r\beta \in \mathfrak{a}^{-1}$. Tornant al raonament d'abans, $(r\beta)\mathfrak{a} = r(\beta\mathfrak{a}) \subseteq r\mathcal{O}_k \subseteq \mathcal{O}_k$ ja que $r \in \mathcal{O}_k$. Doncs ja hem vist que $\mathfrak{b} = c\mathfrak{a}^{-1}$ és un ideal, així que $\mathfrak{a}^{-1} = c^{-1}\mathfrak{b}$ és l'ideal fraccionari que volíem.

□

A continuació farem alguna observació d'aquest Lema que ens serà de vital importància per seguir la demostració. Clarament $\mathcal{O}_k \subseteq \mathfrak{a}^{-1}$, així doncs $\mathfrak{a} = \mathfrak{a}\mathcal{O}_k \subseteq \mathfrak{a}\mathfrak{a}^{-1}$. D'altra banda, de la definició observem que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_k$, per tant l'ideal fraccionari $\mathfrak{a}\mathfrak{a}^{-1}$ és un ideal. Finalment, un altre fet que utilitzarem és que $\mathfrak{a} \subseteq \mathfrak{p}$ implica $\mathcal{O}_k \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$.

Lema 5.18. *Sigui $\mathfrak{a}$ un ideal propi de $\mathcal{O}_k$, aleshores $\mathfrak{a}^{-1} \supsetneq \mathcal{O}_k$*

Demostració. És trivial veure $\mathfrak{a}^{-1} \supseteq \mathcal{O}_k$ ja que $\mathcal{O}_k$ és subanell de K. Per aquest fet hem de veure que la inclusió és estricta. D'una banda, al ser $\mathcal{O}_k$ noetherià, tenim que tot ideal està contingut a un ideal maximal $\mathfrak{p}$. D'altra banda, per definició de l'invers tenim que si $\mathfrak{a} \subseteq \mathfrak{p}$, aleshores $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$ amb $\mathcal{O}_k \subseteq \mathfrak{p}^{-1}$. Per tant hem de trobar algun element de $\mathfrak{p}^{-1}$ que no sigui enter algebraic.

Començarem fixant un $\alpha \in \mathfrak{p}$ qualsevol, per tant $\langle\alpha\rangle \subseteq \mathfrak{p}$. Triem el r més petit tal que existeixen ideals primers $\mathfrak{p}_1, ..., \mathfrak{p}_r$ amb

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \langle\alpha\rangle \subseteq \mathfrak{p}$$

pel Lema 5.16. Com tot ideal maximal és primer, $\mathfrak{p}$ és primer, i de la seva definició deduïm que existeix algun $\mathfrak{p}_i$ tal que $\mathfrak{p}_i \subseteq \mathfrak{p}$. Reordenant, suposarem que aquest $\mathfrak{p}_i$ és $\mathfrak{p}_1$. Com tot ideal primer és maximal pel Teorema 5.12, i els ideals maximals no poden tenir cap ideal contingut un en l'altre, es compleix la següent igualtat $\mathfrak{p}_1 = \mathfrak{p}$. Ara bé, com hem agafat r mínima,

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \nsubseteq \langle\alpha\rangle.$$

Per tant existeix $\beta \in \mathfrak{p}_1 \dots \mathfrak{p}_r \backslash \langle\alpha\rangle$. Però tenim que $\beta\mathfrak{p} \subseteq \langle\alpha\rangle$, així doncs $\beta\alpha^{-1}\mathfrak{p} \subseteq \mathcal{O}_k$ i $\beta\alpha^{-1} \in \mathfrak{p}^{-1}$. D'altra banda, com $\beta \notin \alpha\mathcal{O}_k$, aleshores $\beta\alpha^{-1} \notin \mathcal{O}_k$, que implica $\mathfrak{p}^{-1} \neq \mathcal{O}_k$ com volíem demostrar. □

Lema 5.19. *Si $\mathfrak{a}$ és un ideal de $\mathcal{O}_k$ i $\mathfrak{a}S \subseteq \mathfrak{a}$ per qualsevol subconjunt $S \subseteq K$, aleshores $S \subseteq \mathcal{O}_k$.*

Demostració. El nostre objectiu és provar que si $\mathfrak{a}\theta \subseteq \mathfrak{a}$, amb $\theta \in S$, aleshores $\theta \in \mathcal{O}_k$. Com $\mathcal{O}_k$ és noetherià, $\mathfrak{a}$ és finitament generat; $\mathfrak{a} = \langle a_1, ..., a_m\rangle$. La hipòtesi

és $\mathfrak{a}\theta \subseteq \mathfrak{a}$ i com que ens implica

$$a_1\theta = b_{11}a_1 + ... + b_{1m}a_m$$
$$.....$$
$$a_m\theta = b_{m1}a_1 + ... + b_{mm}a_m$$

amb $b_{ij} \in \mathbb{Z}$. Atès que les equacions

$$(b_{11} - \theta)x_1 + ... + b_{1m}x_m = 0$$
$$.....$$
$$b_{m1}x_1 + ... + (b_{mm} - \theta)x_m = 0$$

tenen una solució $x_1 = a_1, ..., x_m = a_m$ diferent de zero, podem deduir que el determinant de la matriu amb els coeficients del sistema és zero. Per tant el determinant de la matriu és un polinomi mònic amb coeficients enters, que implica que $\theta \in \overline{\mathbb{Z}}$. Finalment com $\theta \in K$, aleshores per definició $\theta \in \mathcal{O}_k$. □

Lema 5.20. *Si $\mathfrak{p}$ és un ideal maximal de $\mathcal{O}_k$, aleshores $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_k$.*

Demostració. Com que $\mathfrak{p}^{-1}$ és un ideal fraccionari i $\mathfrak{p}$ és un ideal (per tant també un ideal fraccionari), el producte $\mathfrak{p}\mathfrak{p}^{-1}$ és un ideal fraccionari. Tanmateix, per la definició de $\mathfrak{p}^{-1}$, $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_k$, en efecte el producte és un ideal de $\mathcal{O}_k$. Com $\mathcal{O}_k \subseteq \mathfrak{p}^{-1}$, aleshores $\mathfrak{p} = \mathfrak{p}\mathcal{O}_k \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. A causa que $\mathfrak{p}$ és maximal, o bé $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ o $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_k$. El primer cas és impossible, ja que pel Lema 5.18 existeix $\theta \in \mathfrak{p}^{-1}$, tal que $\theta \notin \mathcal{O}_k$, i pel Lema 5.19 $\mathfrak{p}\theta \nsubseteq \mathfrak{p}$. Així doncs $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_k$. □

Lema 5.21. *Si $\mathfrak{a}$ és un ideal de $\mathcal{O}_k$ diferent de zero, aleshores $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_k$.*

Demostració. Suposem que no fos així. Per començar agafem el màxim ideal $\mathfrak{a}$ tal que $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathcal{O}_k$. Sigui $\mathfrak{p}$ l'ideal maximal que conté $\mathfrak{a}$, llavors pel Lema 5.17, $\mathcal{O}_k \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, així doncs

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_k.$$

En particular $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathcal{O}_k$ i per aquest fet $\mathfrak{a}\mathfrak{p}^{-1}$ és un ideal. Tot i això no pot ser que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, perquè pel Lema 5.18 existeix un $\theta \in \mathfrak{p}^{-1}\backslash\mathcal{O}_k$ i aquest fet ens contradiu el Lema 5.19. En efecte tenim $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$, i vist que $\mathfrak{a}$ és l'ideal maximal que no compleix la igualtat, $\mathfrak{a}\mathfrak{p}^{-1}$ satisfà

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathcal{O}_k.$$

Per la definició de $\mathfrak{a}^{-1}$ veiem

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$$

de manera que

$$\mathcal{O}_k = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_k.$$

□

Ara provarem un dels dos resultats importants.

