UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

TEOREMA DE CHEBOTAREV

Autor: Isabel Ramon Taltavull

Director: Dr. Xavier Guitart Morales
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 16 de juny de 2019

Abstract

The aim of this dissertation is the study of *Chebotarev's Theorem*, which gives the density of a set of prime ideals in terms of conjugacy classes of Frobenius elements.

In order to achieve our goal, this work has been divided into three parts. The first part is an introduction to the basic properties of number fields. Moreover, two important examples are studied in detail: quadratic and cyclotomic fields. The aim of this part is to define and describe the ring of integrers of a number field.

Furthermore, it is important to understand the Frobenius element to reach the goal of this work, therefore its second part is focused on the Frobenius element associated to a prime ideal of a number field. The element of Frobenius, or more precisely its conjugacy class in the Galois group is essential for the understanding of *Chebotarev Theorem*.

Lastly, assuming previous knowledge corresponding to the Dedekind zeta function, the *Chebotarev Theorem* is stated and proved, and also two of its most known particular cases are given: the *Dirichlet's Theorem on arithmetic progressions* and the *Frobenius Theorem*.

Resum

L'objectiu principal d'aquest treball és estudiar el *Teorema de densitat de Chebotarev*, que dona la densitat d'un conjunt d'ideals primers en termes de classes de conjugació d'elements de Frobenius.

Aquest treball està dividit en tres parts. La primera part és una introducció de les nocions bàsiques dels cossos de nombres, i es detallen els dos exemples més usuals, els cossos quadràtics i els ciclotòmics. L'objectiu d'aquesta part és donar les eines necessàries per poder definir l'anell d'enters corresponents a un cos de nombres, en particular l'anell d'enters dels cossos ciclotòmics.

El segon objectiu del treball és entendre l'element de Frobenius associat a un ideal primer d'un cos de nombres. Aquest element de Frobenius, o la seva classe de conjugació en el grup de Galois, és un dels ingredients essencials per a entendre bé l'enunciat del *Teorema de Chebotarev*.

Finalment, assumint un resultat sobre funcions zeta de Dedekind, enunciem i demostrem el *Teorema de Chebotarev* i donem dos casos particulars d'aquest teorema que són més coneguts: el *Teorema de Dirichlet sobre primers en progressions aritmètiques* i el *Teorema de Frobenius*.

2010 Mathematics Subject Classification. 12F05, 12F10

Agraïments

En primer lloc, agraeixo al tutor del meu treball, Xevi Guitart, per l'orientació constant. M'ha ajudat a organitzar la feina i m'ha resolt tots els dubtes que m'han anat sorgint.

Vull agrair el suport que m'han brindat les meves companyes de pis, la Núria i la Laura, en tots els moments que ho he necessitat, no només aquest darrer semestre sinó durant els darrers anys.

També, un especial agraïment a tota la meva família que sempre m'han recolzat en totes les metes que m'he anat proposant.

Finalment, agraeixo a totes les amistats, tant les noves com les que ja tenia, que d'una manera o altra han estat partícips de la meva vida durant els anys que he cursat el grau.

Índex

1 Introducció

Classifiquem els 100 primers nombres primers segons el seu darrer dígit i obtenim:

$1 : 11, 31, 41, 61, 71$

$2 : 2$

$3 : 3, 13, 23, 43, 53, 73, 83$

$5 : 5$

$7 : 7, 17, 37, 47, 67, 97$

$9 : 19, 29, 59, 79, 89$

Per una banda, podem veure com no hi ha cap primer que acabi amb $0, 4, 6$ o 8 i que només hi ha un primer que acabi en 2 i un en 5.

Per altra banda, observem que els únics enters positius entre 1 i 10 que satisfan la condició de coprimeritat amb 10 són $1, 3, 7$ i 9, que són, precisament, els nombres pels quals podem observar a la taula que hi ha més primers acabats en aquests dígits.

Dirichlet va estudiar aquest fet i demostrà l'anomenat *Teorema de Dirichlet* que afirma que: *"Donats a i m enters primers tals que $(a, m) = 1$, llavors la progressió aritmètica $a + nm$, amb $n \in \mathbb{N}$, conté infinits primers."* Aquest enunciat és equivalent a dir que existeix una quantitat infinita de primers p tals que $p \equiv a (\text{mod } m)$. Per tant, podríem dir que l'experiment que hem fet il·lustra el *Teorema de Dirichlet* en el cas $m = 10$.

Referent a la demostració que va fer Dirichlet d'aquest teorema podem dir que va usar conceptes com les L-sèries de Dirichlet associades als caràcters de Dirichlet. En particular, provà que $L(\chi, 1) \neq 0$ quan $\chi \neq 1$ i que $L(1, s)$, que és essencialment la funció zeta de Riemann, té un pol simple en $s = 1$. Per fer-ho va necessitar resultats de convergència de les L-sèries de Dirichlet.

El *Teorema de Dirichlet* es pot reescriure en termes de grups de Galois, per fer-ho donem el següent isomorfisme: sigui m un enter positiu i sigui $\rho_m = e^{2\pi i/m}$ una arrel primitiva m-éssima de la unitat. Aleshores,

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \text{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q})$$

$$a \mapsto (\rho_m \mapsto \rho_m^a).$$

En particular, a cada primer $p \in (\mathbb{Z}/m\mathbb{Z})^*$ li correspon un element Frob_p del grup de Galois de l'extensió ciclotòmica $\mathbb{Q}(\rho_m)/\mathbb{Q}$. De manera que el *Teorema de Dirichlet* es tradueix a: *"Donat $h \in \text{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q})$ existeixen infinits primers p tals que $\text{Frob}_p = h$."*.

L'objectiu d'aquest treball és entendre el *Teorema de Chebotarev*, que és una generalització del *Teorema de Dirichlet* canviant l'extensió ciclotòmica $\mathbb{Q}(\rho_m)/\mathbb{Q}$ per una extensió de cossos de nombres L/K, on un cos de nombres és una extensió de cossos de dimensió finita de $\mathbb{Q}$. També en donarem una demostració, assumint un resultat de teoria analítica de nombres.

Per estudiar-ho desenvolupem les eines necessàries per poder definir els cossos de nombres i els anells d'enters corresponents. A continuació, ens preguntem quin és i com es tracta l'element del grup de Galois que s'associa a cada primer de L: el concepte que cal assimilar s'anomena element de Frobenius i es denota per Frob_p, i per poder manejar-lo s'estudia com descomponen els ideals primers en els anells d'enters de cossos de nombres. Finalment, acabarem el treball enunciant i demostrant el *Teorema de Chebotarev*.

2 Cossos de nombres

En aquesta secció, es defineixen algunes de les nocions bàsiques de la teoria algebraica de nombres, i es donen alguns resultats per poder definir els conceptes de cos de nombres i de l'anell d'enters corresponent.

Definició 2.1. *Un nombre algebraic α és un nombre complex que satisfà algun polinomi mònic amb coeficients racionals. És a dir, per algun*

$$p(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + ... + a_0$$

amb $a_0, ..., a_{n-1} \in \mathbb{Q}$, es compleix que $p(\alpha) = 0$.

Observació 2.2. Recordem que el polinomi mínim d'un element α és el polinomi mònic de grau més petit que té α com arrel. De fet, cada nombre algebraic té un polinomi mínim de coeficients racionals.

Definició 2.3. *Direm grau d'un nombre algebraic α al grau del seu polinomi mínim. Es denota per* $\deg(\alpha)$.

Teorema 2.4. *Sigui α un nombre complex, llavors són equivalents:*

1) α és un nombre algebraic.

2) L'anell

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} | a_0, ..., a_{n-1} \in \mathbb{Q}\}$$

és un espai vectorial de dimensió finita sobre $\mathbb{Q}$.

3) α pertany a un anell $L \subset \mathbb{C}$ que és espai vectorial de dimensió finita sobre $\mathbb{Q}$.

Demostració. En primer lloc, provarem que 1) implica 2). Com α és un nombre algebraic compleix algun polinomi

$$p(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + ... + a_0$$

amb coeficients racionals. Aleshores $\alpha^n = -\sum_{i=0}^{n-1} a_i\alpha^i$, així l'espai vectorial complex generat per $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ també conté α^n. A més, per recursivitat tenim que totes les potències majors de α estan a l'espai vectorial.

Veure que 2) implica 3) és immediat, ja que $\mathbb{Q}[\alpha] \subset \mathbb{C}$. Cal posar $L = \mathbb{Q}[\alpha]$.

I per acabar, provem que 3) implica 1. Considerem l'anell $L =< g_1, ..., g_n >$ com espai vectorial sobre $\mathbb{Q}$. Per cada $i \in \{1, ..., n\}$, $\alpha g_i = \sum_{j=1}^{n} a_{ij}g_j$. Definint $g = (g_1, ..., g_n)^T$ i una matriu M de dimensió $n \times n$ amb coeficients a_{ij}, tenim

$$\alpha g = Mg.$$

Per tant α és un valor propi de M, és a dir, α és l'arrel del polinomi característic de M, que és mònic i de coeficients racionals.

□

Corol·lari 2.5. *Els nombres algebraics formen un cos $\bar{\mathbb{Q}}$.*

Demostració. Siguin α i β nombres algebraics. Per la demostració de l'anterior teorema i suposant que $\deg(\alpha) = m$ i $\deg(\beta) = n$, tenim que els anells $\mathbb{Q}[\alpha]$ i $\mathbb{Q}[\beta]$ tenen

bases $\{1, \alpha, ..., \alpha^{m-1}\}$ i $\{1, \beta, ..., \beta^{n-1}\}$, respectivament, com a espais vectorials sobre $\mathbb{Q}$. Sigui $L = \mathbb{Q}[\alpha, \beta]$ generat pel conjunt $\{\alpha^i \beta^j | 0 \leq i \leq m-1, 0 \leq j \leq n-1\}$ com a espai vectorial sobre $\mathbb{Q}$. Llavors, $\alpha + \beta$ i $\alpha\beta$ pertanyen a L. Per la condició 3) del teorema sabem que $\alpha + \beta$ i $\alpha\beta$ són nombres algebraics.

Ens queda veure que existeix l'invers pel producte de qualsevol nombre algebraic diferent del zero. Sigui $\alpha \neq 0$ i sigui $p(X)$ el polinomi que té α com arrel i té el seu terme independent $a_0 \neq 0$, llavors $p(\alpha) = 0$ implica que $\alpha^{-1} = \frac{p(\alpha) - a_0}{-a_0 \alpha} \in \mathbb{Q}[\alpha]$, el que significa per la condició 3) que α^{-1} és nombre algebraic.

□

Definició 2.6. *Un cos de nombres K és un subcòs de $\bar{\mathbb{Q}}$ que té dimensió finita com a espai vectorial sobre $\mathbb{Q}$. És a dir, $[K : \mathbb{Q}] = \dim_{\mathbb{Q}}(K) < \infty$.*

Definició 2.7. *Direm que $\dim_{\mathbb{Q}}(K)$ és el grau del cos de nombres K.*

Observació 2.8. Quan K és extensió finita de $\mathbb{Q}$, el cos de nombres K és espai vectorial de dimensió finita sobre $\mathbb{Q}$. Per tant, existeix una base de K sobre $\mathbb{Q}$.

No donarem la demostració del següent teorema, però en cas de ser d'interès pel lector es pot trobar en el *Teorema 50* del *Apèndix B* del llibre [1].

Teorema 2.9. *Sigui K un cos de nombres de grau n. Llavors, existeixen n $\mathbb{Q}$-morfismes de cossos no trivials, és a dir, existeixen $\sigma_i : K \to \mathbb{C}$ per $i \in \{1, ..., n\}$.*

En el cas particular $K = \mathbb{Q}[\alpha]$, denotem per $p(X)$ al polinomi mínim d'α, que és irreductible sobre $\mathbb{Q}$. Aquest polinomi té n arrels complexes diferents, $\alpha_1, ..., \alpha_n$. Per cada i, l'embedding σ_i compleix,

$$\sigma_i(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) = a_0 + a_1\alpha_i + ... + a_{n-1}\alpha_i^{n-1}.$$

2.1 Enters algebraics

Definició 2.10. *Un enter algebraic α és un nombre complex que satisfà algun polinomi mònic amb coeficients enters. És a dir, per algun*

$$p(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + ... + a_0$$

amb $a_0, ..., a_{n-1} \in \mathbb{Z}$, es compleix que $p(\alpha) = 0$.

El polinomi no necessàriament és irreductible sobre $\mathbb{Z}$. Però, a continuació, veurem que cada enter algebraic és arrel d'algun polinomi mònic irreductible sobre $\mathbb{Z}$. Recordem l'enunciat del *Lema de Gauss*:

Lema 2.11. *(Lema de Gauss) Sigui f un polinomi mònic amb coeficients enters, i suposem que $f = gh$, on g i h són polinomis mònics amb coeficients racionals. Llavors g i h són polinomis amb coeficients enters.*

Teorema 2.12. *Sigui α un enter algebraic, i f un polinomi mònic sobre $\mathbb{Z}$ de grau mínim tenint α com arrel. Llavors, f és irreductible sobre $\mathbb{Q}$.*

Demostració. Per provar el teorema suposarem el contrari. Suposem que f no és irreductible sobre $\mathbb{Q}$, llavors $f = gh$ on g i h són polinomis no constants en $\mathbb{Q}[X]$. Suposem

que g i h són mònics i, pel *Lema de Gauss*, tenen coeficients enters. Com α és arrel de f, llavors ho serà o de g o de h. Però, això és impossible per la hipòtesi que f és el polinomi de grau menor que té α com arrel.

□

Teorema 2.13. *Sigui α un nombre complex, llavors són equivalents:*

1) α és un enter algebraic.

2) El grup additiu de l'anell $\mathbb{Z}[\alpha]$ és finitament generat.

3) α pertany a un subanell $L \subset \mathbb{C}$ que té un grup additiu finitament generat.

4) $\alpha A \subset A$ per algun subgrup additiu finitament generat $A \subset \mathbb{C}$

Demostració. Primer, provem que 1) implica 2). Que α sigui un enter algebraic, significa que és solució d'un polinomi mònic $p(X) = a_0 + a_1X + a_2X^2 + ... + a_{n-1}X^{n-1}$ sobre $\mathbb{Z}$. És a dir, $p(\alpha) = 0$. Llavors, obtenim

$$\alpha^n = -\sum_{i_0}^{n-1} a_i \alpha^i.$$

Això significa que α^n es pot generar a partir de $\{1, \alpha, ..., \alpha^{n-1}\}$. Per tant,

$$\mathbb{Z}[\alpha] =< 1, \alpha, ..., \alpha^{n-1} > .$$

Provar que 2) implica 3) és immediat. Posant $L = \mathbb{Z}[\alpha]$ obtenim el que volíem.

Suposem que $\alpha \in L =< g_1, ..., g_n > \subset \mathbb{C}$. Llavors,

$$\alpha L =< \alpha g_1, ..., \alpha g_n > \subset < g_1, ..., g_n >= L$$

Finalment, ens queda veure que 4) implica 1). Sigui A generat per $\{a_1, ..., a_n\}$, per tot $i \in \{1, ..., n\}$ expressem αa_i com a combinació lineal de $\{a_1, ..., a_n\}$ amb coeficients enters. Obtenim,

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

on M és matriu de dimensió $n \times n$ sobre $\mathbb{Z}$. És a dir, $(\alpha Id - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$.

Prenent determinants, com que no tots els a_i són zero tenim $\det(\alpha Id - M) = 0$. Això significa que α és valor propi de M. Per tant, α és arrel del polinomi característic de M, que és mònic i de coeficients enters.

□

Teorema 2.14. *Els enters algebraics $\bar{\mathbb{Z}}$ formen un subanell de $\bar{\mathbb{Q}}$.*

Demostració. Siguin α i β enters algebraics (suposem que els seus polinomis mínims tenen grau n i m, respectivament), llavors per l'apartat *2)* del teorema anterior tenim que existeixen $\{1, \alpha, ..., \alpha^{n-1}\}$ tal que $\mathbb{Z}[\alpha] =< 1, \alpha, ..., \alpha^{n-1} >$ i també existeixen $\{1, \beta, ..., \beta^{m-1}\}$ tal que $\mathbb{Z}[\beta] =< 1, \beta, ..., \beta^{m-1} >$. Llavors, el conjunt de productes $\{\alpha^i \beta^j : i \in \{1, ..., n\}, j \in \{1, ..., m\}\}$ genera $\mathbb{Z}[\alpha, \beta]$.

Com $\alpha+\beta, \alpha\beta \in \mathbb{Z}[\alpha,\beta]$, o sigui els dos elements pertanyen a un subanell que té grup additiu finitament generat, llavors per l'apartat *3)* del teorema anterior $\alpha+\beta$ i $\alpha\beta$ són enters algebraics.

A partir del que acabem de provar i sabent que -1 és enter algebraic (per ser enter), obtenim que per qualsevol enter algebraic γ, $-\gamma$ és enter algebraic.