Teorema 5.22. *El conjunt dels ideals fraccionaris diferents de zero de $\mathcal{O}_k$ formen un grup abelià multiplicatiu.*

Demostració. Primer de tot hem de veure que el producte d'ideals fraccionaris és un ideal fraccionari. Siguin $\mathfrak{a}_1, \mathfrak{a}_2$ dos ideals de $\mathcal{O}_k$ i $c_1, c_2 \in \mathcal{O}_k$, $\mathfrak{b}_1 = c_1^{-1}\mathfrak{a}_1$, llavors $\mathfrak{b}_2 = c_2^{-1}\mathfrak{a}_2$ són ideals fraccionaris i el producte $\mathfrak{b}_1\mathfrak{b}_2 = c_1^{-1}\mathfrak{a}_1 c_2^{-1}\mathfrak{a}_2 = (c_1c_2)^{-1}\mathfrak{a}_1\mathfrak{a}_2$ és un ideal fraccionari. Aquest producte és clarament associatiu i commutatiu. A més hem vist que l'anell d'enters $\mathcal{O}_k$ és la identitat. No obstant, la única cosa que ens falta veure és que podem definir l'invers de qualsevol ideal fraccionari. Ara bé, el Lema 5.21 ens dóna l'invers de qualsevol ideal, i cada ideal fraccionari és de la forma $\mathfrak{b} = c^{-1}\mathfrak{a}$ per qualsevol ideal $\mathfrak{a}$ de $\mathcal{O}_k$ i $c \in \mathcal{O}_k$. Així doncs l'invers $\mathfrak{b}^{-1}$ serà de la forma $c\mathfrak{a}^{-1}$. Per últim veiem que es compleix

$$\mathfrak{b}\mathfrak{b}^{-1} = c^{-1}\mathfrak{a}c\mathfrak{a}^{-1} = \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_k$$

com volíem demostrar. □

Lema 5.23. *Tot ideal $\mathfrak{a}$ és producte d'ideals primers.*

Demostració. Suposem que no passa. Sigui $\mathfrak{a}$ l'ideal maximal que no és producte d'ideals primers. Llavors $\mathfrak{a}$ no és primer, a més, al ser $\mathcal{O}_k$ noetherià, $\mathfrak{a}$ no és maximal i existeix un ideal maximal $\mathfrak{p}$, per tant primer, tal que $\mathfrak{a} \subseteq \mathfrak{p}$. De la mateixa manera que al Lema 5.21

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathcal{O}_k.$$

Per la condició de maximalitat de $\mathfrak{a}$,

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \dots \mathfrak{p}_r$$

on $\mathfrak{p}_2, ..., \mathfrak{p}_r$ són ideals primers. Així doncs

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r.$$

□

Finalment ha arribat el moment que podem provar la unicitat de la factorització d'ideals primers a $\mathcal{O}_k$.

Teorema 5.24. *Tot ideal de $\mathcal{O}_k$ diferent de zero es pot escriure com a producte d'ideals primers de manera única, llevat del ordre dels factors.*

Demostració. El Lema anterior ens diu que tot ideal descompon en producte d'ideals primers, és a dir, només ens falta veure que la descomposició és única.

Sigui r el nombre més petit tal que existeix un ideal $\mathfrak{a}$ amb dues descomposicions diferents

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s \tag{5.3}$$

en ideals primers. Com $\mathfrak{p}_1 = \mathfrak{q}_1 \dots \mathfrak{q}_s\mathfrak{p}_2^{-1} \dots \mathfrak{p}_r^{-1}$, aleshores $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq \mathfrak{p}_1$. Ara bé, al ser $\mathfrak{p}_1$ un ideal primer, existeix $\mathfrak{q}_i$ de manera que $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Però ambdós són ideals maximals, així que $\mathfrak{q}_i = \mathfrak{p}_1$. Finalment, multiplicant l'equació (5.3) per $\mathfrak{p}_1^{-1}$ es cancel·len els termes $\mathfrak{p}_1$ i $\mathfrak{q}_i$, que per tant ens contradiu la nostre elecció de r. □

Proposició 5.25. *Siguin $\mathfrak{a}$ i $\mathfrak{b}$ dos ideals diferents de $\mathcal{O}_k$, $\mathfrak{a}|\mathfrak{b}$ si i només si $\mathfrak{b} \subseteq \mathfrak{a}$.*

Demostració. Si $\mathfrak{a}|\mathfrak{b}$, per definició tenim que existeix un ideal $\mathfrak{c}$ de manera que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, així que, per la definició de producte d'ideals, $\mathfrak{b} \subseteq \mathfrak{a}$. D'altra banda, si $\mathfrak{b} \subseteq \mathfrak{a}$. podem definir l'ideal fraccionari $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$. Així doncs pel Lema 5.21 tenim

$$\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_k$$

i, per tant $\mathfrak{c}$ és un ideal de $\mathcal{O}_k$ i podem escriure $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, que implica que $\mathfrak{a}|\mathfrak{b}$. □

5.3 Norma d'un ideal

A la Proposició 5.11 hem vist que $\mathcal{O}_k/\mathfrak{p}$ és finit si $\mathfrak{p}$ és un ideal primer. Aquest fet s'estén fàcilment amb una potència d'un ideal primer, és a dir, de forma anàloga podríem demostrar que $\mathcal{O}_k/\mathfrak{p}^n$ és finit. A l'anterior secció hem vist que tot ideal $\mathfrak{a}$ descompon de manera única en ideals primers, així doncs aplicant el Teorema Xinès del Residu observem que $\mathcal{O}_k/\mathfrak{a}$ és finit.

Definició 5.26. *Sigui $\mathfrak{a}$ un ideal de $\mathcal{O}_k$. Definim la norma de $\mathfrak{a}$ com*

$$N(\mathfrak{a}) = |\mathcal{O}_k/\mathfrak{a}|.$$

Teorema 5.27. *Tot ideal $\mathfrak{a}$ de $\mathcal{O}_k$ diferent de zero compleix les següents condicions:*

(a) $\mathfrak{a}$ admet una $\mathbb{Z}$-base $\{\alpha_1, ..., \alpha_n\}$ on n és el grau de K.

(b) Es compleix

$$N(\mathfrak{a}) = \left|\frac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta}\right|^{\frac{1}{2}}$$

on Δ és el discriminant de K.

Demostració. (a) D'una banda hem vist al Teorema 3.20 que $(\mathcal{O}_k, +)$ és un grup abelià lliure de rang n. D'altra banda, com $\mathcal{O}_k/\mathfrak{a}$ és finit, pel Teorema 2.10, $(\mathfrak{a}, +)$ és un grup abelià lliure de rang n. Per tant admet una $\mathbb{Z}$-base de la forma $\{\alpha_1, ..., \alpha_n\}$.