Evidentment $0, 1$ són enters algebraics que segueixen sent elements neutres per la suma i el producte, respectivament.

Llavors, $\bar{\mathbb{Z}}$ és subanell de $\mathbb{C}$.

□

Definició 2.15. *L'anell d'enters corresponent a un cos de nombres K és l'anell de tots els enters algebraics que estan continguts en K. Es denota per*

$$\mathcal{O}_K = K \cap \bar{\mathbb{Z}}.$$

Com que K és cos, i per tant anell, i $\bar{\mathbb{Z}}$ és anell pel *Teorema 2.14*, llavors $\mathcal{O}_K$ és anell.

2.2 Traça i norma.

En aquest apartat definim la norma i la traça de cossos de nombres. Són dos conceptes que solen usar-se en la teoria algebraica de nombres.

Definició 2.16. *Sigui K un cos de nombres tal que $n = [K : \mathbb{Q}]$, siguin $\sigma_1, ..., \sigma_n$ els embeddings de K en $\mathbb{C}$. La norma de K és una aplicació $N : K \to \mathbb{C}$ tal que, per cada $\alpha \in K$,*

$$N(\alpha) = \sigma_1(\alpha)...\sigma_n(\alpha).$$

Definició 2.17. *Sigui K un cos de nombres tal que $n = [K : \mathbb{Q}]$, siguin $\sigma_1, ..., \sigma_n$ els embeddings de K en $\mathbb{C}$. La traça de K és una aplicació $T : K \to \mathbb{C}$ tal que, per cada $\alpha \in K$,*

$$T(\alpha) = \sigma_1(\alpha) + ... + \sigma_n(\alpha).$$

Tant la norma com la traça de K depenen del cos K, per això en alguns casos per evitar confusions escriurem $N^K(\alpha)$ i $T^K(\alpha)$.

Observació 2.18. Sigui K un cos de nombres, siguin $\alpha, \beta \in K$ i $\lambda \in \mathbb{Q}$. Aleshores,

$$N(\alpha\beta) = N(\alpha)N(\beta), \quad T(\alpha+\beta) = T(\alpha) + T(\beta)$$

$$N(\lambda) = \lambda^n, \quad T(\lambda) = n\ \lambda$$

$$N(\lambda\alpha) = \lambda^n N(\alpha), \quad T(\lambda\alpha) = \lambda T(\alpha)$$

El següent teorema es dona per provar que la norma i la traça d'un cos de nombres són nombres racionals.

Teorema 2.19. *Sigui K un cos de nombres tal que $n = [K : \mathbb{Q}]$, i sigui $\alpha \in K$ de grau d sobre $\mathbb{Q}$. Llavors, tenim*

$$N(\alpha) = (N^{\mathbb{Q}[\alpha]}(\alpha))^{n/d}, \quad T(\alpha) = \frac{n}{d}(T^{\mathbb{Q}[\alpha]}(\alpha)).$$

Demostració. Tenim $[K:\mathbb{Q}[\alpha]] = [K:\mathbb{Q}]/[\mathbb{Q}[\alpha]:\mathbb{Q}] = n/d$, i pel *Teorema 2.9* sabem que existeixen n/d embeddings de $\mathbb{Q}[\alpha]$ en $\mathbb{C}$. Finalment, per les definicions de la norma i la traça tenim el que volíem provar.

□

Corol·lari 2.20. *Sigui K un cos de nombres i sigui $\alpha \in K$, llavors $N(\alpha)$ i $T(\alpha)$ són nombres racionals.*

Demostració. És suficient provar que $N^{\mathbb{Q}[\alpha]}(\alpha)$ i $T^{\mathbb{Q}[\alpha]}(\alpha)$ són nombres racionals. El polinomi mínim $p(X)$ de α descompon per $p(X) = (X-\alpha_1)...(X-\alpha_n)$ a $\bar{\mathbb{Q}}$, i per tant el terme independent de $p(X)$ és $\pm N^{\mathbb{Q}[\alpha]}(\alpha)$ i el coeficient de X^{n-1} és $-T^{\mathbb{Q}[\alpha]}(\alpha)$.

Com que α és nombre algebraic, llavors els coeficients de $p(X)$ són nombres racionals. Per tant, $N^{\mathbb{Q}[\alpha]}(\alpha)$ i $T^{\mathbb{Q}[\alpha]}(\alpha)$ són nombres racionals.

□

Corol·lari 2.21. *Sigui K un cos de nombres i sigui $\alpha \in K$ és enter algebraic, llavors $N(\alpha)$ i $T(\alpha)$ són nombres enters.*

Demostració. Si α és enter algebraic, llavors el seu polinomi mínim sobre $\mathbb{Q}$ té coeficients enters. Per la demostració del corol·lari anterior, tenim $N^{\mathbb{Q}[\alpha]}(\alpha)$ i $T^{\mathbb{Q}[\alpha]}(\alpha)$ són nombres enters.

□

2.3 Discriminant.

Com bé hem explicat a la introducció, aquest capítol conté una sèrie d'eines necessàries per determinar alguns anells d'enters de cossos de nombres. Per exemple, es necessita per calcular l'anell d'enters corresponent als cossos ciclotòmics.

Definició 2.22. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Siguin $\sigma_1, ..., \sigma_n$ els n embeddings de K en $\mathbb{C}$. Definim el discriminant de $\alpha_1, ..., \alpha_n \in K$ per*

$$\mathrm{disc}(\alpha_1, ..., \alpha_n) = \det([\sigma_i(\alpha_j)]_{i,j=1,...,n})^2$$

Com que el discriminant és un quadrat, és indiferent l'ordre dels σ_i i dels α_j, per a $i, j \in \{1, ..., n\}$.

Teorema 2.23. *Sigui K cos de nombres de grau n sobre $\mathbb{Q}$. Siguin $\alpha_1, ..., \alpha_n \in K$. Llavors,*

$$\mathrm{disc}(\alpha_1, ..., \alpha_n) = \det([T(\alpha_i\alpha_j)]_{i,j=1,...,n})$$

Demostració. Fem producte de matrius,

$$[\sigma_j(\alpha_i)]_{i,j=1,...,n}[\sigma_i(\alpha_j)]_{i,j=1,...,n} = [\sigma_1(\alpha_i\alpha_j) + ... + \sigma_n(\alpha_i\alpha_j)]_{i,j=1,...,n} = [T(\alpha_i\alpha_j)]_{i,j=1,...,n}$$

I prenent determinants tenim el que volíem.

□

Corol·lari 2.24. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Siguin $\alpha_1, ..., \alpha_n \in K$. Aleshores* $\mathrm{disc}(\alpha_1, ..., \alpha_n) \in \mathbb{Q}$.

Demostració. Pel *Teorema 2.23*,

$$\text{disc}(\alpha_1, ..., \alpha_n) = \det([T(\alpha_i\alpha_j)]_{i,j=1,...,n}).$$

Sabem pel *Corol·lari 2.20*, per qualsevol $i, j \in \{1, ..., n\}$, $T(\alpha_i\alpha_j)$ és un nombre racional.

□

Corol·lari 2.25. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Siguin $\alpha_1, ..., \alpha_n \in K$ enters algebraics, llavors* $\text{disc}(\alpha_1, ..., \alpha_n) \in \mathbb{Z}$.

Demostració. Pel *Teorema 2.23*,

$$\text{disc}(\alpha_1, ..., \alpha_n) = \det([T(\alpha_i\alpha_j)]_{i,j=1,...,n}).$$

Sabem que el producte de dos enters algebraics és enter algebraic, i pel *Corol·lari 2.21*, per qualsevol $i, j \in \{1, ..., n\}$, $T(\alpha_i\alpha_j)$ és un nombre enter.

□

A l'*Observació 2.8* hem assegurat l'existència de bases de K en $\mathbb{Q}$. El següent teorema ens dona la relació que existeix entre els discriminants de dos bases de K sobre $\mathbb{Q}$.

Teorema 2.26. *Sigui K cos de nombres de grau n sobre $\mathbb{Q}$. Siguin $\{\omega_1, ..., \omega_n\}$ i $\{\beta_1, ..., \beta_n\}$ dues bases de K sobre $\mathbb{Q}$, llavors*

$$\text{disc}(\omega_1, ..., \omega_n) = \det([a_{ij}]_{i,j=1,...,n})^2 \text{disc}(\beta_1, ..., \beta_n)$$

on $[a_{ij}]_{i,j=1,...,n}$ és la matriu de canvi de la base $\{\omega_1, ..., \omega_n\}$ a la base $\{\beta_1, ..., \beta_n\}$.

Demostració. Escrivim la base $\{\omega_1, ..., \omega_n\}$ en funció de $\{\beta_1, ..., \beta_n\}$. Per $k \in \{1, ..., n\}$,

$$\omega_k = \sum_{i=1}^{n} a_{ik}\beta_i.$$

Com que $\{\omega_1, ..., \omega_n\}$ i $\{\beta_1, ..., \beta_n\}$ són bases de K sobre $\mathbb{Q}$, llavors $\det([a_{ik}]_{i,k=1,...,n}) \neq 0$.

Aplicant que tot automorfisme de K fixa $\mathbb{Q}$, per $j, k \in \{1, ..., n\}$,

$$\sigma_j(\omega_k) = \sigma_j(\sum_{i=1}^{n} a_{ik}\beta_i) = \sum_{i=1}^{n} a_{ik}\sigma_j(\beta_i)$$

Prenent determinants obtenim, per $k \in \{1, ..., n\}$,

$$\det([\sigma_j(\omega_k)]_{j,k=1,...,n}) = \det([\sum_{i=1}^{n} a_{ik}\sigma_j(\beta_i)]_{j,i=1,...,n}) = \det([a_{ik}]_{i,k=1,...,n}) \det([\sigma_j(\beta_i)]_{j,i=1,...,n})$$

Elevant al quadrat l'anterior igualtat, per la *Definició 2.22*, obtenim el que volem provar,

$$\text{disc}(\omega_1, ..., \omega_n) = \det([a_{ik}]_{i,k=1,...,n})^2 \text{disc}(\beta_1, ..., \beta_n)$$

□

El següent teorema ens dona una fórmula del discriminant d'una base, de K sobre $\mathbb{Q}$, que està formada per les potències d'un sol element.

Definició 2.27. *Sigui K un cos de nombres. Sigui $\alpha \in K$. Sigui f un polinomi mònic irreductible per α sobre $\mathbb{Q}$. Els conjugats de α sobre $\mathbb{Q}$ són les arrels $\alpha_1, ..., \alpha_n$ de f.*

Teorema 2.28. *Sigui $K = \mathbb{Q}[\alpha]$, i siguin $\alpha_1, ..., \alpha_n$ els conjugats de α sobre $\mathbb{Q}$. Llavors,*

$$\operatorname{disc}(1, \alpha, ..., \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \pm N^K(f'(\alpha))$$

on f és el polinomi mònic irreductible per α sobre $\mathbb{Q}$.

Demostració. Sabem que existeixen n embeddings, els denotem per $\sigma_1, ..., \sigma_n$.

Comencem provant la primera igualtat. Com que $[\sigma_i(\alpha^{j-1})] = [(\sigma_i(\alpha)^{j-1})]$, llavors tindrem $\operatorname{disc}(1, \alpha, ..., \alpha^{n-1}) = \det([\sigma_i(\alpha^{j-1})]_{i,j=1,...,n})^2 = \det([(\sigma_i(\alpha)^{j-1}]_{i,j=1,...,n})^2$.

Usant que $\{\sigma_i(\alpha)^{j-1}\}_{i,j=1,...,n}$ és matriu Vandermonde, obtenim

$$\operatorname{disc}(\alpha) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

on $\alpha_1, ..., \alpha_n$ són els zeros del polinomi mínim de α. És a dir, $\alpha_1, ..., \alpha_n$ són els conjugats.

Passem a provar la segona igualtat.

Sabem que f té coeficients racionals, i per tant la seva derivada també. Aleshores,

$$N^K(f'(\alpha)) = \prod_{1 \leq i \leq n} \sigma_i(f'(\alpha)) = \prod_{1 \leq i \leq n} f'(\sigma_i(\alpha)) = \prod_{1 \leq i \leq n} f'(\alpha_i).$$

Com que f és polinomi mònic irreductible, i $\alpha_1, ..., \alpha_n$ les seves arrels en $\mathbb{C}$ llavors podem escriure $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$. Fent la derivada, per algun $i \in \{1, ..., n\}$, obtenim

$$f'(X) = (X-\alpha_1) \cdots \widehat{(X-\alpha_i)} \cdots (X-\alpha_n) + (X-\alpha_i)[(X-\alpha_1) \cdots \widehat{(X-\alpha_i)} \cdots (X-\alpha_n)]'.$$

Avaluat a α_i, tenim

$$f'(\alpha_i) = (\alpha_i - \alpha_1) \cdots \widehat{(\alpha_i - \alpha_i)} \cdots (\alpha_i - \alpha_n) + 0 = \prod_{\substack{1 \leq j \leq n \\ i \neq j}} (\alpha_i - \alpha_j)$$

Tenint en compte que

$$\prod_{\substack{1 \leq j \leq n \\ i < j}} (\alpha_i - \alpha_j)^2 = \pm \prod_{\substack{1 \leq j \leq n \\ i \neq j}} (\alpha_i - \alpha_j)$$

obtenim el que volíem.

□

2.4 Aplicacions del discriminant. Base d'enters.

Definició 2.29. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$ s'anomena base d'enters de K.*

Per cada cos de nombres K de grau n, existeixen n enters algebraics $\omega_1, ..., \omega_n$ tals que

$$\mathcal{O}_K = \{m_1\omega_1 + ... + m_n\omega_n | m_1, ..., m_n \in \mathbb{Z}\}.$$

De fet, els enters $\omega_1, ..., \omega_n$ formen una base d'enters de K, és a dir $\mathcal{O}_K =< \omega_1, ..., \omega_n >_{\mathbb{Z}}$. Abans d'usar les bases d'enters cal provar que realment existeixen, cal provar que $\mathcal{O}_K$ és grup abelià lliure de rang n.

Definició 2.30. *Un grup lliure abelià finitament generat de rang n és un grup isomorf a* $\mathbb{Z}^n$.

Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Existeix una base de K sobre $\mathbb{Q}$, $\{\alpha_1, ..., \alpha_n\}$. Definim el conjunt

$$A = \{a_1\alpha_1 + ... + a_n\alpha_n \ | a_1, ..., a_n \in \mathbb{Z}\}$$

que és un grup generat per $< \alpha_1, ..., \alpha_n >$. Podem expressar A com $\mathbb{Z}\alpha_1 \oplus ... \oplus \mathbb{Z}\alpha_n$. Així doncs, podem afirmar que A és un grup abelià lliure de rang n, per tenir cada sumant isomorf a $\mathbb{Z}$. Per tant, $A \subset \mathcal{O}_K$.

A continuació donarem un teorema per provar que $\mathcal{O}_K$ està contingut en un grup lliure abelià de rang n.

Teorema 2.31. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Sigui $\{\alpha_1, ..., \alpha_n\} \subset \mathcal{O}_K$ una base de K sobre $\mathbb{Q}$. Llavors, qualsevol element de $\mathcal{O}_K$ es pot expressar de la forma següent*

$$\frac{a_1\alpha_1 + \cdots + a_n\alpha_n}{\text{disc}(\alpha_1, ..., \alpha_n)}$$

on $a_1, ..., a_n \in \mathbb{Z}$, i per a tot $i \in \{1, ..., n\}$ es compleix que a_i^2 és divisible per $\text{disc}(\alpha_1, ..., \alpha_n)$.

El teorema està ben definit ja que, pel *Corol·lari 2.25*, $\text{disc}(\alpha_1, ..., \alpha_n) \in \mathbb{Z}$ i és no nul.

Demostració. Siguin $\sigma_1, ..., \sigma_n$ els embeddings de K en $\mathbb{C}$. Considerem $\alpha \in \mathcal{O}_K$ tal que

$$\alpha = X_1\alpha_1 + ... + X_n\alpha_n$$

on $X_1, ..., X_n \in \mathbb{Q}$. Apliquem cadascun dels embeddings obtenint un sistema d'equacions lineals

$$\left.\begin{array}{ccc} \sigma_1(\alpha) = X_1\sigma_1(\alpha_1) + ... + X_n\sigma_1(\alpha_n) \\ \vdots \qquad \vdots \qquad\qquad \vdots \\ \sigma_n(\alpha) = X_1\sigma_n(\alpha_1) + ... + X_n\sigma_n(\alpha_n) \end{array}\right\}$$

Resolem el sistema usant el criteri de Cramer, tenim

$$X_j = \frac{\gamma_j}{\delta} \quad \text{per a tot } j \in \{1, ..., n\}$$

on $\delta = \det([\sigma_j(\alpha_i)]_{i,j=1,...,n})$ i γ_j és el determinant de la matriu $[\sigma_j(\alpha_i)]_{i,j=1,...,n}$ canviant la j-éssima columna per el vector columna $\sigma_i(\alpha)$. Per això, γ_j i δ són enters algebraics i $\delta^2 = \text{disc}(\alpha_1, ..., \alpha_n)$. Posem $d = \text{disc}(\alpha_1, ..., \alpha_n)$. Com $\delta^2 = d$, es té que $dX_j = \delta\gamma_j$ és un enter algebraic, i per tant $dX_j = a_j \in \mathbb{Z}$. Ens falta provar que a_j^2 és divisible per d per cada $j \in \{1, ..., n\}$. Tenim

$$\frac{a_j^2}{d} = \frac{(\delta\gamma_j)^2}{d} = \gamma_j^2 \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$$

per tant, a_j^2 és divisible per d.

□

Per tant, hem provat que

$$\mathcal{O}_K \subset \frac{1}{d}A = \mathbb{Z}\frac{\alpha_1}{d} \oplus ... \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

Finalment, com que $\mathcal{O}_K$ conté i està contingut en un grup lliure abelià de rang n llavors $\mathcal{O}_K$ també és grup lliure abelià de rang n. I també, podem afirmar que les bases d'enters existeixen.

Totes les bases d'enters d'un mateix anell d'enters de cossos de nombres tenen el mateix discriminant. Vegem-ho:

Teorema 2.32. *Siguin $\{\omega_1, ..., \omega_n\}$ i $\{\beta_1, ..., \beta_n\}$ dues bases d'enters de $\mathcal{O}_K$. Aleshores,*

$$\text{disc}(\omega_1, ..., \omega_n) = \text{disc}(\beta_1, ..., \beta_n).$$

Demostració. Primer, escrivim la base $\{\omega_1, ..., \omega_n\}$ en funció de l'altra $\{\beta_1, ..., \beta_n\}$.

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

on M és una matriu sobre $\mathbb{Z}$ de dimensió $n \times n$.

Considerem els n embeddings de K en $\mathbb{C}$. Els apliquem en les n equacions anteriors i obtenim

$$[\sigma_j(\omega_i)]_{i,j=1,...,n} = M[\sigma_j(\beta_i)]_{i,j=1,...,n}$$

Prenent determinants i elevant-los al quadrat, tenim

$$\text{disc}(\omega_1, ..., \omega_n) = \det(M)^2 \text{disc}(\beta_1, ..., \beta_n).$$

Com que M és matriu sobre $\mathbb{Z}$, es compleix que $\det(M) \in \mathbb{Z}$. Per tant, $\text{disc}(\omega_1, ..., \omega_n)$ és divisible per $\text{disc}(\beta_1, ..., \beta_n)$ amb el mateix signe.

Fent el mateix però escrivint la base $\{\beta_1, ..., \beta_n\}$ en funció de $\{\omega_1, ..., \omega_n\}$, obtenim que $\text{disc}(\beta_1, ..., \beta_n)$ és divisible per $\text{disc}(\omega_1, ..., \omega_n)$

Per tant, podem concloure dient que

$$\text{disc}(\beta_1, ..., \beta_n) = \text{disc}(\omega_1, ..., \omega_n)$$

□

El teorema que acabem de donar ens permet definir el discriminant d'un cos de nombres sobre $\mathbb{Q}$.

Definició 2.33. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$. Sigui $\omega_1, ..., \omega_n$ una base d'enters. Siguin $\sigma_1, ..., \sigma_n$ els n embeddings de K en $\mathbb{C}$. Definim el discriminant de K per*

$$\text{disc}_K = \det([\sigma_i(\omega_j)]_{i,j=1,..,n})^2.$$

Hem vist que el discriminant serveix per demostrar l'existència de bases d'enters. Però té altres aplicacions com la identificació de bases d'enters. El teorema que es dona a continuació s'usarà per calcular l'anell d'enters dels cossos ciclotòmics. La prova d'aquest es pot trobar al capítol 2 de [1].

Teorema 2.34. *Siguin K i L dos cossos de nombres de grau n i m, respectivament, sobre $\mathbb{Q}$. Sigui $d = \text{mcd}(\text{disc}_K, \text{disc}_L)$. Suposem que $[KL : \mathbb{Q}] = nm$. Llavors,*

$$\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$$

Corol·lari 2.35. *En particular, si $[KL : \mathbb{Q}] = nm$ i $d = 1$, llavors $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.*

Donat un cos de nombres K, no sempre existeix una base d'enters de $\mathcal{O}_K$ de la forma $\{1, \alpha, ..., \alpha^{n-1}\}$ per a $\alpha \in K$, i per tant no tots els anells d'enters de cossos de nombres tenen la forma $\mathbb{Z}[\alpha]$.

2.5 Cossos ciclotòmics i cossos quadràtics

L'objectiu d'aquest apartat és donar l'anell d'enters corresponent als cossos ciclotòmics i el corresponent als cossos quadràtics.

Cossos quadràtics.

Sigui m un enter lliure de quadrats. El cos $\mathbb{Q}[\sqrt{m}]$ s'anomena cos quadràtic.

Teorema 2.36. *Sigui m enter lliure de quadrats. El conjunt d'enters algebraics en un cos quadràtic $\mathbb{Q}[\sqrt{m}]$ és*

$$\begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} | a, b \in \mathbb{Z}\} \text{ si } m \equiv 2 \text{ o } 3 (mod\ 4) \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{a+b\sqrt{m}}{2} | a, b \in \mathbb{Z}, a \equiv b (mod\ 2)\right\} \text{ si } m \equiv 1 (mod\ 4) \end{cases}$$

Demostració. Sigui $\alpha = r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$, on r, s són nombres racionals. Si $s \neq 0$, aleshores el polinomi mònic irreductible sobre $\mathbb{Q}$ que té α com arrel és $X^2 - 2rX + r^2 - ms^2$. Per tant, α és enter algebraic, si i només si, $2r$ i $r^2 - ms^2$ són nombres enters. I si $2r \in \mathbb{Z}$, llavors $r \in \mathbb{Z}$ o bé $r = k + 1/2$, per $k \in \mathbb{Z}$.

Per una banda, si $r \in \mathbb{Z}$ i $r^2 - ms^2 \in \mathbb{Z}$, llavors $ms^2 \in \mathbb{Z}$. Com que m és enter lliure de quadrats, tenim $s \in \mathbb{Z}$.

Per altra banda, suposem que $r = k + 1/2$ per algun $k \in \mathbb{Z}$. Tenim, doncs, que $r^2 = k^2 + k + 1/4$. Com que $r^2 - ms^2 \in \mathbb{Z}$ veiem que $1/4 - ms^2 \in \mathbb{Z}$ també. Posem $n = 1/4 - ms^2$ amb $n \in \mathbb{Z}$. Aleshores $4n = 1 - m(2s)^2$ i, per tant, $m(2s)^2 \in \mathbb{Z}$. Per ser m enter lliure de quadrats tenim que $2s \in \mathbb{Z}$. Aleshores, tenim dues possibilitats: $s \in \mathbb{Z}$, o bé $s = l + 1/2$ amb $l \in \mathbb{Z}$.

La primera opció no pot ser ja que tindríem $4n = 1 - 4s^2$ i reduint mòdul 4 ens quedaria $0 \equiv 1 (\text{mod } 4)$. I si $s = l + 1/2$ amb $l \in \mathbb{Z}$, aleshores $4n = 1 - m(2s)^2 = 1 - m(2l+1)^2$, és a dir, $1 - m(4l^2 + 4l + 1) = 4n$. Reduint la igualtat mòdul 4 ens queda que $m \equiv 1 (\text{mod } 4)$. En resum, suposant que $r = k + 1/2$ amb $k \in \mathbb{Z}$ tenim $s = l + 1/2$ per algun $l \in \mathbb{Z}$ i $m \equiv 1 (\text{mod } 4)$.

Finalment, obtenim que $\frac{1+\sqrt{m}}{2}$ és enter, si i només si, $m \equiv 1 (\text{mod } 4)$.

□

El discriminant de $\mathbb{Q}[\sqrt{m}]$ és

$$\text{disc}_{\mathbb{Q}[\sqrt{m}]} = \begin{cases} d & si \quad d \equiv 1(\text{mod } 4) \\ 4d & si \quad d \not\equiv 1(\text{mod } 4). \end{cases}$$

Cossos ciclotòmics.

Sigui $\omega = e^{2\pi i/m}$ l'arrel m-éssima primitiva de la unitat, on m és un enter lliure de quadrats. El cos $\mathbb{Q}[\omega]$ s'anomena m-éssim cos ciclotòmic. Tots els resultats que es donen a continuació poden trobar-se demostrats a [1].

Teorema 2.37. *Els conjugats de ω són els ω^k, per $k \in [1, m]$ tal que $(k, m) = 1$.*

Corol·lari 2.38. *El m-éssim cos ciclotòmic té grau $\varphi(m)$ sobre $\mathbb{Q}$, on φ és la funció d'Euler.*

Corol·lari 2.39. *El grup de Galois de $\mathbb{Q}[\omega]$ sobre $\mathbb{Q}$ és isomorf al grup multiplicatiu d'enters mòdul m. És a dir,*

$$\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^* = \{k \in \mathbb{Z} | k \in [1, m] \text{ tal que } (k, m) = 1\}.$$

Cada element $k \in (\mathbb{Z}/m\mathbb{Z})^*$ correspon a un automorfisme del grup de Galois de $\mathbb{Q}[\omega]$ sobre $\mathbb{Q}$ que envia ω a ω^k.

Volem estudiar com són els anells d'enters corresponents als cossos ciclotòmics per a m primer. Volem provar que l'anell d'enters corresponent al cos de nombres $K = \mathbb{Q}[\omega]$, on $\omega = e^{2\pi i/m}$, per algun m enter, és $\mathbb{Z}[\omega]$.

En el cas de $m = 2$, tenim $\omega = e^{2\pi i/2} = -1$. Per tant, el cos ciclòtomic és $\mathbb{Q}(-1) = \mathbb{Q}$ i el seu anell d'enters és $\mathbb{Z}$.

En el cas de $m \neq 2$, ho separem en dos resultats, el primer assumeix que m és una potència de primers i el segon que m no és potència de primers.

Teorema 2.40. *Sigui $\omega = e^{2\pi i/m}$, on $m = p^r$ per un primer p. Aleshores,*

$$\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega].$$

Per provar aquest teorema necessitem dos lemes.

Lema 2.41. *Per $m \geq 3$ enter, tenim*

$$\text{disc}(1 - \omega) = \text{disc}(\omega).$$

Demostració. Denotem per α_i als conjugats de ω, per a tot $1 \leq i \leq n$. Pel *Teorema 2.28* tenim

$$\text{disc}(\omega) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \prod_{1 \leq i < j \leq n} ((1 - \alpha_i) - (1 - \alpha_j))^2 = \text{disc}(1 - \omega)$$

on usem que $1 - \alpha_i$ són els conjugats de $1 - \omega$, per a tot $1 \leq i \leq n$.

□

Lema 2.42. *Per $m = p^r$ enter, tenim*

$$\prod_{\substack{1 \leq k \leq m \\ p \nmid k}} (1 - \omega^k) = p$$

Demostració.

Prenem

$$f(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + ... + X^{(p-1)p^{r-1}}$$

Llavors tot ω^k, per $k \in [1, m]$ tal que p no divideix k, són arrels de f, per ser arrels de $X^{p^r} - 1$ però no de $X^{p^{r-1}} - 1$. Per tant,

$$f(X) = \prod_{\substack{1 \leq k \leq m \\ p \nmid k}} (X - \omega^k)$$

ja que exactament hi ha $\varphi(p^r) = (p-1)p^{r-1}$ valors de k. Finalment, prenem $X = 1$.

□

Demostració del Teorema 2.40.

Denotem per $n = \varphi(p^r) = (p-1)p^{r-1}$ i $d = \text{disc}(\omega)$ que, pel *Lema 2.41* , és igual a $disc(1 - \omega)$. Pel *Teorema 2.31* tenim que tot element $\alpha \in \mathcal{O}_{\mathbb{Q}[\omega]}$ es pot escriure de la forma

$$\alpha = \frac{m_1 + m_2(1-\omega) + \cdots + m_n(1-\omega)^{n-1}}{d}$$

on $m_1, m_2, ..., m_n$ són nombres enters.

Volem provar que $\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[1 - \omega]$. Suposem el contrari, és a dir ha d'existir algun α pel qual no tot m_i és divisible per d. Tenim que $\mathcal{O}_{\mathbb{Q}[\omega]}$ conté un element de la forma

$$\beta = \frac{m_i(1-\omega)^{i-1} m_{i+1}(1-\omega)^i + \cdots + m_n(1-\omega)^{n-1}}{p}.$$

per algun $i \leq n$ i l'enter m_i no és divisible per p. Pel *Lema 2.42* tenim

$$\prod_{\substack{1 \leq k \leq m \\ p \nmid k}} (1 - \omega^k) = p$$

i per ser $1 - \omega^k$ divisible per $1 - \omega$, llavors $\frac{p}{(1-\omega)^n} \in \mathbb{Z}[\omega]$. Aleshores, $\frac{p}{(1-\omega)^i} \in \mathbb{Z}[\omega]$, i per tant, $\frac{\beta p}{(1-\omega)^i} \in \mathcal{O}_{\mathbb{Q}[\omega]}$. Això significa que $\frac{m_i}{1-\omega} \in \mathcal{O}_{\mathbb{Q}[\omega]}$.

Prenent la norma de $\mathbb{Q}[\omega]$, tenim $N(1-\omega)|N(m_i)$, però és impossible ja que $N(m_i) = m_i^n$, i pel segon lema tenim $N(1-\omega) = p$.

□

Teorema 2.43. *Sigui $\omega = e^{2\pi i/m}$, on m no és potència d'un primer. Aleshores,*

$$\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega].$$

Demostració. Fem inducció sobre el nombre de primers diferents en que es descompon m, denotem-lo per n. Comencem fent el cas $n = 2$: sigui $m = m_1 m_2$, on m_1 i m_2 són potències de primers que satisfan $\text{mcd}(m_1, m_2) = 1$. Denotem per $\omega_1 = e^{2\pi i/m_1}$ i $\omega_2 = e^{2\pi i/m_2}$. Suposem que $\mathcal{O}_{\mathbb{Q}(\omega_1)} = \mathbb{Z}[\omega_1]$ i $\mathcal{O}_{\mathbb{Q}(\omega_2)} = \mathbb{Z}[\omega_2]$. Tenim que $\omega^{m_1} = e^{2\pi i m_1/m} = e^{2\pi i/m_2} = \omega_2$ i $\omega^{m_2} = e^{2\pi i m_2/m} = e^{2\pi i/m_1} = \omega_1$. La Identitat de Bézout afirma que si dos nombres enters m_1 i m_2 són coprimers, llavors existeixen dos enters r i s tal que $rm_1 + sm_2 = 1$. Per tant,

$$\omega = e^{2\pi i/(m_1 m_2)} = e^{(2\pi i)(rm_1+sm_2)/(m_1 m_2)} = e^{2\pi i r/m_1 + 2\pi i s/m_2} = \omega_1^r \omega_2^s.$$

Per tant, $\mathbb{Q}[\omega] = \mathbb{Q}[\omega_1^r \omega_2^s] = \mathbb{Q}[\omega_1]\mathbb{Q}[\omega_2]$. Com que

$$[\mathbb{Q}[\omega_1]\mathbb{Q}[\omega_2] : \mathbb{Q}] = [\mathbb{Q}[\omega_1] : \mathbb{Q}][\mathbb{Q}[\omega_2] : \mathbb{Q}] = \varphi(m_1)\varphi(m_2) = \varphi(m),$$

per ser m_1 i m_2 coprimers, llavors pel *Corol·lari 2.35*, obtenim que $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathcal{O}_{\mathbb{Q}(\omega_1)}\mathcal{O}_{\mathbb{Q}(\omega_2)}$. És a dir,

$$\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega_1]\mathbb{Z}[\omega_2] = \mathbb{Z}[\omega].$$

Ara, suposem que és cert per $n-1$ i ho provem per n. Posem $m = m_1 \cdots m_n$, on $m_1, ..., m_n$ són potències de primers que satisfan $\text{mcd}(m_1, ..., m_n) = 1$. Per a tot $i \in \{1, ..., n\}$, denotem per $\omega_i = e^{2\pi i/m_i}$, i pel *Teorema 2.40* tenim $\mathcal{O}_{\mathbb{Q}(\omega_i)} = \mathbb{Z}[\omega_i]$. Per la Identitat de Bézout afirmem que existeixen $r_1, ..., r_n$ nombres enters tals que $r_1 m_1 + \cdots + r_n m_n = 1$. Per tant,

$$\omega = e^{2\pi i/m_1 \cdots m_n} = e^{2\pi i r_1/m_1 + \cdots + 2\pi i r_n/m_n} = \omega_1^{r_1} \cdots \omega_n^{r_n}$$

Per tant, $\mathbb{Q}[\omega] = \mathbb{Q}[\omega_1^{r_1} \cdots \omega_n^{r_n}] = \mathbb{Q}[\omega_1 \cdots \omega_{n-1}]\mathbb{Q}[\omega_n]$. Com que

$$[\mathbb{Q}[\omega] : \mathbb{Q}] = \varphi(m_1) \cdots \varphi(m_n) = \varphi(m)$$

per ser $m_1, ..., m_n$ coprimers, llavors pel *Corol·lari 2.35*, obtenim que

$$\mathcal{O}_{\mathbb{Q}[\omega]} = \mathcal{O}_{\mathbb{Q}[\omega_1 \cdots \omega_{n-1}]}\mathcal{O}_{\mathbb{Q}[\omega_n]}.$$

Per hipòtesi d'inducció tenim que $\mathcal{O}_{\mathbb{Q}[\omega_1 \cdots \omega_{n-1}]} = \mathbb{Z}[\omega_1 \cdots \omega_{n-1}]$, i pel *Teorema 2.40* tenim que $\mathcal{O}_{\mathbb{Q}[\omega_n]} = \mathbb{Z}[\omega_n]$ llavors

$$\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega_1 \cdots \omega_{n-1}]\mathbb{Z}[\omega_n] = \mathbb{Z}[\omega].$$

□

Finalment, calculem el discriminant del cos de nombres $\mathbb{Q}(\omega)$, on $\omega = e^{2\pi i/p}$ per algun p enter primer.