(b) Sigui $\{\omega_1, ..., \omega_n\}$ una $\mathbb{Z}$-base de $\mathcal{O}_k$, suposem que $\alpha_i = \sum_{j=1}^{n} c_{ij}\omega_j$, amb $1 \leq i \leq n$ i $c_{ij} \in \mathbb{Z}$. Primerament, pel Teorema 2.10, tenim

$$N(\mathfrak{a}) = |\mathcal{O}_k/\mathfrak{a}| = |det(c_{ij}|.$$

Però per la Proposició 3.16 tenim

$$\Delta[\alpha_1, ..., \alpha_n] = (\det c_{ij})^2 \Delta[\omega_1, ..., \omega_n] = N(\mathfrak{a})^2 \Delta$$

Aleshores

$$N(\mathfrak{a}) = \left|\frac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta}\right|^{\frac{1}{2}}$$

ja que el discriminant és diferent de zero i la $N(\mathfrak{a})$ és positiva. □

Corol·lari 5.28. *Si $\mathfrak{a} = \langle a \rangle$ és un ideal principal de $\mathcal{O}_k$, aleshores $N(\mathfrak{a}) = |N(a)|$.*

Demostració. Si $\{\omega_1, ..., \omega_n\}$ és una $\mathbb{Z}$-base de $\mathcal{O}_k$, clarament també $\mathbb{Q}$-base de K, aleshores $\{a\omega_1, ..., a\omega_n\}$ és una $\mathbb{Z}$-base de $\mathfrak{a}$. Per tant aplicant el Teorema 5.27, la definició de discriminant i la definició de norma d'un element

$$N(\mathfrak{a}) = \left| \frac{\Delta[a\omega_1, ..., a\omega_n]}{\Delta[\omega_1, ..., \omega_n]} \right|^{\frac{1}{2}} = \left| \frac{\sigma_1(a)^2 \dots \sigma_n(a)^2 \Delta[\omega_1, ..., \omega_n]}{\Delta[\omega_1, ..., \omega_n]} \right|^{\frac{1}{2}} = |N(a)|.$$

□

Lema 5.29. *Sigui $\mathfrak{a}$ i $\mathfrak{p}$ ideals de $\mathcal{O}_k$ diferent de zero, tal que $\mathfrak{p}$ és un ideal primer, aleshores*

$$|\mathcal{O}_k/\mathfrak{p}| = |\mathfrak{a}/\mathfrak{a}\mathfrak{p}|.$$

Demostració. Per començar suposem que existeix un ideal $\mathfrak{b}$ de $\mathcal{O}_k$ tal que $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a}\mathfrak{p}$. Multiplicant-ho tot per $\mathfrak{a}^{-1}$ obtenim $\mathcal{O}_k \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{p}$. Ara bé, com $\mathfrak{p}$ és un ideal primer, $\mathfrak{p}$ és maximal, per tant $\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_k$ o $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$. Això ens implica que $\mathfrak{b} = \mathfrak{a}$ o $\mathfrak{b} = \mathfrak{a}\mathfrak{p}$. Això vol dir que per qualsevol element $a \in \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ es compleix que

$$\mathfrak{a}\mathfrak{p} + \langle a \rangle = \mathfrak{a}. \tag{5.4}$$

Una vegada vist això fixem un $\alpha \in \mathfrak{a}$, de manera que $\alpha \notin \mathfrak{a}\mathfrak{p}$. Aleshores com $\langle \alpha \rangle \subseteq \mathfrak{a}$ i $\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}$, però, $\langle \alpha \rangle$ és estrictament més gran que $\mathfrak{a}\mathfrak{p}$, i per tant tenim que $\langle \alpha \rangle = \mathfrak{a}$. Ara definim l'aplicació

$$\begin{aligned} \phi : \mathcal{O}_k &\longrightarrow \mathfrak{a}/\mathfrak{a}\mathfrak{p} \\ x &\longmapsto \alpha x + \mathfrak{a}\mathfrak{p} \end{aligned}$$

Veiem que ϕ és un morfisme de $\mathcal{O}_k$-mòduls, en concret un morfisme exhaustiu per l'equació (5.4). A més el nucli satisfà que $\mathfrak{p} \subseteq \ker \phi$, ja que si $x \in \mathfrak{p}$, aleshores $\alpha x \in \mathfrak{a}\mathfrak{p}$. Però $1 \notin \ker \phi$, donat que $\phi(1) = \alpha + \mathfrak{a}\mathfrak{p}$ i hem triat un $\alpha \notin \mathfrak{a}\mathfrak{p}$. Com $\mathfrak{p}$ és maximal, veiem que $\ker \phi = \mathfrak{p}$. Per tant, pel primer teorema d'isomorfia de mòduls obtenim $\mathcal{O}_k/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{p}$, la qual cosa ens demostra el Lema.

□

Teorema 5.30. *Si $\mathfrak{a}$ i $\mathfrak{b}$ són dos ideals de $\mathcal{O}_k$ diferent de zero, aleshores*

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

Demostració. Primer de tot veiem que per la factorització única en ideals primers és suficient provar

$$N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{p}).$$

on $\mathfrak{p}$ és ideal primer.

Considerem ara el morfisme

$$\begin{aligned}\phi : \mathcal{O}_k/\mathfrak{ap} &\longrightarrow \mathcal{O}_k/\mathfrak{a} \\ \alpha + \mathfrak{ap} &\longmapsto \alpha + \mathfrak{a}\end{aligned}$$

que és clarament exhaustiu i el seu nucli és $\mathfrak{a}/\mathfrak{ap} = \{\alpha + \mathfrak{ap} | \alpha \in \mathfrak{a}\}$. Aleshores, pel primer teorema d'isomorfia

$$\left|\frac{\mathcal{O}_k/\mathfrak{ap}}{\mathfrak{a}/\mathfrak{ap}}\right| = |\mathcal{O}_k/\mathfrak{a}|.$$

Així doncs

$$|\mathcal{O}_k/\mathfrak{ap}| = |\mathcal{O}_k/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|$$

i pel Lema 5.29 observem

$$|\mathcal{O}_k/\mathfrak{ap}| = |\mathcal{O}_k/\mathfrak{a}||\mathcal{O}_k/\mathfrak{p}|.$$

Finalment tenim, per la definició de norma d'un ideal, $N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p})$. □

Proposició 5.31. *Sigui $\mathfrak{a}$ un ideal de $\mathcal{O}_k$ diferent de zero, si $N(\mathfrak{a})$ és un nombre primer, aleshores $\mathfrak{a}$ és ideal primer.*

Demostració. Suposem que $\mathfrak{a}$ no és un ideal primer. Aleshores tenim $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i$, amb $r > 2$ i $\mathfrak{p}_i$ ideals primers. Posant normes tenim

$$N(\mathfrak{a}) = N\left(\prod_{i=1}^{r} \mathfrak{p}_i\right) = \prod_{i=1}^{r} N(\mathfrak{p}_i)$$

on la última igualtat és conseqüència de la multiplicitat de la norma. Per tant $N(\mathfrak{a})$ no és primer, ja que és el producte de diferents nombres. □

6 Grup de classe i grup de les unitats

En aquest capítol enunciarem dos teoremes fonamentals de la teoria algebraica de nombres; la finitud del nombre de classe i el teorema de les unitats de Dirichlet.

6.1 Teorema de finitud del grup de classes

Anteriorment hem vist que en un domini d'ideals principals és un domini de factorització única en elements irreductibles. El nostre problema és que, en general, a l'anell d'enters $\mathcal{O}_k$ d'un cos algebraic K, la descomposició única en factors irreductibles falla. A més acabem de veure que els ideals de qualsevol anell d'enters $\mathcal{O}_k$ admeten sempre descomposició única en ideals primers. A conseqüència d'això veiem que si la factorització única falla, aleshores no tots els ideals són principals. Per tant, tenint en compte aquest resultat, el nostre objectiu és donar una mesura quantitativa de quan pot fallar la descomposició única. Usant el fet que els ideals fraccionaris formen un grup, construirem el grup que mesuri quan falla la descomposició.

Sigui K un cos de nombre amb anell d'enters $\mathcal{O}_k$. Anomenarem

$$\mathcal{F}_k = \{\, els\ ideals\ fraccionaris\ de\ \mathcal{O}_k\}$$

i

$$\mathcal{PF}_k = \{\, els\ ideals\ fraccionaris\ principals\ de\ \mathcal{O}_k\}$$

com $\mathcal{F}_k$ és un grup, $\mathcal{PF}_k$ és un subgrup normal d'aquest, ja que tot subgrup d'un grup abelià és normal.