Teorema 2.44. *Sigui p enter primer. El discriminant del cos de nombres $\mathbb{Q}(\omega)$, on $\omega = e^{2\pi i/p}$, és*

$$\text{disc}_{\mathbb{Q}(\omega)} = \pm p^{p-2}.$$

Demostració. Com hem vist abans $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$, això significa que existeix una base d'enters de $\mathbb{Q}(\omega)$ de la forma $\{1, \omega, ..., \omega^{p-1}\}$. Aleshores, pel *Teorema 2.28* tenim que el $\text{disc}(1, \omega, ..., \omega^{p-1}) = \pm N^{\mathbb{Q}(\omega)}(\phi_p'(\omega))$, on ϕ és el polinomi mínim de $\omega = e^{2\pi i/p}$ que en el cas de p primer és de la forma:

$$\phi_p(X) = \frac{X^p - 1}{X - 1}.$$

Fem la derivada $\phi_p'(X) = \frac{(X-1)pX^{p-1}-(X^p-1)}{(X-1)^2}$, i llavors $\phi_p'(\omega) = \frac{-p\omega^{p-1}}{1-\omega}$. Aleshores,

$$\pm N(\phi_p'(\omega)) = \pm N\left(\frac{-p\omega^{p-1}}{1-\omega}\right) = \pm\frac{N(-p)N(\omega)^{p-1}}{N(1-\omega)} = \pm\frac{(-p)^{p-1}}{p} = \pm p^{p-2}.$$

Per tant, tenim $\mathrm{disc}_{\mathbb{Q}(\omega)} = \pm p^{p-2}$.

□

3 Cossos de nombres de Galois

3.1 Descomposició de primers en anells d'enters de cossos de nombres.

A continuació estudiarem com els nombres enters primers es converteixen en ideals en l'anell d'enters corresponent. Donarem una sèrie de definicions bàsiques per poder introduir la teoria de ramificació d'ideals primers. La majoria de resultats d'aquest apartat no estan demostrats ja que es considera que és més important entendre la construcció de l'automorfisme de Frobenius. Si el lector vol consultar les proves que falten, pot trobar-les en el capítol 3 de [1].

Definició 3.1. *Sigui K un cos de nombres. Un ideal $\mathfrak{a}$ de $\mathcal{O}_K$ és un subconjunt no buit de $\mathcal{O}_K$ que compleix:*

1) Siguin $a, b \in \mathfrak{a}$, llavors $a + b \in \mathfrak{a}$

2) Siguin $a \in \mathfrak{a}$ i $r \in \mathcal{O}_K$, llavors $ra \in \mathfrak{a}$.

Definició 3.2. *Sigui $\mathfrak{p}$ un ideal de $\mathcal{O}_K$. Direm que $\mathfrak{p}$ és un ideal primer si no és igual a $\mathcal{O}_K$ i si per a qualsevol $a, b \in \mathcal{O}_K$ tal que $ab \in \mathfrak{p}$ es té que $a \in \mathfrak{p}$ o bé $b \in \mathfrak{p}$.*

Definició 3.3. *Sigui $\mathfrak{p}$ un ideal de $\mathcal{O}_K$. Direm que $\mathfrak{p}$ és un ideal maximal si no existeix cap ideal $\mathfrak{b}$ tal que $\mathfrak{a} \subsetneqq \mathfrak{b} \subsetneqq \mathcal{O}_K$.*

El *Teorema Fonamental de l'Aritmètica* afirma que:

"Qualsevol enter positiu major que 1 pot escriure's de forma única com a producte de potències de nombres primers."

En aquest cas, el generalitzarem per a qualsevol cos de nombres.

Teorema 3.4. *(Teorema Fonamental de l'Aritmètica) Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Llavors, cada ideal no zero de $\mathcal{O}_K$ es pot escriure com a producte d'ideals primers de manera única llevat reordenacions dels factors.*

Volem resoldre el problema de determinar com un ideal primer no zero es factoritza en un anell d'enters donat. Tots els ideals primers que tractarem en aquesta secció són diferents del trivial tot i que no s'especifiqui.

Definició 3.5. *Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Sigui L un cos de nombres tal que $K \subset L$. Donat $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$. L'ideal que es genera per $\mathfrak{p}$ en l'anell de nombres $\mathcal{O}_L$ és*

$$\mathfrak{p}\mathcal{O}_L = \{\alpha_1\beta_1 + ...\alpha_r\beta_r | \alpha_i \in \mathfrak{p}, \beta_i \in \mathcal{O}_L\}.$$

Observació 3.6. Si $\mathfrak{p}$ és un ideal principal, és a dir que està generat per un sol element α tal que $\mathfrak{p} = (\alpha)$, llavors tenim que

$$\mathfrak{p}\mathcal{O}_L = \{\alpha\beta | \beta \in \mathcal{O}_L\}.$$

Teorema 3.7. *Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Sigui L un cos de nombres tal que $K \subset L$. Considerem un ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$ i un ideal primer $\mathfrak{q}$ de $\mathcal{O}_L$. Aleshores, es diu que $\mathfrak{q}$ està a sobre de $\mathfrak{p}$ si es compleix alguna de les següents condicions, totes elles equivalents.*

1) $\mathfrak{q}$ *divideix a* $\mathfrak{p}\mathcal{O}_L$.

2) $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$.

3) $\mathfrak{p} \subset \mathfrak{q}$.

4) $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

Teorema 3.8. *Cada ideal primer* $\mathfrak{q}$ *de* $\mathcal{O}_L$ *està a sobre d'un únic ideal primer* $\mathfrak{p}$ *de* $\mathcal{O}_K$.

Donada una extensió $K \subset L$ de cossos de nombres . Els ideals primers de $\mathcal{O}_L$ que es troben a sobre d'un ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$ són els que es troben en $\mathfrak{p}\mathcal{O}_L$. A més, com que $\mathfrak{p}\mathcal{O}_L$ és un ideal de $\mathcal{O}_L$, pel *Teorema Fonamental de l'Aritmètica*, tenim que es factoritza de manera única per $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, on $\mathfrak{p}_1, ..., \mathfrak{p}_g$ són ideals primers de $\mathcal{O}_L$.

Definició 3.9. *Els exponents* $e_1, ..., e_g$ *es diuen índexs de ramificació de* $\mathfrak{p}$ *en* L.

Definició 3.10. *Direm índex de descomposició de* $\mathfrak{p}$ *en* L *a* g, *que és el nombre d'ideals primers diferents en què es factoriza* $\mathfrak{p}\mathcal{O}_L$.

Suposem que $\mathfrak{q}$ es troba a sobre $\mathfrak{p}$, com que els dos ideals són maximals podem afirmar que $\mathcal{O}_K/\mathfrak{p}$ i $\mathcal{O}_L/\mathfrak{q}$ són cossos.

La inclusió $\mathcal{O}_K \subset \mathcal{O}_L$ indueix un morfisme d'anells $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{q}$ i, per tant el seu nucli és $\mathcal{O}_K \cap \mathfrak{q}$. Sabem que $\mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$ pel *Teorema 3.7.* Aleshores, obtenim un embedding

$$\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{q}.$$

Definició 3.11. *Si els cossos* $\mathcal{O}_K/\mathfrak{p}$ *i* $\mathcal{O}_L/\mathfrak{q}$ *són de dimensió finita, llavors* $\mathcal{O}_L/\mathfrak{q}$ *és una extensió de* $\mathcal{O}_K/\mathfrak{p}$ *de grau finit. Aquest s'anomena grau d'inèrcia de* $\mathfrak{q}$ *sobre* $\mathfrak{p}$.

Sabem que el cardinal de $\mathcal{O}_L/\mathfrak{q}$ és $N(\mathfrak{q})$.

Teorema 3.12. *Sigui* $K \subset L$ *una extensió de cossos de nombres de grau finit* n. *Sigui* $\mathfrak{p}$ *un ideal de* $\mathcal{O}_K$. *Siguin* $\mathfrak{p}_1, ..., \mathfrak{p}_g$ *els ideals primers diferents de* $\mathcal{O}_L$ *en els quals factoritza* $\mathfrak{p}\mathcal{O}_L$. *Siguin* $e_1, ..., e_g$ *els seus índexs de ramificació i* $f_1, ..., f_g$ *els graus d'inèrcia corresponents. Llavors,*

$$n = e_1 f_1 + ... + e_g f_g.$$

Definició 3.13. *Sigui* K *un cos de nombres i* $\mathcal{O}_K$ *el seu anell d'enters. Sigui* L *una extensió de* K *de dimensió* n, *i denotem per* $\mathcal{O}_L$ *al seu anell d'enters.*

1) Un ideal primer $\mathfrak{p}$ *de* $\mathcal{O}_K$ *ramifica en* $\mathcal{O}_L$, *si i només si, l'índex de ramificació* e *de* $\mathfrak{q}$ *en* K *és major que 1, per algun primer* $\mathfrak{q}$ *de* $\mathcal{O}_L$ *que es troba a sobre de* $\mathfrak{p}$.

2) Un ideal primer $\mathfrak{p}$ *de* $\mathcal{O}_K$ *és totalment ramificat en* $\mathcal{O}_L$ *si* $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^n$, *per un primer* $\mathfrak{q}$ *de* $\mathcal{O}_L$ *que es troba a sobre de* $\mathfrak{p}$.

3) Un ideal primer $\mathfrak{p}$ *de* $\mathcal{O}_K$ *és inert en* $\mathcal{O}_L$ *si* $\mathfrak{p}\mathcal{O}_L$ *és un ideal primer de l'anell* $\mathcal{O}_L$.

Teorema 3.14. *Sigui* K *un cos de nombres i* $\mathcal{O}_K$ *el seu anell d'enters. Sigui* p *un primer enter. Aleshores* p *ramifica en* $\mathcal{O}_K$, *si i només si,* $p|\mathrm{disc}_K$.

3.2 Automorfisme de Frobenius.

L'objectiu del nostre treball és el *Teorema de Chebotarev* que tracta extensions de Galois. Per això ens serà útil aplicar la teoria de Galois a la descomposició de primers en anells d'enters de cossos de nombres.

Donem la definició d'una extensió de Galois de cossos, i la de grup de Galois.

Definició 3.15. *Siguin K i L cossos. Direm que $K \subset L$ és una extensió de Galois si és una extensió normal i separable.*

Definició 3.16. *Siguin K i L cossos tal que $K \subset L$ és extensió de Galois. S'anomena grup de Galois de L sobre K al grup d'automorfismes de L que deixen fixe a tot element de K. L'operació del grup és la composició. Es denota per* $\mathrm{Gal}(L/K)$.

Donada una extensió normal, el seu grup de Galois permuta transitivament els ideals primers que es troben a sobre un mateix ideal primer. Vegem-ho:

Teorema 3.17. *Siguin K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Sigui L una extensió normal de K. Siguin $\mathfrak{q}$ i $\mathfrak{q}'$ dos ideals primers de $\mathcal{O}_L$ a sobre del mateix primer $\mathfrak{p}$ de $\mathcal{O}_K$. Llavors, $\sigma(\mathfrak{q}) = \mathfrak{q}'$, per algun $\sigma \in \mathrm{Gal}(L/K)$.*

Demostració. Suposem el contrari del que volem provar, és a dir suposem que $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ per a tot $\sigma \in \mathrm{Gal}(L/K)$. Pel *Teorema Xinès del Residu*, existeix una solució del sistema de congruències

$$\begin{cases} X \equiv 0 (\mathrm{mod}\ \mathfrak{q}') \\ X \equiv 1 (\mathrm{mod}\ \sigma(\mathfrak{q})), \text{per a tot } \sigma \in \mathrm{Gal}(L/K). \end{cases}$$

Denotem la solució per $\alpha \in \mathcal{O}_L$, aleshores tenim que

$$N_K^L(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$$

té un factor que és $\alpha \in \mathfrak{q}'$. Per tant, $N_K^L(\alpha) \in \mathcal{O}_K \cap \mathfrak{q}' = \mathfrak{p}$.

A més, sabem que existeix almenys un $\sigma \in \mathrm{Gal}(L/K)$ tal que $\alpha \notin \sigma(\mathfrak{q})$ i per tant, $\sigma^{-1}(\alpha) \notin \mathfrak{q}$. Doncs, podem expressar la norma de la següent forma

$$N_K^L(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}(\alpha)$$

i com que no tots pertanyen a $\mathfrak{q}$ llavors $N_K^L(\alpha) \notin \mathfrak{q}$. Però això es contradiu amb el que havíem vist que $N_K^L(\alpha) \in \mathfrak{p} \subset \mathfrak{q}$.

□

Corol·lari 3.18. *Sigui L una extensió normal sobre K. Llavors, els índexs de ramificació i els graus d'inèrcia de dos ideals primers $\mathfrak{q}$ i $\mathfrak{q}'$ de $\mathcal{O}_L$ que estan a sobre del mateix primer $\mathfrak{p}$ de $\mathcal{O}_K$, són iguals.*

Observació 3.19. A més, pel *Teorema 3.12* es té que $[L : K] = efg$.

A partir d'aquí, considerem un cos de nombres K i una extensió L de Galois de K. Denotarem per $G = \mathrm{Gal}(L/K)$. Definirem dos subgrups de G per poder entendre la definició de l'element de Frobenius.

Definició 3.20. *Sigui $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$. Per cada ideal primer $\mathfrak{q}$ de $\mathcal{O}_L$ que es troba a sobre de $\mathfrak{p}$, definim el grup de descomposició de $\mathfrak{q}$ sobre K per*

$$D_{\mathfrak{q}} = \{\sigma \in G | \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Proposició 3.21. *El grup de descomposició té ordre ef.*

Demostració. Com que els elements del grup de descomposició de $\mathfrak{q}$ sobre K satisfan que, per $\sigma \in G$, $\sigma(\mathfrak{q}) = \mathfrak{q}$, llavors podem dir que $D_\mathfrak{q}$ és l'estabilitzador de $\mathfrak{q}$ per l'acció de G. L'òrbita de $\mathfrak{q}$ és el conjunt $\{\sigma(\mathfrak{q})|\sigma \in G\}$, i pel *Teorema 3.17* sabem que G actua transitivament i per tant l'òrbita té cardinal g. Tenint en compte l'*Observació 3.19* que afirma $[L : K] = efg$, llavors $\#D_\mathfrak{q} = ef$.

□

Definició 3.22. *Sigui $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$. Per cada ideal primer $\mathfrak{q}$ de $\mathcal{O}_L$ que es troba a sobre de $\mathfrak{p}$, definim el grup d'inèrcia de $\mathfrak{q}$ sobre K com*

$$I_\mathfrak{q} = \{\sigma \in G|\sigma(X) \equiv X(mod\ \mathfrak{q}), \quad \forall X \in \mathcal{O}_L\}.$$

Observació 3.23. L'expressió $\sigma(\mathfrak{q}) = \mathfrak{q}$ pot escriure's, també, de la forma

$$\sigma(X) \equiv 0(\text{mod } \mathfrak{q}), \text{ si i només si, } X \equiv 0(\text{mod } \mathfrak{q}).$$

Per això, sabem que $I_\mathfrak{q} \subset D_\mathfrak{q}$.

Donat un primer $\mathfrak{p}$ de $\mathcal{O}_K$, siguin $\mathfrak{q}_1, ..., \mathfrak{q}_g$ ideals primers de $\mathcal{O}_L$ que es troben a sobre de $\mathfrak{p}$. Pel *Teorema 3.17*, G actua transitivament en el conjunt $\{\mathfrak{q}_1, ..., \mathfrak{q}_g\}$, i per tant els grups de descomposició de $\mathfrak{q}_1, ..., \mathfrak{q}_g$ sobre K són conjugats en G.

Sigui $\mathfrak{q}$ de $\mathcal{O}_L$ sobre $\mathfrak{p}$. Sigui σ un element del grup de descomposició $D_\mathfrak{q}$ de $\mathfrak{q}$ sobre K. El restringim a $\mathcal{O}_L$, $\sigma_{|\mathcal{O}_L} : \mathcal{O}_L \to \mathcal{O}_L$.

Reduïm l'automorfisme $\sigma_{|\mathcal{O}_L}$ mòdul $\mathfrak{q}$ i obtenim: $\bar{\sigma} : \mathcal{O}_L/\mathfrak{q} \to \mathcal{O}_L/\mathfrak{q}$.

Definició 3.24. *Es diu que $\mathbb{F}_\mathfrak{q} = \mathcal{O}_L/\mathfrak{q}$ és el cos residual de l'ideal $\mathfrak{q}$ de $\mathcal{O}_L$.*

Sabem que els automorfismes $\sigma \in \text{Gal}(L/K)$ deixen fixe a tot element de K (i per tant, $\sigma_{|\mathcal{O}_L}$ fixa a tot element de $\mathcal{O}_K$), llavors els automorfismes $\bar{\sigma}$ deixen fixe tot element del subcòs $\mathcal{O}_K/\mathfrak{p}$. Per tant, $\bar{\sigma} \in \text{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. Això defineix un morfisme de grups:

$$\phi : D_\mathfrak{q} \to \text{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}).$$

És fàcil comprovar que ϕ és morfisme de grups, ja que la composició d'automorfismes de $D_\mathfrak{q}$ correspon a la composició en $\text{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$

Proposició 3.25. *La aplicació $\phi : D_\mathfrak{q} \to \text{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ és exhaustiva.*

Demostració. Si $t \in \mathcal{O}_L$ denotarem per $\bar{t} \in \mathbb{F}_\mathfrak{q}$ la seva classe mòdul $\mathfrak{q}$. Donat $\tau \in \text{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$, volem provar que per algun $\sigma \in \text{Gal}(L/K)$ es satisfà

$$\overline{\sigma(X)} = \tau(\overline{X})$$

per a qualsevol $X \in \mathcal{O}_L$. Això significa que $\sigma(\mathfrak{q}) = \mathfrak{q}$, és a dir σ pertany al grup de descomposició de $\mathfrak{q}$, i que $\phi(\sigma) = \tau$.

Per ser $\mathcal{O}_L$ un subanell finitament generat de $\mathcal{O}_K$, existeixen enters algebraics $\omega_1, ..., \omega_n$ de L tals que podem escriure qualsevol element de l'anell d'enters de L de la forma $\sum_{j=1}^n \alpha_j\omega_j$, per $\alpha_j \in \mathcal{O}_K$.

Considerem el polinomi

$$P(Y, X_1, ..., X_n) = \prod_{\sigma \in G} (Y - \sigma(\omega_1)X_1 - \cdots - \sigma(\omega_n)X_n)$$

que pertany a $\mathcal{O}_L[Y, X_1, ..., X_n]$. Els coeficients del polinomi P pertanyen a $\mathcal{O}_L \cap K = \mathcal{O}_K$.

Avaluem per $Y = \omega_1 X_1 + \cdots + \omega_n X_n$ en el polinomi P i ens queda:

$$P(\omega_1 X_1 + \cdots + \omega_n X_n, X_1, ..., X_n) = \prod_{\sigma \in G} ((\omega_1 - \sigma(\omega_1))X_1 + \cdots + (\omega_n - \sigma(\omega_n))X_n) = 0.$$

Si ho reduïm mòdul $\mathfrak{q}$, en $\mathbb{F}_\mathfrak{q}[X_1, ..., X_n]$, obtenim:

$$\overline{P}(\overline{\omega_1} X_1 + \cdots + \overline{\omega_n} X_n, X_1, ..., X_n) = \overline{0}.$$

Si estenem $\tau \in \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}))$ en $\mathbb{F}_\mathfrak{q}[X_1, ..., X_n]$, i ho apliquem a banda i banda de la igualtat anterior, llavors:

$$\overline{P}(\tau(\overline{\omega_1}) X_1 + \cdots + \tau(\overline{\omega_n}) X_n, X_1, ..., X_n) = \overline{0}.$$

Per tant,

$$\prod_{\sigma \in G} ((\tau(\overline{\omega_1}) - \overline{\sigma(\omega_1)})X_1 + \cdots + ((\tau(\overline{\omega_n}) - \overline{\sigma(\omega_n)})X_n = \overline{0}.$$

Aleshores, un dels factors del producte ha de ser 0, per ser $\mathbb{F}_\mathfrak{q}[X_1, ..., X_n]$ un domini. Per tant, existeix algun $\sigma \in G$ tal que $\overline{\sigma(\omega_j)} = \tau(\overline{\omega_j})$, per a tot $j \in \{1, ..., n\}$.

□

El nucli de ϕ és el grup d'inèrcia de $\mathfrak{q}$ sobre K (i.e. $\mathrm{Ker}(\phi) = I_\mathfrak{q}$). Per tant, $I_\mathfrak{q}$ és subgrup normal de $D_\mathfrak{q}$. Llavors, $D_\mathfrak{q}/I_\mathfrak{q} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$.

El grup de Galois $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ és un grup cíclic d'ordre f generat per l'automorfisme $x \mapsto x^{N(\mathfrak{p})}$. Per tant, per l'isomorfisme que abans hem definit, $D_\mathfrak{q}/I_\mathfrak{q}$ també ho és.

Posem $K = \mathbb{Q}$, i per tant $\mathcal{O}_K = \mathbb{Z}$. Considerem un nombre primer p i un ideal $\mathfrak{q}$ de $\mathcal{O}_L$ a sobre p. Si $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ el veim com a subcós de $\mathbb{F}_\mathfrak{q} \cong \mathbb{F}_{p^f}$, llavors tindrem un isomorfisme $\phi : D_\mathfrak{q}/I_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_p)$. Es satisfà que

$$\begin{gathered} \phi(\sigma) : \mathbb{F}_\mathfrak{q} \to \mathbb{F}_\mathfrak{q} \\ X + \mathfrak{q} \mapsto \phi(\sigma)(X + \mathfrak{q}) = \sigma(X) + \mathfrak{q}. \end{gathered}$$

Definició 3.26. *Sigui L/K una extensió de Galois. Sigui $\mathfrak{p}$ ideal primer de $\mathcal{O}_K$ que no ramifica a l'extensió L/K. Sigui $\mathfrak{q}$ un ideal primer de $\mathcal{O}_L$ a sobre de $\mathfrak{p}$. L'element de Frobenius de $\mathfrak{q}$ sobre $\mathfrak{p}$,* $\mathrm{Frob}_\mathfrak{q}$*, és l'element del grup de descomposició $D_\mathfrak{q}$ que satisfà*

$$\mathrm{Frob}_\mathfrak{q}(X) \equiv X^{N(\mathfrak{p})} (mod\ \mathfrak{q}) \quad \text{per a tot } X \in \mathcal{O}_L.$$

Observació 3.27. Podem assegurar que és únic l'element de Frobenius, ja que quan $\mathfrak{q}$ és no ramificat aleshores $I_\mathfrak{q} = \{1\}$. Si $\mathfrak{p}$ ramifica llavors no podem assegurar la unicitat de l'element de Frobenius de $\mathfrak{q}$ sobre $\mathfrak{p}$.

Proposició 3.28. *Sigui L/K una extensió de Galois. Sigui $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$ que no ramifica a l'extensió L/K. Sigui $\mathfrak{q}$ un ideal primer de $\mathcal{O}_L$ que es troba a sobre de $\mathfrak{p}$. Per a tot ideal primer $\mathfrak{q}'$ de $\mathcal{O}_L$ que es troba a sobre de $\mathfrak{p}$, els elements de Frobenius* $\mathrm{Frob}_\mathfrak{q}$ *i* $\mathrm{Frob}_{\mathfrak{q}'}$ *són conjugats en el grup de Galois de L/K.*

Demostració. Denotem per $G = \mathrm{Gal}(L/K)$. Pel *Teorema 3.17* tenim que G permuta transitivament els ideals primers que es troben a sobre d'un mateix ideal primer. Considerem $\sigma \in G$ tal que $\mathfrak{q}' = \sigma(\mathfrak{q})$. Per a tot $X \in \mathcal{O}_L$ tenim, per definició de l'element de Frobenius de $\mathfrak{q}$ sobre $\mathfrak{p}$, que

$$\mathrm{Frob}_{\mathfrak{q}}(X) \equiv X^{N(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{q}).$$

Apliquem σ a banda i banda, i obtenim:

$$\sigma(\mathrm{Frob}_{\mathfrak{q}}(X)) \equiv \sigma(X^{N(\mathfrak{p})}) (\mathrm{mod}\ \sigma(\mathfrak{q})).$$

És a dir,

$$\sigma \mathrm{Frob}_{\mathfrak{q}}(X) \equiv \sigma(X)^{N(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{q}').$$

Reemplacem X per $\sigma^{-1}(X)$, i tenim que:

$$\sigma \mathrm{Frob}_{\mathfrak{q}}(\sigma^{-1}(X)) \equiv \sigma(\sigma^{-1}(X))^{N(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{q}')$$

per tant, ens queda:

$$(\sigma \mathrm{Frob}_{\mathfrak{q}} \sigma^{-1})(X) \equiv X^{N(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{q}')$$

Per la unicitat de l'element de Frobenius $\mathrm{Frob}_{\mathfrak{q}'}$ tenim $\mathrm{Frob}_{\mathfrak{q}'} = \sigma \mathrm{Frob}_{\mathfrak{q}} \sigma^{-1}$ que és el que volíem demostrar.

□

Observació 3.29. Quan G és abelià, tenim que $\mathrm{Frob}_{\mathfrak{q}}$ només depèn de $\mathfrak{p}$ i podem dir que

$$\mathrm{Frob}_{\mathfrak{q}}(X) \equiv X^{N(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{p}\mathcal{O}_L), \quad \text{per a tot } X \in \mathcal{O}_L.$$

Això es satisfà ja que, per cada $\sigma \in G$, $\mathrm{Frob}_{\mathfrak{q}'} = \sigma\, \mathrm{Frob}_{\mathfrak{q}}\, \sigma^{-1} = \sigma\sigma^{-1}\, \mathrm{Frob}_{\mathfrak{q}} = \mathrm{Frob}_{\mathfrak{q}}$, i tots els primers que es trobin a sobre de $\mathfrak{p}$ també tindran aquesta forma.

Observació 3.30. Seguint en el cas particular, $K = \mathbb{Q}$. Sigui p primer racional i sigui $\mathfrak{q}$ ideal primer de $\mathcal{O}_L$ a sobre p. Un element de Frobenius de $\mathfrak{q}$ sobre p és un element $\mathrm{Frob}_{\mathfrak{q}}$ del grup de descomposició $D_{\mathfrak{q}}$ que satisfà

$$\mathrm{Frob}_{\mathfrak{q}}(X) \equiv X^{p} (\mathrm{mod}\ \mathfrak{q}) \quad \text{per a tot } X \in \mathcal{O}_L.$$

Si p no ramifica en L, aleshores l'element de Frobenius és l'únic automorfisme de $D_{\mathfrak{q}}$ que ho satisfà. A més, es compleix que

$$D_{\mathfrak{q}} \cong \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p).$$

3.3 Exemples: cossos ciclotòmics i cossos quadràtics.

En aquest apartat estudiarem els elements de Frobenius en el cas dels cossos ciclotòmics i quadràtics, i també altres propietats de ramificació. És una continuació de l'apartat 2.5.

Cossos quadràtics.

Estudiarem com els nombres enters primers factoritzen en els cossos quadràtics. Sigui m un enter lliure de quadrats, posem $K = \mathbb{Q}$ i $L = \mathbb{Q}(\sqrt{m})$. Denotem per $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ a l'anell d'enters corresponent a $\mathbb{Q}(\sqrt{m})$, el discriminant del qual és

$$\mathrm{disc}_{\mathbb{Q}[\sqrt{m}]} = \begin{cases} m & si \quad m \equiv 1 (\mathrm{mod}\ 4) \\ 4m & si \quad m \not\equiv 1 (\mathrm{mod}\ 4). \end{cases}$$

I una base d'enters és

$$\begin{cases} \{1, (1+\sqrt{m})/2\} \text{ si } m \equiv 1 (\text{mod } 4) \\ \{1, \sqrt{m}\} \text{ si } m \not\equiv 1 (\text{mod } 4). \end{cases}$$

Sigui p un enter primer. Com que $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$, tenint en compte el *Teorema 3.12*, l'ideal generat per p en $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ és

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathfrak{p}^2, \text{ si el grau d'inèrcia de } \mathfrak{p} \text{ sobre } p \text{ és } 1 \\ \mathfrak{p}, \text{ si el grau d'inèrcia de } \mathfrak{p} \text{ sobre } p \text{ és } 2 \\ \mathfrak{p}_1\mathfrak{p}_2, \text{ si el grau d'inèrcia de } \mathfrak{p}_1 \text{ i } \mathfrak{p}_2 \text{ sobre } p \text{ és } 1. \end{cases}$$

Teorema 3.31. *1)Si p divideix m, llavors $p\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = (p, \sqrt{m})^2$.*

2) Si $p = 2$, llavors

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} (2, 1+\sqrt{m})^2 \text{ si } m \equiv 3 (\text{mod } 4) \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) \text{ si } m \equiv 1 (\text{mod } 8) \\ \text{és primer si } m \equiv 5 (\text{mod } 8). \end{cases}$$

3) Si p és imparell i p no divideix m, llavors

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} (p, n+\sqrt{m})(p, n-\sqrt{m}) \text{ si } n \text{ és una solució de } m \equiv X^2 (\text{mod } p) \\ \text{és primer si l'equació } m \equiv X^2 (\text{mod } p) \text{ no té solució.} \end{cases}$$

Demostració. En aquesta demostració denotarem per $\mathcal{O}$ a l'anell $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

Com que la factorització en producte d'ideals primers és única, llavors si $p\mathcal{O}$ conté el producte de dos ideals $\mathfrak{p}$ i $\mathfrak{q}$ aleshores $\mathfrak{pq} = p\mathcal{O}$.

Si p divideix a m llavors $(p\mathcal{O} + \sqrt{m}\mathcal{O})^2 = p^2\mathcal{O} + p\sqrt{m}\mathcal{O} + m\mathcal{O} \subset p\mathcal{O}$.

Suposem que $m \equiv 3 (\text{mod } 4)$, és a dir $m = 3 + 4t$. Aleshores,

$$(2\mathcal{O} + (1+\sqrt{m})\mathcal{O})^2 = 4\mathcal{O} + 2(1+\sqrt{m})\mathcal{O} + 2\sqrt{m} \subset 2\mathcal{O}.$$

Suposem que $m \equiv 1 (\text{mod } 4)$, llavors $\frac{1+\sqrt{m}}{2}$ i $\frac{1-\sqrt{m}}{2}$ pertanyen a $\mathcal{O}$. Sigui

$$\mathfrak{p} = 2\mathcal{O} + \frac{1+\sqrt{m}}{2}\mathcal{O} \text{ i } \mathfrak{q} = 2\mathcal{O} + \frac{1-\sqrt{m}}{2}\mathcal{O}$$

aleshores $\mathfrak{pq} = 4\mathcal{O} + (1+\sqrt{m})\mathcal{O} + (1-\sqrt{m})\mathcal{O} + t\mathcal{O}$.

Si t no és parell, aleshores $1 \in \mathfrak{pq}$, i això implica que $\mathfrak{p} = \mathfrak{q} = \mathcal{O}$.

Si tenim que t és parell, que és equivalent a $m \equiv 1 (\text{mod } 8)$. Aleshores $\mathfrak{pq} \subset 2\mathcal{O}$, i per tant com que $\mathfrak{p}$ i $\mathfrak{q}$ no estan continguts en $2\mathcal{O}$ llavors $\mathfrak{pq} = 2\mathcal{O}$.

Per la darrera part de la demostració, suposem que p és imparell i suposem que $m \equiv n^2 (\text{mod } p)$ té solució, és a dir, $m = n^2 + tp$. Siguin

$$\mathfrak{p} = p\mathcal{O} + (n+\sqrt{m})\mathcal{O} \text{ i } \mathfrak{q} = p\mathcal{O} + (n-\sqrt{m})\mathcal{O}.$$

Com que $\mathfrak{p}$ i $\mathfrak{q}$ no estan continguts en $p\mathcal{O}$ i

$$\mathfrak{pq} = p^2\mathcal{O} + p(n+\sqrt{m})\mathcal{O} + p(n-\sqrt{m})\mathcal{O} + tp\mathcal{O} \subset p\mathcal{O}$$

llavors, $\mathfrak{p}\mathcal{O} = \mathfrak{pq}$.