Definició 6.1. *Definim el grup de classe de K com el grup quocient*

$$\mathbf{C}_k = \frac{\mathcal{F}_k}{\mathcal{PF}_k}. \tag{6.1}$$

Definició 6.2. *Anomenarem nombre de classe al cardinal de $\mathbf{C}_k$.*

$$h_k = |\mathbf{C}_k|.$$

Direm que dos ideals fraccionaris $\mathfrak{a}$ i $\mathfrak{b}$ són equivalents si $\mathfrak{ab}^{-1} \in \mathcal{FP}_k$. En aquest cas escriurem

$$\mathfrak{a} \sim \mathfrak{b}$$

i utilitzarem $[\mathfrak{a}]$ per designar la classe de $\mathfrak{a}$.

Corol·lari 6.3. *Tota classe d'equivalència conté un ideal de $\mathcal{O}_k$.*

Demostració. Si $\mathfrak{a}$ un ideal fraccionari, és de la forma $\mathfrak{a} = c^{-1}\mathfrak{b}$, on $c \in \mathcal{O}_k$ i $\mathfrak{b} \subseteq \mathcal{O}_k$ és un ideal. Com $\mathfrak{b} = c\mathfrak{a} = \langle c\rangle\mathfrak{a}$, per tant $\mathfrak{a}^{-1}\mathfrak{b} = \langle c\rangle \in \mathcal{FP}_k$, i en conseqüència $\mathfrak{a} \sim \mathfrak{b}$. □

Teorema 6.4. *Si $h_k = 1$, aleshores $\mathcal{O}_k$ admet factorització única*

Demostració. Si el nombre de classe és 1, aleshores $\mathbf{C}_k$ és trivial i $\mathcal{F}_k = \mathcal{PF}_k$. Per tant $\mathcal{O}_k$ és domini d'ideals principals i conseqüentment admet factorització única en factors irreductibles. □

A continuació donarem un teorema que ens diu que el cardinal de $\mathbf{C}_k$ és finit.

Teorema. *El grup de classe d'un cos de nombres és un grup abelià finit. El nombre de classe h_k és finit*

Proposició 6.5. *Sigui K un cos de nombres amb nombre de classe h_k i sigui $\mathfrak{a}$ un ideal de l'anell d'enters $\mathcal{O}_k$, aleshores:*

(a) $\mathfrak{a}^{h_k}$ és un ideal principal,

(b) Si q és coprimer amb h_k i $\mathfrak{a}^q$ és principal, aleshores $\mathfrak{a}$ és principal.

Demostració. (a) Com $h_k = |\mathbf{C}_k|$, aleshores $[\mathfrak{a}]^{h_k} = [\mathcal{O}_k]$ per tot $[\mathfrak{a}] \in \mathbf{C}_k$, ja que $[\mathcal{O}_k]$ és l'element identitat de $\mathbf{C}_k$. D'altra banda $[\mathfrak{a}^{h_k}] = [\mathfrak{a}]^{h_k}$ pel morfisme de pas al quocient. Per tant $\mathfrak{a}^{h_k} \sim \mathcal{O}_k$ i d'aquesta manera $\mathfrak{a}^{h_k}$ és principal, ja que $[\mathcal{O}_k]$ consisteix en tots els ideals principals fraccionaris.

(b) Com h_k i q són coprimers, per la Identitat de Bézout, existeixen $a, b \in \mathbb{Z}$ tal que $aq + bh_k = 1$. Com $[\mathfrak{a}^q] = [\mathfrak{a}]^q = [\mathcal{O}_k]$, aleshores

$$[\mathfrak{a}] = [\mathfrak{a}]^{aq+bh_k} = ([\mathfrak{a}]^q)^a([\mathfrak{a}]^{h_k})^b = [\mathcal{O}_k]^a[\mathcal{O}_k]^b = [\mathcal{O}_k]$$

□

6.2 Teorema de les unitats de Dirichlet

En aquesta secció enunciarem un teorema que determina l'estructura de les unitats de l'anell d'enters $\mathcal{O}_k$ d'un cos de nombres K. Concretament estipula que el grup de les unitats és el producte d'un grup cíclic finit i un grup abelià finitament generat. Abans de formalitzar-lo necessitarem alguna definició prèvia.

Sigui K un cos de nombres amb grau d'extensió n. Recordem pel Teorema 3.10 que hi ha exactament n monomorfismes diferents de K a $\mathbb{C}$.

Definició 6.6. *Sigui $\sigma : K \longrightarrow \mathbb{C}$ un monomorfisme tal que $\sigma(K) \subset \mathbb{R}$, aleshores direm que σ és real. Altrament direm que σ és complex. En aquest cas, definirem el seu conjugat com $\overline{\sigma}(k) = \overline{\sigma(k)}$, que és també un monomorfisme.*

Si designem r_1 el nombre de monomorfismes reals i r_2 la parella de monomorfismes conjugats complexos, es compleix $n = r_1 + 2r_2$.

Teorema. (Dirichlet) *El grup d'unitats $\mathcal{O}_k^\times$ és un grup abelià finitament generat. Més concretament*

$$\mathcal{O}_k^\times \cong \mu(K) \times \mathbb{Z}^r,$$

on $\mu(K)$ és el grup de le arrels de la unitat i $r = r_1 + r_2 - 1$. Equivalentment, existeixen unitats $u_1, ..., u_r$ tal que

$$u = \zeta u_1^{v_1} \dots u_r^{v_r}$$

on $\zeta \in \mu(K)$ i $v_i \in \mathbb{Z}$.

A les unitats $u_1, ..., u_r$ les anomenarem unitats fonamentals.

Les demostracions d'aquests dos teoremes fonamentals de la teoria algebraica de nombres es poden trobar al llibre [2] a les pàgines 158-168.

7 Cossos ciclotòmics

En aquest capítol estudiarem les propietats més importants dels anells d'enters dels cossos ciclotòmics. Començarem determinant quin és aquest anell d'enters i posteriorment donarem algunes propietats de les seves unitats.

7.1 Anell d'enters ciclotòmic

Les arrels n-èsimes de la unitat són les arrels complexes de l'equació $x^n = 1$, és a dir, els nombres $e^{\frac{2\pi i}{n}k}$ amb $k = 1, ..., n$. El conjunt d'aquestes formen un grup cíclic multiplicatiu d'ordre n. Una arrel n-èsima de la unitat ζ és una arrel primitiva n-èsima de la unitat si és generador del grup cíclic de les arrels n-èsimes de la unitat. Un cos ciclotòmic és un cos algebraic de nombres de la forma $\mathbb{Q}(\zeta)$, on ζ és una arrel n-èsima primitiva de la unitat.