Finalment, per provar quan $p\mathcal{O}$ és ideal primer cal veure que el grau d'inèrcia f és 2. És suficient provar que $\mathbb{Z} + p\mathcal{O} \neq \mathcal{O}$. Per una banda, si p és imparell i no divideix a m, llavors el polinomi $X^2 - m$ és irreductible sobre $\mathbb{Z}/p\mathbb{Z}$, i per tant $\sqrt{m}$ és un element de $\mathcal{O}$ que no està en $\mathbb{Z} + p\mathcal{O}$. Per altra banda, si $m \equiv 5(\text{mod } 4)$ llavors $\frac{1+\sqrt{m}}{2}$ pertany a $\mathcal{O}$, però no a $\mathbb{Z} + 2\mathcal{O}$.

□

Donarem una sèrie d'eines per poder donar l'element de Frobenius d'un ideal primer de l'anell d'enters corresponent a $\mathbb{Q}(\sqrt{m})$.

Usarem el símbol de Legendre per saber si, per $a \in \mathbb{Z}$ i p primer imparell, a és residu quadràtic mòdul p. Recordem la definició del símbol de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si} \quad p|a \\ 1 & \text{si} \quad X^2 \equiv a(\text{mod } p) \text{ té solució} \\ -1 & \text{si} \quad X^2 \equiv a(\text{mod } p) \text{ no té solució.} \end{cases}$$

El símbol de Kroneker és una generalització del símbol de Jacobi, l'usarem en el cas $a \equiv 0, 1(\text{mod } 4)$ i $p = 2$,

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{si} \quad a \equiv 1(\text{mod } 8) \\ -1 & \text{si} \quad a \equiv 5(\text{mod } 8) \\ 0 & \text{si} \quad 4|a. \end{cases}$$

Per una banda, suposem que p és imparell. Usem el *Teorema 3.14* i el *Teorema 3.31*, llavors obtenim que:

$$\left(\frac{\text{disc}_L}{p}\right) = \begin{cases} 0 \text{ si } p|\text{disc}_L \\ 1 \text{ si } X^2 \equiv \text{disc}_L(\text{mod } p) \text{ té solució} \\ -1 \text{ si } X^2 \equiv \text{disc}_L(\text{mod } p) \text{ no té solució} \end{cases} = \begin{cases} 0 \text{ si } p \text{ ramifica en } \mathcal{O}_L \\ 1 \text{ si } p \text{ descompon en } \mathcal{O}_L \\ -1 \text{ si } p \text{ és inert en } \mathcal{O}_L \end{cases}$$

D'altra banda, suposem que p és parell, és a dir $p = 2$.

$$\left(\frac{\text{disc}_L}{2}\right) = \begin{cases} 0 \text{ si } \text{disc}_L \equiv 0(\text{mod } 4) \\ 1 \text{ si } \text{disc}_L \equiv 1(\text{mod } 8) \\ -1 \text{ si } \text{disc}_L \equiv 5(\text{mod } 8) \end{cases} = \begin{cases} 0 \text{ si } 2 \text{ ramifica en } \mathcal{O}_L \\ 1 \text{ si } 2 \text{ descompon en } \mathcal{O}_L \\ -1 \text{ si } 2 \text{ és inert en } \mathcal{O}_L \end{cases}$$

Considerem un primer enter p que no ramifica. Sigui $\mathfrak{q}$ un ideal primer de $\mathcal{O}_L$ que es troba a sobre de p. Llavors, l'element de Frobenius de $\mathfrak{q}$ sobre p és únic. Com que el grup de Galois de l'extensió $\mathbb{Q} \subset \mathbb{Q}(\sqrt{m})$ és abelià, aleshores $\text{Frob}_{\mathfrak{q}}$ només depèn de p. Considerem l'element d'aquest grup de Galois que envia $\sqrt{\text{disc}_L}$ a $-\sqrt{\text{disc}_L}$. Cada $a + b\frac{\text{disc}_L + \sqrt{\text{disc}_L}}{2} \in \mathcal{O}_L$ es redueix al cos residual $\mathbb{F}_{\mathfrak{p}}$ de la següent manera:

$$\left(a + b\frac{\text{disc}_L + \sqrt{\text{disc}_L}}{2}\right)^p \equiv a + b\frac{\text{disc}_L + \text{disc}_L{}^{(p-1)/2}\sqrt{\text{disc}_L}}{2}(\text{mod } \mathfrak{p})$$

on a, b i disc_L es redueixen en el subcós $\mathbb{F}_p$, i 2 es redueix al grup multiplicatiu de $\mathbb{F}_p$.

L'element de Frobenius és l'element de $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ que envia $\sqrt{\mathrm{disc}_L}$ a $\left(\frac{\mathrm{disc}_L}{p}\right)\sqrt{\mathrm{disc}_L} = (\mathrm{disc}_L)^{(p-1)/2}$, per enters primers $p \nmid \mathrm{disc}_L$.

Existeix, per tant, un isomorfisme de la següent forma:

$$\begin{gathered}\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \to \{\pm 1\} \\ \mathrm{Frob}_{\mathfrak{q}} \mapsto \left(\frac{\mathrm{disc}_L}{p}\right) \text{ per } p \text{ primers imparells tal que } p \nmid \mathrm{disc}_L.\end{gathered}$$

Cossos ciclotòmics.

Posem $K = \mathbb{Q}$ i $\mathcal{O}_K = \mathbb{Z}$. Sigui L un cos de nombres tal que $\mathbb{Q} \subset L$. Donat $\mathfrak{q}$ un ideal primer de $\mathcal{O}_L$, tenim, pel *Teorema 3.8*, que $\mathfrak{q}$ es troba a sobre d'un únic primer enter p. Aleshores, $\mathcal{O}_L/\mathfrak{q}$ és un cos d'ordre p^f on f és el grau d'inèrcia de $\mathfrak{q}$ sobre p.

Fixem un primer enter p. Sigui m un enter positiu i sigui $L = \mathbb{Q}(\omega) = e^{2\pi i/m}$. Tenim $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(m)$. Per ser $\mathbb{Q} \subset \mathbb{Q}(\omega)$ una extensió normal, pel *Corol·lari 3.18* tenim $p\mathcal{O}_L = (\mathfrak{q}_1 \cdots \mathfrak{q}_g)^e$ on $\mathfrak{q}_i$ són ideals primers diferents de $\mathbb{Z}[\omega]$ amb el mateix grau d'inèrcia f sobre p. A més, pel *Teorema 3.12* tindrem $efg = \varphi(m)$.

Sabem que $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Aleshores, tot element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ correspon a $\overline{k} \in (\mathbb{Z}/m\mathbb{Z})^*$, si i només si, $\sigma(\omega) = \omega^k$.

Considerem un primer enter p que no ramifica, és a dir un primer que no divideix m. Sigui $\mathfrak{q}$ un ideal primer de $\mathcal{O}_{\mathbb{Q}(\omega)}$ a sobre de p. Llavors, l'element de Frobenius de $\mathfrak{q}$ sobre p és únic. Com que el grup de Galois de l'extensió $\mathbb{Q} \subset \mathbb{Q}(\omega)$ és abelià, aleshores $\mathrm{Frob}_{\mathfrak{q}}$ només depèn de p, de fet tenim, per a tot $X \in \mathbb{Z}(\omega)$,

$$\mathrm{Frob}_{\mathfrak{q}}(X) \equiv X^p (\mathrm{mod}\ p\mathbb{Z}(\omega)).$$

Sigui $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ l'automorfisme que envia ω en ω^p. En general, tenim

$$\sigma\left(\sum_i a_i\omega^i\right) = \sum a_i\omega^{pi}, \quad \text{per a tot } a_i \in \mathbb{Z}.$$

Per tant, reduint mòdul $p\mathbb{Z}(\omega)$ tenim

$$\sum_i a_i\omega^{pi} \equiv \left(\sum_i a_i\omega^i\right)^p (\mathrm{mod}\ p\mathbb{Z}(\omega)).$$

Per tant, l'element de Frobenius de $\mathfrak{q}$ sobre p és σ.

Existeix, per tant, un isomorfisme de la següent forma:

$$\begin{gathered}\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^* \\ \mathrm{Frob}_{\mathfrak{q}} \mapsto n\end{gathered}$$

tal que $p \equiv n\,(\mathrm{mod}\ m)$ per p primers tals que $p \nmid m$.

4 Teorema de Chebotarev

Per entendre l'enunciat del teorema cal entendre les classes de conjugació. Ens serveixen per tractar varis elements d'un grup en un conjunt en el qual els seus elements comparteixen moltes propietats.

Definició 4.1. *Sigui $\sigma \in \mathrm{Gal}(L/K)$. Direm que C és classe de conjugació de σ si es compleix que*

$$C = \{h^{-1}\sigma h : h \in \mathrm{Gal}(L/K)\}.$$

Com hem vist a la *Proposició 3.28* els elements de Frobenius dels ideals primers que es troben a sobre d'un mateix ideal primer són conjugats, per tant, formen una classe de conjugació.

Definició 4.2. *Sigui $K \subset L$ una extensió de cossos de nombres. Sigui $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$. Es diu classe de conjugació de Frobenius de $\mathfrak{p}$ en L/K a la classe de conjugació que té la següent forma:*

$$\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Frob}_{\mathfrak{q}} : \mathfrak{q}|\mathfrak{p}\mathcal{O}_L\}.$$

Definim la funció zeta d'un cos de nombres per poder entendre el concepte de densitat. De fet, és la generalització, en el cas de cossos de nombres, de la funció zeta de Riemann.

Definició 4.3. *Per $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, la funció zeta de Riemann és*

$$\zeta(s) = \prod_{\substack{p \in \mathbb{Z} \\ p \text{ primer}}} \frac{1}{1 - \frac{1}{p^s}}.$$

Definició 4.4. *Sigui K un cos de nombres. Per $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, definim la funció zeta de Dedekind per*

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}$$

on el producte recorre tots els ideals primers $\mathfrak{p}$ de $\mathcal{O}_K$.

Sigui $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, prenem logaritmes a banda i banda de la seva definició, i obtenim:

$$\log(\zeta_K(s)) = \sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \log\left(\frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}\right) = -\sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \log\left(1 - \frac{1}{N(\mathfrak{p})^s}\right).$$

Desenvolupant per la sèrie de Taylor, tenim:

$$-\sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \log\left(1 - \frac{1}{N(\mathfrak{p})^s}\right) = \sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \left(N(\mathfrak{p})^{-s} + \frac{1}{2}N(\mathfrak{p})^{-2s} + ...\right) = \sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{1}{N(\mathfrak{p})^s} + g(s)$$

on $g(s)$ és una funció acotada quan s tendeix a 1. Anem a provar-ho: sabem que $N(\mathfrak{p}) \geq p$, per un primer racional p que es troba a sota de $\mathfrak{p}$, per tant $N(\mathfrak{p})^{-j} \leq \frac{1}{p^j}$ per $j = 2, 3, ...$

Cal tenir en compte, també, que el sumatori recorre tots els ideals primers de $\mathcal{O}_K$, de manera que ens queda:

$$\left| \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \left(\frac{1}{2} N(\mathfrak{p})^{-2} + \frac{1}{3} N(\mathfrak{p})^{-3} + ... \right) \right| \leq \left| \sum_{\substack{p\in\mathbb{Z} \\ p \text{ primer}}} \frac{1}{2} \frac{[K:\mathbb{Q}]}{p^2} + \frac{1}{3} \frac{[K:\mathbb{Q}]}{p^3} + ... \right|.$$

Traient factor comú ens queda:

$$[K:\mathbb{Q}] \left| \sum_{\substack{p\in\mathbb{Q} \\ p \text{ primer}}} \frac{1}{p^2} + \frac{1}{p^3} + ... \right| \leq 2[K:\mathbb{Q}] \left| \sum_{\substack{p\in\mathbb{Q} \\ p \text{ primer}}} \frac{1}{p^2} + \frac{1}{p^4} + ... \right| \leq 2[K:\mathbb{Q}] \left| \sum_{n\geq 1} \frac{1}{n^2} \right|.$$

Finalment, obtenim una sèrie convergent tal i com volíem.

Per tant, podem escriure

$$\log(\zeta_K(s)) \sim \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{1}{N(\mathfrak{p})^s}.$$

La notació $f(s) \sim g(s)$ significa que dues funcions, que tenen una singularitat en 1, difereixen per una funció analítica en 1.

El lector pot trobar demostrat a [3] el següent resultat.

Teorema 4.5. *Sigui K un cos de nombres. Aleshores, la funció zeta de Dedekind $\zeta_K(s)$ defineix una funció holomorfa en el semiplà $\mathrm{Re}(s) > 1$ que pot ser estesa a una funció meromorfa a tot el pla complex amb un únic pol simple a $s = 1$.*

Desenvolupant per la sèrie de Taylor, tenim

$$\zeta_K(s) = \frac{1}{s-1}(a_{-1} + a_0 + a_1(s-1) + a_2(s-1)^2 + ...),$$

a més, sabem que el numerador no s'anul·la en $s = 1$ per ser un pol. Per això, podem prendre logaritmes a banda i banda de la igualtat, de manera que ens queda:

$$\log(\zeta_K(s)) = \log\left(\frac{1}{s-1}\right) + \log(a_{-1} + a_0 + a_1(s-1) + ...).$$

Com que $\log(a_{-1} + a_0 + a_1(s-1) + ...)$ està acotada en $s = 1$, aleshores

$$\log(\zeta_K(s)) \sim -\log(s-1).$$

Llavors, podem escriure

$$\sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{1}{N(\mathfrak{p})^s} \sim \log\left(\frac{1}{s-1}\right).$$

Donem el concepte de densitat natural perquè el lector pugui entendre millor la noció de densitat, tot i que sol usar-se la densitat analítica per provar resultats. De fet, si la densitat natural existeix aleshores la densitat analítica també. Però, en general, al revés no es compleix.

Definició 4.6. *Si S és un conjunt d'ideals primers de $\mathcal{O}_K$. Definim la densitat natural de S, sempre que el límit existeixi, per*

$$d_n(S) = \lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) \leq X\}}{\#\{\mathfrak{p} \in \mathcal{O}_K : N(\mathfrak{p}) \leq X\}}.$$

Definició 4.7. *Sigui K un cos de nombres. Sigui S un conjunt d'ideals primers de $\mathcal{O}_K$.*

1) La densitat inferior es defineix per $d_K^-(S) = \liminf_{s\to 1} \left(\sum_{\mathfrak{p}\in S} \frac{1}{N(\mathfrak{p})^s} / \log(\frac{1}{s-1}) \right)$.

2) La densitat superior es defineix per $d_K^+(S) = \limsup_{s\to 1} \left(\sum_{\mathfrak{p}\in S} \frac{1}{N(\mathfrak{p})^s} / \log(\frac{1}{s-1}) \right)$.

Definició 4.8. *Sigui K un cos de nombres. Sigui S un conjunt d'ideals primers de $\mathcal{O}_K$. La densitat analítica de S existeix quan la densitat superior i la inferior de S són iguals. Si això passa, es defineix per $d_K(S) = d_K^-(S) = d_K^+(S)$.*

Observació 4.9. Pel fet que

$$\sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{1}{N(\mathfrak{p})^s} \sim \log\left(\frac{1}{s-1}\right),$$

els denominadors de les densitats superior i inferior són, llevat d'una certa funció acotada, igual a $\sum_{\mathfrak{p}\subseteq\mathcal{O}_K} \frac{1}{N(\mathfrak{p})^s}$. De manera informal, es pot dir que la densitat és la proporció de primers de $\mathcal{O}_K$ que són de S.

Proposició 4.10. *Sigui K un cos de nombres. La densitat d'un conjunt S d'ideals primers de $\mathcal{O}_K$ és igual a la densitat del conjunt format pels primers de S de grau 1.*

Demostració. Denotarem per $\mathrm{gr}(\mathfrak{p})$ al grau de l'ideal primer $\mathfrak{p}$. Per provar que la densitat d'un conjunt S d'ideals primers de $\mathcal{O}_K$ és igual a la densitat del conjunt format pels ideals primers de S de grau 1, cal demostrar que la següent sèrie convergeix.

$$\sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathrm{gr}(\mathfrak{p})>1}} \frac{1}{N(\mathfrak{p})}.$$

Sigui p el primer racional que es troba a sota dels ideals primers de $\mathcal{O}_K$. Per definició tenim $N(\mathfrak{p}) = p^{\mathrm{gr}(\mathfrak{p})}$, per tant, per a tot primer $\mathfrak{p}$ de grau major que 1 tenim

$$\frac{1}{N(\mathfrak{p})} \leq \frac{1}{p^2}.$$

A més, si posem $d = [K : \mathbb{Q}]$ sabem que qualsevol primer racional p té com a molt d primers $\mathfrak{p}$ de $\mathcal{O}_K$ per sobre seu. És a dir,

$$\sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathrm{gr}(\mathfrak{p})>1}} \frac{1}{N(\mathfrak{p})} \leq \sum_{p\in\mathbb{Z}} \frac{d}{p^2}.$$

Sabem que $\sum_{p\in\mathbb{Z}} \frac{d}{p^2}$ és convergent i això ens dona la convergència de

$$\sum_{\substack{\mathfrak{p}\in S\\ \mathrm{gr}(\mathfrak{p})>1}} \frac{1}{N(\mathfrak{p})}.$$

Sigui S un conjunt d'ideals primers de $\mathcal{O}_K$. Escrivim la seva densitat de la següent forma:

$$\lim_{s\to 1}\left(\frac{\sum_{\mathfrak{p}\in S}\frac{1}{N(\mathfrak{p})^s}}{\log\left(\frac{1}{s-1}\right)}\right) = \lim_{s\to 1}\left(\frac{\sum_{\substack{\mathfrak{p}\in S\\ \mathrm{gr}(\mathfrak{p})>1}}\frac{1}{N(\mathfrak{p})^s}}{\log\left(\frac{1}{s-1}\right)} + \frac{\sum_{\substack{\mathfrak{p}\in S\\ \mathrm{gr}(\mathfrak{p})=1}}\frac{1}{N(\mathfrak{p})^s}}{\log\left(\frac{1}{s-1}\right)}\right) = \lim_{s\to 1}\left(\frac{\sum_{\substack{\mathfrak{p}\in S\\ \mathrm{gr}(\mathfrak{p})=1}}\frac{1}{N(\mathfrak{p})^s}}{\log\left(\frac{1}{s-1}\right)}\right)$$

Podem afirmar la segona igualtat ja que el primer terme de la suma tendeix a 0, quan s tendeix a 1, per ser el numerador una sèrie convergent.

Per tant, tal i com volíem demostrar la densitat del conjunt d'ideals primers de S és igual a la densitat del conjunt d'ideals primers de S amb grau 1.

□

Proposició 4.11. *Sigui K un cos de nombres i m un nombre enter positiu. Sigui ρ_m una arrel m-éssima primitiva de la unitat. Per cada $h \in \mathrm{Gal}(K(\rho_m)/K)$, la densitat del conjunt d'ideals primers de $\mathcal{O}_K$ pels quals l'element de Frobenius és h, és igual a $1/\#\mathrm{Gal}(K(\rho_m)/K)$.*

Demostració. Denotem per H al grup $\mathrm{Gal}(K(\rho_m)/K)$. Per qualsevol ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$, el seu element de Frobenius és $N(\mathfrak{p}) \in H$. Tenim el morfisme de restricció $\mathrm{Gal}(K(\rho_m)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q})$, en particular tenim el morfisme $H \to \mathrm{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q})$ que és injectiu i permet identificar H amb un subgrup de $\mathrm{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$.

Per cada caràcter de Dirichlet $\chi : H \to \mathbb{C}^*$ i per $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, definim la L-sèrie de Dirichlet per

$$L(s,\chi) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{\chi(N(\mathfrak{a}))}{N(\mathfrak{a})^s}$$

on $\mathfrak{a}$ recorre tots els ideals de $\mathcal{O}_K$.

La L-sèrie de Dirichlet es pot expressar pel producte d'Euler de la següent forma:

$$L(s,\chi) = \prod_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K\\ \mathfrak{p}\text{ primer}}} \frac{1}{\left(1-\frac{\chi(N(\mathfrak{p}))}{N(\mathfrak{p})^s}\right)}.$$

El conductor de χ és el nombre r més petit tal que χ es pot veure com un caràcter mòdul r. Llavors, té sentit parlar de $\chi(k)$ quan k és un enter coprimer amb r. Si k no és coprimer amb r, aleshores $\chi(k)$ val 0 per definició.

Aleshores, per la *Definició 4.4* tenim

$$\zeta_{K(\rho_m)}(s) = \prod_{\chi:H\to\mathbb{C}} L(s,\chi),$$

on χ recorre els caràcters de Dirichlet de H. Observem que la L-sèrie corresponent al caràcter trivial és la funció zeta del cos de nombres K.

Referent a les L-sèries corresponents als caràcters no trivials volem saber si convergeixen, per $s \in \mathrm{Re}(s) > 1$. Farem servir el Criteri de Dirichlet que afirma que per a tota successió de nombres complexos $\{a_n\}_n$ tal que $\sum_n^N a_n$ és acotat quan $N \to \infty$, i considerant $\{b_n\}_n$ una successió de nombres complexos que tendeix monòtonament a 0, quan $n \to \infty$, llavors $\sum_{n\geq 1} a_n b_n$ convergeix. L'apliquem en $\sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{\chi(N(\mathfrak{a}))}{N(\mathfrak{a})^s}$, i obtenim que, per a $s \in \mathrm{Re}(s) > 1$, les L-series de χ no trivial convergeixen. A més com que $\zeta_K(s)$ i $\zeta_{K(\rho_m)}(s)$ tenen pols simples d'ordre 1 en $s = 1$, llavors per χ no trivial tenim $L(1, \chi) \neq 0$.

Llavors, per qualsevol χ no trivial,

$$\sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{\chi(N(\mathfrak{p}))}{N(\mathfrak{p})^s}$$

està acotada per $s \to 1$.

Per cada element $h \in H$ i per a qualsevol $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, definim:

$$F_h = \sum_{\chi: H\to\mathbb{C}} \chi^{-1}(h) \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{\chi(N(\mathfrak{p}))}{N(\mathfrak{p})^s}$$

on χ recorre els caràcters de Dirichlet de H en el primer sumatori. Tenim que F_h difereix de $L(s, 1)$ per una funció acotada quan $s \to 1$.

Per tant, $F_h(s) \sim \log\left(\frac{1}{s-1}\right)$.

Posem

$$F_h \sim \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{\sum_\chi \chi^{-1}(h)\chi(N(\mathfrak{p}))}{N(\mathfrak{p})^s} = \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ \mathfrak{p} \text{ primer}}} \frac{\sum_\chi \chi(h^{-1}N(\mathfrak{p}))}{N(\mathfrak{p})^s}.$$

Donat $h \in H$, una propietat dels caràcters de Dirichlet són les relacions d'ortogonalitat que satisfan

$$\sum_{\chi: H\to\mathbb{C}} \chi(h) = \begin{cases} \#H \text{ si } h = 1 \\ 0 \text{ altrament.} \end{cases}$$

Per tant,

$$F_h \sim \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ N(\mathfrak{p})\equiv h(\mathrm{mod}\ m)}} \frac{\#H}{N(\mathfrak{p})^s}$$

on la suma recorre tots els ideals $\mathfrak{p}$ que satisfan que $N(\mathfrak{p}) \equiv h(\mathrm{mod}\ m)$. És a dir,

$$\log\left(\frac{1}{s-1}\right) \sim \sum_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \\ N(\mathfrak{p})\equiv h(\mathrm{mod}\ m)}} \frac{\#H}{N(\mathfrak{p})^s}.$$

Llavors, la densitat del conjunt d'ideals primers de $\mathcal{O}_K$ pels quals l'element de Frobenius és $N(\mathfrak{p}) \equiv h(\mathrm{mod}\ m)$, és igual a

$$\lim_{s\to 1} \left(\frac{\sum \frac{1}{N(\mathfrak{p})^s}}{\log\left(\frac{1}{s-1}\right)} \right) = \lim_{s\to 1} \left(\frac{\sum \frac{1}{N(\mathfrak{p})^s}}{\sum \frac{\#H}{N(\mathfrak{p})^s}} \right) = \frac{1}{\#H},$$

on els sumatoris recorren els ideals $\mathfrak{p}$ tals que $N(\mathfrak{p}) = h(\text{mod } m)$.

□

Per provar el teorema de Chebotarev usarem el cas particular en extensions cícliques. La següent proposició dona la densitat d'un conjunt d'ideals primers pels quals l'element de Frobenius pertany al grup de Galois d'una extensió cíclica. Però abans, donem un lema i una definició que necessitem per la prova d'aquest resultat. El lema es pot trobar provat a la secció *13.11* del llibre [9].

Lema 4.12. *Sigui K un grup cíclic d'ordre m. Sigui d un divisor positiu de m. El nombre d'elements en K d'ordre divisible per d és*

$$m \prod_{p|d} \left(1 - \frac{1}{p^{ord_p(m) - ord_p(d)+1}}\right)$$

Definició 4.13. *Sigui H un subgrup de* $\text{Gal}(L/K)$*. El subcòs de L fix per H és*

$$L_H = \{X \in L | \sigma(X) = X, \forall \sigma \in H\}.$$

Observació 4.14. Per tant, $L_{\{1\}} = L$ i $L_G = K$, ja que L/K és una extensió de Galois.

Proposició 4.15. *Sigui K un cos de nombres. Sigui $K \subset L$ una extensió cíclica de Galois. Posem $G = \text{Gal}(L/K)$. Aleshores, per $\sigma \in G$, el conjunt d'ideals primers de $\mathcal{O}_K$ pels quals l'element de Frobenius és igual a σ té densitat $1/\#G$.*

Demostració. Donat $\sigma \in G$ i sigui q un nombre primer que no ramifica a l'extensió $\mathbb{Q} \subset L$. Denotarem per ρ a una arrel primitiva q-éssima de la unitat. Tenim que $L \cap \mathbb{Q}(\rho) = \mathbb{Q}$ i posant $H = \text{Gal}(K(\rho)/K)$ tenim $H \cong (\mathbb{Z}/q\mathbb{Z})^*$. Identifiquem el grup $\text{Gal}(L(\rho)/K)$ amb $G \times H$ via el morfisme de restricció.

Sigui S el conjunt d'ideals primers de $\mathcal{O}_K$ pels quals l'element de Frobenius és $\sigma \in G$. Usant la restricció d'abans, escriurem S com la unió de conjunts d'ideals primers de $\mathcal{O}_K$ pels quals l'element de Frobenius és $(\sigma, \mu) \in G \times H$, per a algun $\mu \in H$. Aquests conjunts els denotarem per S_μ.

Treballarem amb el concepte de densitat inferior que sempre existeix. Prenent límits inferior a la igualtat $S = \underset{\mu \in H}{\cup} S_\mu$, obtenim

$$d_K^-(S) \geq \sum_{\mu \in H} d_K^-(S_\mu).$$

Fixem $\mu \in H$ i suposem que $q \equiv 1(\text{mod } \#G)$. Suposem que μ té ordre divisible per $\#G$. Siguin $< (\sigma, \mu) >$ i $G \times \{1\}$ dos subgrups de $G \times H$. Denotem per $L(\rho)_{<(\sigma,\mu)>}$ i $L(\rho)_{G \times \{1\}}$ els subcossos de $K(\rho)$ fixos per $< (\sigma, \mu) >$ i $G \times \{1\}$, respectivament. Com que $< (\sigma, \mu) > \cap G \times \{1\} = \{1\}$, i tenint en compte l'*Observació 4.14* tenim

$$L(\rho)_{<(\sigma,\mu)>} \cdot L(\rho)_{G \times \{1\}} = L(\rho)_{\{1\}} = L(\rho).$$

Posant $L(\rho)_{<(\sigma,\mu)>} = F$, tenim que $F(\rho) = L(\rho)$, per això l'extensió $F \subset L(\rho)$ és ciclotòmica. Per la *Proposició 4.11* que tracta les extensions ciclotòmiques, sabem que existeix la densitat del conjunt d'ideals primers T de $\mathcal{O}_F$ pels quals l'element de Frobenius en $\text{Gal}(L(\rho)/F) \subset G \times H$ és (σ, μ), i és igual a:

$$d_F(T) = \frac{1}{\#\text{Gal}(L(\rho)/F))}.$$

Com hem vist a la *Proposició 4.10*, el subconjunt de T format pels ideals primers de $\mathcal{O}_F$ de grau 1 té la mateixa densitat. Recordem que S_μ, on $\mu \in H$, és el conjunt d'ideals primers de $\mathcal{O}_K$ pels quals l'element de Frobenius és $(\sigma, \mu) \in G \times H$. Per tant, $d_F(T) = d_F^-(T) = [F : K] d_K^-(S_\mu)$. Aleshores, per la restricció que hem suposat al principi de la demostració, tenim:

$$d_K^-(S_\mu) = \frac{d_F(T)}{[F : K]} = \frac{1}{[F : K]\#\mathrm{Gal}(L(\rho)/F)} = \frac{1}{\#G\#H}.$$

Sigui H' el conjunt de $\mu \in H$ d'ordre divisible per $\#G$. Llavors, sumant tots els seus elements i tenint en compte la desigualtat $d_K^-(S) \geq \sum_{\mu \in H} d_K^-(S_\mu)$ obtenim

$$d_K^-(S) \geq \#H' d_K^-(S_\mu) = \frac{\#H'}{\#G\#H}.$$

Volem aplicar l'anterior proposició per a demostrar que existeix q tal que $q \equiv 1 (\mathrm{mod}\ (\#G)^k)$. L'apliquem a l'extensió ciclotòmica $\mathbb{Q}(\rho_{(\#G)^k})/\mathbb{Q}$, on $\rho_{(\#G)^k}$ és una arrel de la unitat d'ordre $(\#G)^k$, i obtenim que per cada $\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ la densitat del conjunt d'ideals primers pels quals l'element de Frobenius és σ, és igual a $1/[\mathbb{Q}(\rho) : \mathbb{Q}] = 1/\varphi(q)$. Això és el *Teorema de Dirichlet sobre progressions aritmètiques* que més endavant enunciarem. Llavors, per qualsevol $k \geq 0$, existeix un nombre primer $q \equiv 1 (\mathrm{mod}\ (\#G)^k)$ que no ramifica en L.

Pel *Lema 4.12*, tenim que el nombre d'elements en $H \cong (\mathbb{Z}/q\mathbb{Z})^*$ d'ordre divisible per $(\#G)^k$ és

$$(q-1) \prod_{p | \#G} \left(1 - \frac{1}{p^{(k-1)\mathrm{ord}_p(\#G)+1}}\right).$$

Per tant, per a cada $k \geq 0$ tenim $\frac{\#H'}{\#H} \geq \prod_{p|\#G} \left(1 - \frac{1}{p^k}\right)$. Aleshores,

$$d_K^-(S) \geq \frac{1}{\#G} \prod_{p | \#G} \left(1 - \frac{1}{p^k}\right).$$

Fent tendir k a l'infinit, $d_K^-(S) \geq \frac{1}{\#G}$.

Fent el mateix considerant, enlloc de la densitat inferior, la densitat superior que també existeix, ens queda $d_K^+(S) \leq \frac{1}{\#G}$. És a dir, tenim $d_K^-(S) \geq \frac{1}{\#G} \geq d_K^+(S)$. Com que les densitats han de coincidir tenim el que volíem provar

$$d_K(S) = \frac{1}{\#G}.$$

□

Teorema 4.16. *(Teorema de densitat de Chebotarev) Sigui K un cos de nombres. Sigui $K \subset L$ extensió de Galois de dimensió finita. Posem $G = \mathrm{Gal}(L/K)$. Sigui $C \subset G$ una classe de conjugació. Aleshores, el conjunt S d'ideals primers $\mathfrak{p}$ de $\mathcal{O}_K$ pels quals la seva classe de conjugació de Frobenius és C, té densitat*

$$d_K(S) = \frac{\#C}{\#G}.$$

Demostració del Teorema de densitat de Chebotarev.

Sigui C una classe de conjugació de G. Sigui $\sigma \in C$ que deixa fixa a tot element d'un cos E, és a dir $E = \{X \in L | \sigma(X) = X\}$. Per tant, $E \subset L$ és una extensió cíclica de Galois tal que $G' = \mathrm{Gal}(L/E) =< \sigma >$.

Sigui T el conjunt dels ideals primers de E pels quals l'element de Frobenius és σ en $\mathrm{Gal}(L/E)$, per la *Proposició 4.15*,

$$d_E(T) = \frac{1}{\#G'}.$$

Per la *Proposició 4.10* tenim que el subconjunt de T format pels ideals primers de grau 1 sobre $\mathcal{O}_E$ té la mateixa densitat que $d_E(T)$. Recordem que S és el conjunt d'ideals primers de $\mathcal{O}_K$ pels quals la classe de conjugació de Frobenius és C. Considerant un ideal primer $\mathfrak{p}$ de S, existeixen $\#G/\#G'$ ideals primers $\mathfrak{q}$ de $\mathcal{O}_E$ a sobre de $\mathfrak{p}$. Els elements de Frobenius d'aquests ideals $\mathfrak{q}$ són conjugats i, per tant, pertanyen a la classe de conjugació C. Per tant, per qualsevol $\sigma' \in C$, el nombre d'ideals de $\mathcal{O}_L$ que estan per sobre de $\mathfrak{p}$ i el seu element de Frobenius és σ' és el mateix, és a dir, aquest nombre no depèn de σ', i és $\frac{\#G}{\#G'\#C}$. En particular, es satisfà per $\sigma \in C$.