A continuació considerem els casos n=p, un nombre primer. (Ja que per la demostració només necessitem p primers). Si p=2, aleshores ζ és -1 i per tant és suficient considerar p primers senars. El polinomi mínim de $\zeta_p = e^{\frac{2\pi i}{p}}$ sobre $\mathbb{Q}$ és

$$\Phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1$$

l'anomenem polinomi p-èsim ciclotòmic. És fàcil veure que el polinomi ciclotòmic $\Phi(x)$ és irreductible, per tant tenim que el grau de l'extensió $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ és $p-1$. Tenim que les potències de $\zeta, \zeta^2, \zeta^3, ..., \zeta^{p-1}$ són arrels p-èsimes primitives de la unitat per tant són arrels de $\Phi(x)$. Podem escriure el polinomi ciclotòmic de la següent manera

$$\Phi(x) = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1}) \tag{7.1}$$

així els conjugats de ζ són $\zeta, \zeta^2, \zeta^3, ..., \zeta^{p-1}$. És a dir, els monomorfismes de $\mathbb{Q}(\zeta)$ a $\mathbb{C}$ són de la forma

$$\sigma_i(\zeta) = \zeta^i, \quad i = 1, ..., p - 1.$$

Com el grau del polinomi minim $\Phi(x)$ és $p - 1$, una base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ és $\{1, \zeta, ..., \zeta^{p-2}\}$, aleshores per qualsevol element α de la forma

$$\alpha = a_0 + a_1\zeta + ... + a_{p-2}\zeta p - 2, \quad a_i \in \mathbb{Q}$$

tenim que

$$\sigma_i(\alpha) = a_0 + a_1\zeta^i + ... + a_{p-2}\zeta^{i(p-2)}, \quad a_i \in \mathbb{Q}.$$

Pels següents resultats és important determinar la norma i la traça dels elements de $\mathbb{Q}(\zeta)$. Per la definició de norma tenim

$$N(\alpha) = \prod_{i=1}^{p-1} \sigma_i(\alpha)$$

en particular tenim $N(\zeta) = \zeta \cdot \zeta^2 \cdots \zeta^{p-1}$. Ara, com ζ i ζ^i són conjugades, fixant $x = 0$ a (7.1) ens queda

$$1 = (-1)^{p-1} N(\zeta)$$

pern tant al ser p senar i $N(\zeta) = N(\zeta^i)$, aleshores

$$N(\zeta^i) = 1, \quad i = 1, .., p-1.$$

Determinar en general la norma dels elements de $\mathbb{Q}(\zeta)$ és complicat, però un cas que utilitzarem molt és l'element $1 - \zeta \in \mathbb{Z}[\zeta]$, per tant calcularem la norma d'aquest

$$N(1-\zeta) = \prod_{i=1}^{p-1} (1 - \zeta^i) = p \tag{7.2}$$

on la última igualtat s'obté de posar $x = 1$ a (7.1). Per la definició de traça tenim

$$T(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha)$$

Per tant, al ser ζ i ζ^i conjugades,

$$T(\zeta^i) = T(\zeta) = \zeta + \zeta^i + ... + \zeta^{p-1}$$

i usant el factor que $\Phi(\zeta) = 1 + \zeta + \zeta^i + ... + \zeta^{p-1} = 0$ és trivial veure

$$T(\zeta^i) = -1 \quad i = 1, ..., p-1.$$

D'altra banda, com els monomorfismes de $\mathbb{Q}$ a $\mathbb{C}$ deixen fixes els elements de $\mathbb{Q}$, tenim que per tot $a \in \mathbb{Q}$ es compleix

$$\begin{aligned} N(a) &= a^{p-1} \\ T(a) &= (p-1)a. \end{aligned}$$

Per últim podem donar la fórmula de la traça de qualsevol element de $\mathbb{Q}(\zeta)$

$$\begin{aligned} T\left(\sum_{i=0}^{p-2} a_i \zeta^i\right) &= \sum_{i=0}^{p-2} T(a_i \zeta^i) = T(a_0) + \sum_{i=1}^{p-2} a_i T(\zeta^i) = \\ &= (p-1)a_0 - \sum_{i=1}^{p-2} a_i = p a_0 - \sum_{i=0}^{p-2} a_i \end{aligned} \tag{7.3}$$

Teorema 7.1. *Sigui K=$\mathbb{Q}(\zeta)$. L'anell d'enters $\mathcal{O}_k$ és $\mathbb{Z}[\zeta]$.*

Demostració. És trivial que $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_k$.

Per demostrar l'altra implicació suposarem que $\alpha \in \mathcal{O}_k$. Al ser $\{1, \zeta, ..., \zeta^{p-2}\}$ una $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$, podem escriure $\alpha = a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}$, $a_i \in \mathbb{Q}$. Aleshores hem de demostrar que els nombres racionals a_i, amb $i = 0, ..., p-2$, són enters.

Per $k = 0, ..., p-2$ l'element $\alpha\zeta^{-k} - \alpha\zeta \in \mathcal{O}_k$ per tant la seva traça és entera per la Proposició 3.23. A més a més podem explicitar la traça d'aquest element de la següent manera

$$T(\alpha\zeta^{-k} - \alpha\zeta) = T(a_0\zeta^{-k} + ... + a_k + ... + a_{p-2}\zeta^{p-k-2} - a_0\zeta - ... - a_{p-2}\zeta p - 1) =$$
$$= (p-1)a_k + a_k - (a_0 + ... + a_{k-1} + a_{k+1} + ... + a_{p-2}) - (-a_0 - ... - a_{k-1} - a_{k+1} - ... - a_{p-2}) =$$
$$= pa_k.$$

I obtenim que $b_k := pa_k$ és un enter.

D'altra banda fent el canvi $\lambda = 1 - \zeta$ tenim

$$p\alpha = b_0 + b_1\zeta + ... + b_{p-2}\zeta^{p-2} = c_0 + c_1\lambda + ... + c_{p-2}\lambda^{p-2} \tag{7.4}$$

on substituint $\zeta = 1 - \lambda$ i desenvolupant obtenim

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} b_j$$

amb $c_i \in \mathbb{Z}$, per $i = 0, ..., p-2$. Per simetria, com $\lambda = 1 - \zeta$ tenim

$$b_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} c_j.$$

Tot seguit demostrarem per inducció completa que cada c_i és divisible per p.

En primer lloc ens adonem que $c_0 = b_0 + b_1 + ... + b_{p-2} = pa_0 + ... + pa_{p-2} = p(-T(\alpha) + b_0)$, on la $T(\alpha)$ ve donada a l'equació (7.3), per tant $p|c_0$ i tenim que el cas inicial és cert.

A continuació suposarem que la hipòtesi és certa per tot c_i amb $i \leq k-1$, on $k = 1, ..., p-2$. Per l'equació (7.2) tenim:

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i) = (1-\zeta)^{p-1} \prod_{i=1}^{p-1} (1 + \zeta + ... + \zeta^{i-1}) = \lambda^{p-1}\kappa \tag{7.5}$$

on $\kappa \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}_k$. Considerant (7.5) com una congruència mòdul l'ideal $\langle \lambda^{k+1} \rangle$ de $\mathcal{O}_k$ tenim:

$$p \equiv 0 \pmod{\langle \lambda^{k+1} \rangle}.$$

Ara bé, considerant l'equació (7.4) mòdul $\langle \lambda^{k+1} \rangle$, els termes $c_0, .., c_{k-1}\lambda^{k-1}$ s'anul·len per la hipòtesi d'inducció; i els termes $c_{k+1}\lambda^{k+1}, .., c_{p-2}\lambda^{p-2}$ s'anul·len perquè són múltiples de λ^{k+1}. Aleshores l'equació (7.4) ens queda

$$c_k\lambda^k \equiv 0 \pmod{\langle \lambda^{k+1} \rangle}.$$

Que és equivalent a

$$c_k\lambda^k = \mu\lambda^{k+1}$$

per alguna $\mu \in \mathcal{O}_k$. D'aquesta manera dividint per λ^k obtenim

$$c_k = \mu\lambda.$$

Finalment prenent normes ens adonem

$$c_k^{p-1} = N(c_k) = N(\mu\lambda) = N(\mu)N(\lambda) = N(\mu)p,$$

ja que N(λ)=p per (7.2).

Això ens implica que $p|c_k^{p-1}$, la qual cosa comporta que $p|c_k$. De fet, per inducció tenim que $p|c_k$ per tot $k = 0, ..., p-2$. Com hem vist que b_k és múltiple de c_k per tot k, aleshores $p|b_k \forall k$. Per tant $a_k \in Z\ \forall k$ i el teorema està demostrat. □

Escrivim $\lambda = 1 - \zeta$ com al teorema anterior, i considerem l'ideal $\mathcal{I} = \langle\lambda\rangle \subseteq \mathbb{Z}[\zeta]$. A continuació volem estudiar algunes propietats de $\mathcal{I}$.

Lema 7.2. *L'ideal $\mathcal{I}$ de $\mathbb{Z}[\zeta]$ satisfà les següents condicions:*

(a) $\mathcal{I}^{p-1} = \langle p\rangle$

(b) $N(\mathcal{I}) = p$

Demostració. a) Primer de tot hem de veure que els K-conjugats de λ són associats a $\mathbb{Z}[\zeta]$. És a dir, que $1-\zeta$ i $1-\zeta^i$, amb $i = 1, ..., p-1$ són associats. Clarament $1-\zeta|1-\zeta^i$. D'altra banda utilitzem el fet que p és primer per veure que existeix un j tal que $ij \equiv 1 \pmod p$. Com $1-\zeta = 1-\zeta^{ij}$, aleshores $1-\zeta^i|1-\zeta^{ij} = 1-\zeta$.

Finalment per l'equació (7.2) observem

$$\langle p\rangle = \prod_{i=1}^{p-1}\langle 1-\zeta^i\rangle$$

i com hem vist que són associats $\langle 1-\zeta^i\rangle = \langle 1-\zeta\rangle = \mathcal{I}$. Així doncs $\langle p\rangle = \mathcal{I}^{p-1}$.

(b) Pel que fa al segon apartat, prenent normes a l'apartat (a) observem $N(\mathcal{I}^{p-1}) = N(\langle p\rangle) = p^{p-1}$. Com la $N(\mathcal{I})$ és positiva i $\mathcal{I}$ factoritza de manera única en ideals primers, aleshores $N(\mathcal{I}) = \mathfrak{p}$. □

Per la definició de norma d'un ideal, observem que $|\mathbb{Z}[\zeta]/\mathcal{I}| = p$. Com a conseqüència de l'apartat (b) el morfisme $\mathbb{Z}[\zeta] \longleftarrow \mathbb{Z}[\zeta]/\mathcal{I}$ ens mostra que tot element de $\mathbb{Z}[\zeta]$ és congruent amb $0, 1, ..., p-1$ mòdul $\mathcal{I}$.

7.2 Unitats de $\mathbb{Z}[\zeta]$

Un dels punts més importants és determinar les característiques de les unitats de $\mathbb{Z}[\zeta]$. Al teorema de les unitats de Dirichlet hem vist l'estructura del grup d'unitats $\mathcal{O}_k^\times$. Clarament les arrels de la unitat són enters algebraics i unitats, així doncs és suficient presentar quines arrels de la unitat hi ha a $K = \mathbb{Q}(\zeta)$, la qual la farem amb el següent teorema.

Teorema 7.3. *Les úniques arrels de la unitat a* $\mathbb{Q}(\zeta)$ *són* $\pm\zeta^m$*, on* $m \in \mathbb{Z}$*.*

La demostració d'aquest teorema es pot trobar al llibre [5] a les pàgines 189-190.

Lema 7.4. *Per tot* $\alpha \in \mathbb{Z}[\zeta]$ *existeix un* $a \in \digamma$ *tal que* $\alpha^p \equiv a \pmod{\mathcal{I}^p}$*.*

Demostració. A conseqüència del Lema 7.2 podem observar que tot $\alpha \in \mathbb{Z}[\zeta]$ és congruent amb $0, 1, ..., p-1$ mòdul $\mathcal{I}$. Sigui b aquest enter tenim $\alpha \equiv b \pmod{\mathcal{I}}$. D'altra banda podem factoritzar

$$\alpha^p - b^p = \prod_{i=0}^{p-1}(\alpha - \zeta^i b).$$

Com que $\zeta \equiv 1 \pmod{\mathcal{I}}$ i $1-\zeta$ i $1-\zeta^i$ són associats, cada factor de la dreta de l'equació és congruent amb $\alpha - b \equiv 0 \pmod{\mathcal{I}}$. Per tant multiplicant-se $\alpha^p - b^p \equiv 0 \pmod{\mathcal{I}^p}$. □

Lema 7.5. *Sigui* $p(t) \in \mathbb{Z}$ *un polinomi mònic, tal que tots els seus zeros de* $\mathbb{C}$ *pertanyen a la frontera del cercle unitat, aleshores tots els zeros són arrels de la unitat.*

Demostració. Sigui $\alpha_1, ..., \alpha_k$ zeros de $p(t)$. Aleshores per tot $l \in \mathbb{Z}, l > 0$, el polinomi

$$p_l(t) = (t - \alpha_1^l) \dots (t - \alpha_k^l) \in \mathbb{Z}[t]$$

per l'argument dels polinomis simètrics. Si desenvolupem

$$p_l(t) = t^k + a_{k-1}t^{k-1} + ... + a_0,$$

aleshores, per les Formules de Viète i atès que $|\alpha_i^l| = 1$ per tot $i = 1, ..., k$, els coeficients satisfan la següent desigualtat

$$|a_i| \leq \binom{k}{i}.$$

Per tant, com hem acotat els coeficients, només hi ha un nombre finit de polinomis amb coeficients enters. Així doncs $p_l(t) = p_m(t)$ per algun $m \neq l$. D'aquesta manera existeix una permutació $\pi \in S_k$ tal que

$$\alpha_j^l = \alpha_{\pi(j)}^m$$

per $j = 1, ..., k$. Aplicant aquesta construcció de manera iterativa obtenim

$$\alpha_j^{l^r} = \alpha_{\pi^r(j)}^{m^r}.$$

D'altra banda l'ordre de π divideix $k!$ i per tant $\alpha_j^{l^{k!}} = \alpha_j^{m^{k!}}$. En definitiva

$$\alpha_j^{(l^{k!} - m^{k!})} = 1$$

i com $l^{k!} \neq m^{k!}$, ens implica que α_j és arrel de la unitat. □

Lema 7.6. *Tota unitat de $\mathbb{Z}[\zeta]$ és de la forma $r\zeta^k$, on $r \in \mathbb{R}$ i $k \in \mathbb{Z}$.*

Demostració. Sigui u una unitat de $\mathbb{Z}[\zeta]$. Aleshores existeix un polinomi $g(x) \in \mathbb{Z}[\zeta]$ tal que $u = g(\zeta)$. Per $j = 1, ..., p-1$ tenim que

$$u_j = g(\zeta^j)$$

són els conjugats de u. Alhora, per la Proposició 3.24, es compleix $1 = \pm N(u) = \pm u_1 \dots u_{p-1}$ de manera que cada u_j també és una unitat de $\mathbb{Z}[\zeta]$. A més a més, si la barra determina la conjugació complexa,

$$u_{p-j} = g(\zeta^{p-j}) = g(\zeta - j) = g(\overline{\zeta^j}) = \overline{g(\zeta^j)} = \overline{u_j}.$$

En efecte

$$u_j \overline{u_j} = u_j u_{p-j} = |u_j|^2 > 0$$

En definitiva com

$$\pm 1 = N(u) = (u_1 u_{p-1})(u_2 u_{p-2}) \dots > 0$$

ens implica $N(u) = 1$. Com $|u_j| = |\overline{u_j}|$, per tot $j = 1, ..., p-1$, cada $\frac{u_j}{u_{p-j}}$ és una unitat de $\mathbb{Z}[\zeta]$ amb valor absolut 1. A més per l'argument dels polinomis simètrics, el polinomi

$$\prod_{j=1}^{p-1} (t - \frac{u_j}{u_{p-j}})$$

té tots els coeficients a $\mathbb{Z}$. Per tant, pel Lema 7.5, tots els seus zeros són arrels de la unitat. El Teorema 7.3 ens diu que les arrels de la unitat de K són de la forma $\pm\zeta^a$, aleshores existeix alguna $a \in \mathbb{Z}$ tal que

$$\frac{u}{u_{p-1}} = \pm\zeta^a.$$

Com p és senar o bé u ó $u + p$ és parell i d'aquesta manera

$$\frac{u}{u_{p-1}} = \pm\zeta^{2k}. \tag{7.6}$$

per$0 < k \in \mathbb{Z}$.