Com que per cada ideal primer de $\mathcal{O}_E$ n'existeix un de $\mathcal{O}_L$ a sobre aquest, aleshores existeixen $\frac{\#G}{\#G'\#C}$ ideals primers de $\mathcal{O}_E$ que es troben a sobre de $\mathfrak{p}$ amb l'element de Frobenius igual a σ. A més sabem que $\mathfrak{p}$ factoritza completament en E, i això implica que $N(\mathfrak{q}) = N(\mathfrak{p})$ si $\mathfrak{q}$ està per sobre de $\mathfrak{p}$. Per tant,

$$\sum_{p \in S} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{\frac{\#G}{(\#G'\#C)}} \sum_{q \in T} \frac{1}{N(\mathfrak{q})^s}.$$

Quan s tendeix a 1, llavors

$$d_K(S) = \liminf_{s \to 1} \frac{\sum_{\mathfrak{p} \in S} 1/N(\mathfrak{p})^s}{\log(1/(s-1))} = \liminf_{s \to 1} \frac{\frac{\#G'\#C}{\#G} \sum_{\mathfrak{q} \in T} 1/N(\mathfrak{q})^s}{\log(1/(s-1))} = \frac{\#G'\#C}{\#G} d_E(T)$$

Com $d_E(T) = \frac{1}{\#G'}$, ens queda que

$$d_K(S) = \frac{\#G'\#C}{\#G} \frac{1}{\#G'} = \frac{\#C}{\#G}.$$

□

El *Teorema de Chebotarev* és més fàcil d'entendre quan el cos que tractem són els racionals. Sigui f un polinomi mònic irreductible de grau n amb coeficients enters, que té α com arrel. Considerem $K = \mathbb{Q}(\alpha)$. Sigui $P = (n_1, ..., n_r)$ una partició de n, és a dir, un conjunt ordenat d'enters $n_1 \geq ... \geq n_r$ amb $n = n_1 + ... + n_r$. Com hem vist al *Teorema 3.14*, un nombre primer no ramifica sobre el cos de nombres K si no divideix el discriminant de f.

Sigui p un primer i sigui S un conjunt de primers que no ramifiquen. Sigui S_p un conjunt de primers que no ramifiquen pels quals f es descompon en factors irreductibles f_i mòdul p que tenen grau n_i. És a dir, $f(X) \equiv f_1(X) \cdots f_r(X) (\mathrm{mod}\ p)$. La densitat del conjunt S_p és la densitat natural, és a dir

$$d_n(S_p) = \lim_{N \to \infty} \frac{\#\{p \in S_p | p \leq N\}}{\#\{p \in S | p \leq N\}}.$$

Denotem per G al grup de Galois de l'extensió $\mathrm{Gal}(K/\mathbb{Q})$ del cos de nombres K. Com bé sabem, G és un subgrup del grup simètric S_n, llavors cada element de G es pot escriure com una permutació de n membres, els quals tenen una única factorització com a producte de cicles disjunts. Ara, considerem el subconjunt d'elements G_p de G que consisteix en cicles disjunts de dimensió $n_1, ..., n_r$. Aleshores,

$$d(S_p) = \frac{\#G_p}{\#G}.$$

4.1 Casos particulars del Teorema de Chebotarev

Dos dels resultats més coneguts són el *Teorema de Dirichlet sobre primers en progressions aritmètiques* i el *Teorema de Frobenius*, els dos són casos particulars del *Teorema de Chebotarev*.

Teorema de Dirichlet sobre primers en progressions aritmètiques.

Com bé hem dit a la introducció del treball, el resultat de Dirichlet es considera un cas particular del *Teorema de Chebotarev* per extensions ciclotòmiques. De fet, el primer es pot deduir a partir de l'anàlisi de l'element de Frobenius en el cas ciclotòmic, a la demostració de la *Proposició 4.15* ho podem veure.

Teorema 4.17. *(Teorema de Dirichlet sobre primers en progressions aritmètiques.) Sigui m un nombre enter positiu. Aleshores, per cada enter a tal que $\mathrm{mcd}(a, m) = 1$ el conjunt de nombres primers p amb $p \equiv a (mod\ m)$ té densitat $1/\varphi(m)$.*

Demostració La demostració es deduirà del *Teorema de Chebotarev*. Sigui m un nombre enter positiu. Recordem l'isomorfisme del *Corol·lari 2.39*

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q})$$

que envia un primer $p \in (\mathbb{Z}/m\mathbb{Z})^*$ a l'element de Frobenius corresponent, Frob_p. A més, a qualsevol enter a tal que $a \in (\mathbb{Z}/m\mathbb{Z})^*$ li associem un element h del grup de Galois de l'extensió $\mathbb{Q}(\rho_m)/\mathbb{Q}$. Aplicant el resultat de Chebotarev obtenim que la densitat del conjunt de nombres primers p tal que $p \equiv a (\mathrm{mod}\ m)$ té densitat

$$1/\#\mathrm{Gal}(\mathbb{Q}(\rho_m)/\mathbb{Q}) = 1/\varphi(m).$$

□

Teorema de Frobenius.

Per moltes aplicacions del *Teorema de Chebotarev* és suficient usar el *Teorema de Frobenius*, per exemple una d'elles és determinar el grup de Galois d'un polinomi amb coeficients enters. Més endavant en veurem un exemple.

Sigui $f(X)$ un polinomi mònic irreductible amb coeficients enters. Siguin $\alpha_1, ..., \alpha_n$ les arrels de f en $\bar{\mathbb{Q}}$. Denotem per G al grup de Galois de l'extensió $\mathbb{Q}(\alpha_1, ..., \alpha_n) \subset \mathbb{Q}$, que és subgrup del grup de permutacions S_n, també denotem per $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$. Sigui p un primer racional que no divideix al discriminant de $\mathbb{Q}(\alpha_1, ..., \alpha_n)$, és a dir, p no ramifica i, per tant, descompon en $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ com $p = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, on cada $\mathfrak{p}_i$ és un ideal primer de $\mathcal{O}_{\mathbb{Q}(\alpha_1,...,\alpha_n)}$. Sabem que tots ells tenen el mateix índex de ramificació pel *Corol·lari 3.18*, denotem-lo per f. Escollim un $\mathfrak{p}_i$ i definim el següent morfisme de reducció:

$$\pi : \mathcal{O}_{\mathbb{Q}}(\alpha_1, ..., \alpha_n) \to \mathcal{O}_{\mathbb{Q}}(\alpha_1, ..., \alpha_n)/\mathfrak{p}_\mathfrak{i},$$

a més, tal i com hem pogut veure a la secció 3.2 tenim que $\mathcal{O}_{\mathbb{Q}}(\alpha_1, ..., \alpha_n)/\mathfrak{p}_\mathfrak{i} \cong \mathbb{F}_{p^f}$.

Reduint la igualtat $f(\alpha_j) = 0$, per a qualsevol $1 \leq j \leq n$, pel morfisme de restricció definit abans, i tenint en compte que reduir els coeficients de f mòdul $\mathfrak{p}_i$ és el mateix que reduir-los mòdul p, ja que són nombres enters, obtenim que les arrels $\alpha_1, ..., \alpha_n$ corresponen a arrels de $f(X)$ mòdul p. Per tant, $\mathcal{O}_{\mathbb{Q}}(\alpha_1, ..., \alpha_n)/\mathfrak{p}_\mathfrak{i}$ és el cos de descomposició de $f(X)$ mòdul p sobre el cos finit de p elements.

Denotem per σ_p a l'automorfisme de Frobenius de $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ que envia X a X^p. Tal i com hem vist a la secció 3 tenim el següent isomorfisme:

$$D_{\mathfrak{p}_i} \cong \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$$

que envia l'element de Frobenius $\mathrm{Frob}_{\mathfrak{p}_i}$, que és un element de $D_{\mathfrak{p}_i}$, a σ_p. Això significa que $\mathrm{Frob}_{\mathfrak{p}_i}$ permuta les arrels $\alpha_1, ..., \alpha_n$ de la mateixa manera que σ_p permuta les arrels $\pi(\alpha_1), ..., \pi(\alpha_n)$. Sabem que el polinomi $f(X)$ descompon en factors irreductibles sobre el cos $\mathbb{F}_p$, aleshores podem escriure $f(X) \equiv f_1(X) \cdots f_r(X) (\mathrm{mod}\ p)$, direm *tipus de descomposició de f mòdul p* a cadascun dels graus de f_i. Per tant, σ_p permuta les arrels de cada factor irreductible, i com que G és un subgrup del grup de permutacions S_n tenim que σ_p correspon a un producte de r permutacions.

Volem veure que cadascuna d'aquestes permutacions és un cicle de longitud igual que el grau de f_i. Per una banda, tenim que $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ actua transitivament en les arrels de cada factor irreductible de f, i per l'altra banda, el grup de Galois està generat per σ_p. I l'única manera que les potències de σ_p actuïn de manera transitiva en les arrels de cada factor irreductible és que cadascuna de les permutacions corresponents a cada f_i sigui un cicle de longitud el grau de f_i.

Direm *tipus de cicle d'un element de S_n* a les longituds de cadascun dels factors de la descomposició d'aquest element en producte de cicles.

Teorema 4.18. *(Teorema de Frobenius.) Sigui S el conjunt de nombres primers pels quals f té un tipus de descomposició $n_1, ..., n_r$ donat. Llavors, la densitat de S existeix i és igual a $\frac{1}{\#G}$ vegades el nombre d'elements de G amb tipus de cicle $n_1, ..., n_r$.*

Demostració. Com que acabem de provar que el tipus de cicle de $\mathrm{Frob}_{\mathfrak{p}_i}$ coincideix amb la partició de n donada pels graus f_i mòdul p, el conjunt S està formant pels nombres primers pels quals el tipus de cicle és $n_1, ..., n_r$.

Pel *Teorema de Chebotarev*, obtenim que el conjunt d'ideals primers $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{Q}}(\alpha_1, ..., \alpha_r)$, és a dir, el conjunt S té densitat i és $\frac{1}{\#G}$ vegades el nombres primers pels quals el tipus de cicle de σ_p és $n_1, ..., n_r$.

□

Donem un exemple de com determinar el grup de Galois d'un polinomi amb coeficients enters mitjançant el *Teorema de Frobenius*. Considerem diferents polinomis f de grau 4, i donem les densitats de les quantitats de nombres primers pels quals f mòdul p té un tipus de descomposició donat.

Considerem el polinomi X^4+3X^2+7X+4 i el descomponem en polinomis irreductibles mòdul els diferents nombres primers menors que 1000. Llavors, per exemple, tenim:

$$f \equiv X(X^3 + X + 1) (\mathrm{mod}\ 2) \text{ que té tipus de descomposició 1, 3}$$

$$f \equiv (X - 3)^2(X + 3)^2 (\mathrm{mod}\ 7) \text{ que té tipus de descomposició 2, 2}$$

$f \equiv (X+9)(x-3)^3 (\text{mod } 19)$ que té tipus de descomposició 1, 3.

Classifiquem els 168 nombres primers més petits que 1000 depenent del tipus de descomposició en que descompon f mòdul tal primer, i obtenim que: hi ha 112 primers que els hi correspon el tipus $1,3$, 44 el tipus $2,2$ i 10 el tipus $1,1,1,1$. Per tant, les densitats de les quantitats de nombres primers pels quals f mòdul p té un tipus de descomposició donat són:

tipus	densitat
$1,3$	$112/168 = 2/3$
$2,2$	$44/168 \approx 1/4$
$1,1,1,1$	$10/168 \approx 1/12$

De manera similar per altres polinomis de grau 4, obtenim que:

f	4	$1,3$	$2,2$	$1,1,2$	$1,1,1,1$
$X^4 - X - 1$	$1/4$	$1/3$	$1/8$	$1/4$	$1/24$
$X^4 - X^2 + 1$	0	0	$3/4$	0	$1/4$
$X^4 + X^3 + X^2 + X + 1$	$1/2$	0	$1/4$	0	$1/4$
$X^4 - X^2 - 1$	$1/4$	0	$3/8$	$1/4$	$1/8$
$X^4 + 3X^2 + 7X + 4$	0	$2/3$	$1/4$	0	$1/12$

Tenint en compte el *Teorema de Frobenius* que ens afirma que la densitat del conjunt de primers p pels quals f mòdul p descompon completament en factors lineals té densitat $1/\#G$, el grup de Galois de cadascun dels polinomis anterior tenen ordre 24, 4, 4, 8 i 12, respectivament. Això es pot veure directament amb la darrera columna de la taula.

De fet, els grups de Galois d'aquests polinomis, que són irreductibles de grau 4, són subgrups de S_4. Tenint en compte que han de ser transitius i mirant l'ordre de $\#G$, tenim que:

f	G	
$X^4 - X - 1$	S_4	grup simètric de grau 4
$X^4 - X^2 - 1$	D_4	grup diedral d'ordre 8
$X^4 + 3X^2 + 7X + 4$	A_4	grup alternat d'ordre 12.

Pels altres polinomis, no serà suficient l'ordre per determinar el seu grup de Galois, ja que existeixen diferents subgrups transitius de S_4 d'ordre 4. Existeixen dues possibilitats: el grup de Klein i el grup cíclic d'ordre 4.

Per una banda, sabem que $V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$, o sigui té tres elements amb tipus de descomposició $2,2$ i un element amb tipus de descomposició $1,1,1,1$. D'aquí, deduïm que el polinomi $X^4 - X^2 + 1$ té com a grup de Galois el grup de Klein d'ordre 4.

Per altra banda, sabem que $C_4 = \{Id, (1234), (13)(24), (1423)\}$, és a dir, té dos elements amb tipus de descomposició 4, un amb $1,1,1,1$ i un altre amb $2,2$. Per tant, es pot deduir que el polinomi $X^4 + X^3 + X^2 + X + 1$ té com a grup de Galois el grup cíclic d'ordre 4.

Resumint, tenim:

f	G	
$X^4 - X^2 + 1$	V_4	grup de Klein d'ordre 4
$X^4 + X^3 + X^2 + X + 1$	C_4	grup cíclic d'ordre 4.

5 Conclusions

L'estudi que s'ha fet en aquest treball està centrat en entendre i demostrar el *Teorema de Chebotarev*, i, a més, s'han donat dos casos particulars: el *Teorema de Dirichlet sobre progressions aritmètiques* i el *Teorema de Frobenius*, el primer il·lustra el cas d'extensions ciclotòmiques i el darrer ens serveix per donar una de les aplicacions que té el resultat principal d'aquest treball.

Es pot dir que la motivació de Nikolai Grigorévich Chebotarev per provar el seu teorema fou la conjectura que va formular Frobenius quan estudiava el teorema de la densitat. Tot i que algunes proves d'aquest utilitzen la teoria dels cossos de classes, Chebotarev ho va fer sense aquesta eina. De fet, en el moment de la publicació del resultat, Chebotarev encara no tenia coneixements sobre aquesta teoria. La clau del raonament de Chebotarev fou barrejar les extensions abelianes d'un cos de nombres amb els cossos ciclotòmics, només usant la teoria bàsica de Galois. En aquest treball, s'ha demostrat el *Teorema de Chebotarev* seguint l'estratègia original de l'autor, sense usar la teoria de cossos de classes.

Referències

[1] Marcus, Daniel A.: Number Fields, *Springer-Verlag*, N.Y., 12-130, 1945.

[2] Beukers, F.: Algebraic Number Theory. Disponibilitat i accés a `http://www.math.leidenuniv.nl/ evertse/dio2011-algnumbers.pdf`, 2011.

[3] Lang, S.: Algebraic Number Theory, *Springer-Verlag*, N.Y., 159-160, 1986.

[4] Schoof, René: Catalan's Conjecture, *Springer-Verlag*, London, 95-106, 2008.

[5] Diamond, F.; Shurman, J.: A First Course in Modular Forms, *Springer Science+Bussines Media*, 230-233, 365-372, 2005.

[6] Conrad, Keith: Existence of Frobenius Elements. Disponibilitat i accés a `https://kconrad.math.uconn.edu/blurbs/gradnumthy/frobeniuspf.pdf`.

[7] Stevenhagen, P.; Lenstra, Jr.H.W.: Chebotarev and his density theorem. Disponibilitat i accés a `http://www.math.leidenuniv.nl/ hwl/papers/cheb.pdf`.

[8] Lenstra, H.: The Chebotarev Density Theorem. Disponibilitat i accés a `http://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf`.

[9] Apostol, T.M.: Introduction to Analytic Number Theory, *Springer-Verlag*, N.Y., 1980.

[10] Conrad, Keith: Dedekind's factorization criterion. Disponibilitat i accés a `http://math.stanford.edu/ conrad/154Page/handouts/dedekindcrit.pdf`.