Tot seguit volem determinar si el signe de (7.6) és positiu o negatiu. Per començar notem que per algun $b \in \mathbb{Z}$,

$$\zeta^{-k} u \equiv b \pmod{\mathcal{I}}$$

i prenent els conjugats complexes

$$\zeta^k u_{p-1} \equiv b \pmod{\langle\overline{\lambda}\rangle}$$

Recordem que $\overline{\lambda} = 1 - \zeta^{p-1}$ és un associat de λ, així doncs $\langle\overline{\lambda}\rangle = \langle\lambda\rangle = \mathcal{I}$. Llavors podem igualar les congruències eliminant b i el resultat és

$$\frac{u}{u_{p-1}} \equiv \zeta^{2k} \pmod{\mathcal{I}}.$$

En cas que el signe de l'equació (7.6) fos negatiu, aleshores $\mathcal{I}|\langle 2\zeta^{2k}\rangle$ i prenent normes $N(\mathcal{I})|2^{p-1}$, fet que contradiu el Lema 7.2 (b). Consegüentment el signe de (7.6) és positiu, i

$$\zeta^{-g}u = \zeta^{g}u_{p-1}.$$

Ambdós costats d'aquesta última equació són conjugats complexos, la qual cosa implica que són reals; per tant $r = \zeta^{-g}u \in \mathbb{R}$ i queda demostrat el Lema. □

8 L'especial cas de Kummer sobre l'últim teorema de Fermat

8.1 Consideracions elementals

L'objectiu d'aquesta secció és aclarir un parell de consideracions bàsiques que tenien els matemàtics alhora d'enfrontar-se a demostrar el teorema. Considerem ara l'equació de Fermat

$$x^n + y^n = z^n. \tag{8.1}$$

En primer lloc, si existeix una solució entera x, y, z de l'equació (8.1), aleshores x, y, z han de ser coprimers dos a dos. Suposem que existeix un nombre primer q que divideix x i y de manera que $x = qx'$ i $y = qy'$ i de l'equació (8.1) observem que $q^n(x'^n + y'^n) = z^n$. Per tant q també divideix z, amb $z = qz'$. Finalment ens queda $x'^n + y'^n = z'^n$.

D'altra banda notem que si l'equació (8.1) no té solucions enteres per un exponent n, aleshores no té solucions enteres per qualsevol múltiple d'aquest. Si l'equació $x^{mn} + y^{mn} = z^{mn}$ té solucions enteres, llavors $(x^m)^n + (y^m)^n = (z^m)^n$ també. Però qualsevol enter més gran o igual a 3 és divisible o per 4 o per p primer senar. Per tant és suficient considerar els casos $n = 4$ i n primer senar.

8.2 Demostració del primer cas

Per poder demostrar el primer cas de l'últim teorema de Fermat necessitem la següent definició.

Definició 8.1. *Direm que un nombre primer p és regular si no divideix el nombre de classe de $K = \mathbb{Q}(\zeta)$.*

Teorema. *Si p és un nombre primer regular senar, aleshores l'equació*

$$x^p + y^p = z^p$$

no té solucions enteres tal que x, y, z són coprimers amb p.

Demostració. Considerem l'equació

$$x^p + y^p + z^p = 0 \tag{8.2}$$

que prové de fer el canvi $z = -z$ a l'equació de Fermat.

Ho demostrarem per contradicció, per tant suposem que existeix una solució entera (x, y, z), coprimers amb p, de l'equació (8.2). Encara més podem suposar que (x, y, z) són coprimers dos a dos. Factoritzem l'equació (8.2) a $\mathbb{Q}(\zeta)$ i obtenim

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = -z^p$$

i passant a ideals

$$\prod_{i=0}^{p-1}\langle x+\zeta^i y\rangle = \langle z^p\rangle \tag{8.3}$$

Per començar hem de provar que tots els factors de l'esquerra de l'equació són coprimers dos a dos. Per veure-ho suposarem que existeix un ideal primer $\mathfrak{p}$ que divideix $\langle x+\zeta^k y\rangle$ i $\langle x+\zeta^l y\rangle$ amb $0 \leq k < l \leq p-1$. Aleshores $\langle x+\zeta^k y\rangle \subseteq \mathfrak{p}$ i $\langle x+\zeta^l y\rangle \subseteq \mathfrak{p}$, de manera que

$$\langle x+\zeta^k y\rangle - \langle x+\zeta^l y\rangle = y\zeta^k(1-\zeta^{l-k}) \in \mathfrak{p}$$

Recordem que $1-\zeta^{l-k}$ és un element associat de $\lambda = 1-\zeta$ i naturalment ζ^k és una unitat, així doncs $y\lambda \in \mathfrak{p}$. Al ser $\mathfrak{p}$ un ideal primer, per definició, notem que $\langle y\rangle \subset \mathfrak{p}$ o $\langle\lambda\rangle = \mathcal{I} \subset \mathfrak{p}$. Al primer cas $y \in \mathfrak{p}$ i $x+\zeta^i \in \mathfrak{p}$, de manera que $x \in \mathfrak{p}$. Com x i y són comprimers, aleshores existeixen $a, b \in \mathbb{Z}$ tal que $ax+by=1$. Però això ens implicaria que $1 \in \mathfrak{p}$, que no pot ser. D'altra banda tenim $\lambda \in \mathfrak{p}$. Al Lema 7.2 hem vist que $N(\mathcal{I}) = p$ és un nombre primer i la Proposició 5.31 ens implica que $\mathcal{I}$ és un ideal primer. Ara bé, al Teorema 5.12 tot ideal primer de $\mathbb{Z}[\zeta]$ és ideal maximal, per tant $\mathfrak{p}\mathcal{I}$. A més, com $\mathcal{I}$ divideix el costat esquerra de l'equació 8.3, aleshores $\mathcal{I}$ divideix $\langle z\rangle$. Per tant

$$p = N(\mathcal{I}) | N(\langle z\rangle) = z^{p-1}$$

doncs $p|z$ fet que ens contradiu la hipòtesi. En efecte els ideals de l'esquerra de l'equació (8.3) són primers dos a dos.

La factorització única en ideals primers implica que el costat esquerra de l'equació (8.3) és el producte de la potència p-èsima d'ideals primer. Tanmateix, com els ideals $\langle x+\zeta^i y\rangle$ són primers dos a dos, cada factor $\langle x+\zeta^i y\rangle$ és una potència p-èsima. En particular, existeix un ideal $\mathfrak{a}$ tal que

$$\langle x+\zeta y\rangle = \mathfrak{a}^p$$

En efecte $\mathfrak{a}^p$ és un ideal principal. La regularitat de p implica que p no divideix el nombre de classe h de $\mathbb{Q}(\zeta)$ i aplicant la Proposició 6.5 (b) obtenim que $\mathfrak{a}$ és principal. És a dir $\mathfrak{a} = \langle\delta\rangle$ per algun $\delta \in \mathbb{Z}[\zeta]$. D'aquesta manera

$$x+\zeta y = u\delta^p$$

on u és una unitat de $\mathbb{Z}[\zeta]$. Per la caracterització que hem fet de U_k al Lema 7.6 tenim que

$$x+\zeta y = r\zeta^k\delta^p$$

amb $r \in \mathbb{R}$ i $k \in \mathbb{R}$. Aleshores pel Lema 7.4 existeix un enter a tal que

$$\delta^p \equiv a \pmod{\mathcal{I}^p}.$$

i unint les dues equacions anteriors obtenim

$$x+\zeta y \equiv ra\zeta^k \pmod{\mathcal{I}^p}.$$

És més, pel Lema 7.2, $\langle p\rangle|\mathcal{I}^p$, llavors $x+\zeta y \equiv ra\zeta^k \pmod{\langle p\rangle}$. Com ζ^{-k} és una unitat de $\mathbb{Z}[\zeta]$, dividint obtenim la congruència $\zeta^{-k}(x+\zeta y) \equiv ra \pmod{\langle p\rangle}$ i prenent les conjugacions complexes ens porta a $\zeta^k(x+\zeta^{-1}y) \equiv ra \pmod{\langle p\rangle}$. Si restem una menys l'altre per eliminar ra tenim

$$x\zeta^{-k} + y\zeta^{1-k} - x\zeta^k - y\zeta^{k-1} \equiv 0 \pmod{\langle p\rangle}. \tag{8.4}$$

Volem provar que $1+\zeta$ és una unitat de $\mathbb{Z}[\zeta]$. Substituint $t=-1$ a l'equació (7.1) ens queda $1 = (-1-\zeta)(-1-\zeta)^2\ldots(-1-\zeta^{p-1}) = (-1)^{p-1}(1+\zeta)\ldots(1+\zeta^{p-1})$. Per tant $1+\zeta$ és unitat.

A continuació estudiarem els possibles valors de k a l'equació (8.4). Suposem que $k \equiv 0 \pmod p$. Aleshores $\zeta^k = 1$, que comporta que els termes de x desapareixen i l'equació (8.4) es transforma en

$$y(\zeta - \zeta^{-1}) \equiv y(-\zeta^{-1})(1-\zeta^2) \equiv y(1+\zeta)(1-\zeta) \equiv 0 \pmod{\langle p\rangle}.$$

Però hem vist que $1+\zeta$ és unitat, aleshores $y\lambda \equiv 0 \pmod{\langle p\rangle}$. Al lema 7.2 hem vist que $\langle p\rangle = \langle\lambda\rangle^{p-1}$ i $p-1 \geq 2$, així doncs $\lambda|y$. Prenent normes $p = N(\lambda)|N(y) = y^{p-1}$, de manera que $p|y$, fet que contradiu la hipòtesi. De manera semblant, si $k \equiv 1 \pmod p$ l'equació (8.4) es converteix en $x(\zeta-\zeta^{-1}) \equiv x(-\zeta^{-1})(1-\zeta^2) \equiv x(1+\zeta)(1-\zeta) \equiv 0 \pmod{\langle p\rangle}$. i els mateixos arguments mostren que $p|x$. En efecte $k \not\equiv 0,1 \pmod p$.

Ara, de l'equació (8.4) sabem que $x\zeta^{-k} + y\zeta^{1-k} - x\zeta^k - y\zeta^{k-1} = \alpha p$ per algun $\alpha \in \mathbb{Z}[\zeta]$. Per l'anterior paràgraf sabem que cap exponent és divisible per p i tenim la següent equació

$$\alpha = \frac{x}{p}\zeta^{-k} + \frac{y}{p}\zeta^{1-k} - \frac{x}{p}\zeta^k - \frac{y}{p}\zeta^{k-1}. \tag{8.5}$$

D'altra banda sabem que $\{1,\zeta,...,\zeta^{p-2}\}$ és una $\mathbb{Z}$-base de $\mathbb{Z}[\zeta]$. Llavors si tots els seus exponents no són congruents mòdul p, la independència lineal d'aquest conjunt sobre $\mathbb{Q}$ ens implica que $\frac{x}{p}, \frac{y}{p} \in \mathbb{Z}$, ja que $\alpha \in \mathbb{Z}[\zeta]$. Fet que ens contradiu la hipòtesi.

Per aquest motiu algun parell d'exponents ha de ser congruent mòdul p. Com $k \not\equiv 0,1 \pmod p$ la única possibilitat és que $2k \equiv 1 \pmod p$ que és equivalent a $k \equiv k-1 \pmod p$. Reescrivint (8.5) obtenim

$$\alpha p\zeta^k = x + y\zeta - x\zeta^{2k} - y\zeta^{2k-1} = x + y\zeta - x\zeta - y = (x-y)\lambda.$$

Prenent normes $N(\alpha)p^{p-1} = (x-y)^{p-1}p$, de manera que $p|(x-y)$, i per tant $x \equiv y \pmod p$. Per simetria de l'equació (8.2) hem de tenir $y \equiv z \pmod p$ i per tant

$$0 \equiv x^p + y^p + z^p \equiv 3x^p \pmod p.$$

Per hipòtesi $x \nmid p$i d'aquesta manera p ha de ser igual a 3.

Així doncs només queda fer front a la possibilitat que $p=3$. Notem que els nombres $a = 1,2,4,5,7,8$ coprimers amb 9 satisfan o bé $a \equiv 1 \pmod 9$ o $a \equiv -1 \pmod 9$. Per tant qualsevol solució de (8.2) d'enters coprimers amb 3 és de la forma

$$\pm 1 \pm 1 \pm 1 \equiv 0 \pmod 9$$

que és impossible. Així doncs, finalment, $p \neq 3$ i tenim una contradicció.

□

9 Conclusions

La realització d'aquest projecte permet entendre com va sorgir històricament el què actualment s'entén per teoria algebraica de nombres bàsica. D'altra banda conté la teoria necessària i comprensible, amb nocions d'estructures algebraiques, per entendre la demostració del primer cas de l'Últim Teorema de Fermat feta per Kummer.

M'agradaria remarcar que no he inclòs les demostracions del teorema de finitud de classes i del teorema de les unitats de Dirichlet perquè necessitava teoria de mètodes geomètrics que no formava part de l'objectiu d'aquest treball.

La continuació d'aquest treball seria completar la demostració de l'Últim Teorema de Fermat pels primers regulars, és a dir demostrar el segon cas. Aquest consisteix en que algun dels x, y, z és múltiple de p. La demostració de Kummer d'aquest cas també depèn de la teoria d'ideals, no obstant necessitaríem una proposició que és coneguda pel Lema de Kummer. És a dir, veure que si una unitat de $\mathbb{Q}(\zeta)$ és congruent a un nombre enter mòdul p, aleshores aquesta unitat és una potència d'una altre unitat de $\mathbb{Q}(\zeta)$. Tanmateix, la prova d'aquesta necessita mètodes nous.

Referències

[1] Edwards, Harold M: *Fermat's Last Theorem: a genetic introduction to algebraic number theory*, Springer-Verglag, New york, 1977.

[2] Jarvis, Frazer: *Algebraic Number Theory*, Springer, Sheffield, 2014.

[3] Kato, Kazuya; Kurokawa, Nobushige; Saito, Takeshi: *Number Theory 1: Fermat's Dream*, American Mathematical Society, USA, 1996.

[4] Ono, Takashi: *An introduction to Algebraic Number Theory*, Plenum Publishing Corporation, New York, 1990.

[5] Stewart, Ian; Tall, David: *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, Natick, 2002.

[6] Washington, Lawrence C: *Introduction cyclotomic fields*, Springer, New York, 1997.