Universitat Autònoma de Barcelona

Treball Final de Grau

Conceptes bàsics de l'extensió ciclotòmica, funcions L de Dirichlet i fórmules del nombre de classes

Jordi Gual Tallero

$$\lim_{s\longrightarrow 1^+}(s-1)\zeta_K(s)=\frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K\sqrt{|D_K|}}$$

Tutor
Francesc Bars Cortina

Any
2022

Resum

Sigui $K/\mathbb{Q}$ una extensió finita, abeliana i Galois, definim el caràcter de Dirichlet com el morfisme de grups $\chi : Gal(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \to \mathbb{C}^\times$, per a alguna arrel f-èssima de l'unitat. En el treball demostrem que $\zeta_K(s) = \prod_\chi L(s,\chi)$, on χ recorre $Hom(Gal(K/\mathbb{Q}), \mathbb{C}^\times)$, i fem un esbós del residu de ζ_K en el pol simple a $s = 1$. En particular obtenim $L(1,\chi) \neq 0$, una expressió per a $L(1,\chi)$ i la relació de $L(1-n,\chi)$ amb els nombres de Bernoulli. Com a aplicació de la fórmula del residu quan $K/\mathbb{Q}$ és una extensió de grau 2 veiem com podem calcular el nombre de classes de K fent servir les fórmules per $L(1,\chi)$, el regulador de K i via sumes de Gauss.

1 Caràcters de Dirichlet i funció L de Dirichlet

Aquest apartat està basat en les primeres pàgines del capítol 3 i tot el capítol 4 del llibre [15].

Definició 1 (Caràcter de Dirichlet)**.** *Sigui m un nombre natural. Definim un caràcter de Dirichlet mod m com un homomorfisme de grups:*

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

En diem un caràcter de Dirichlet primitiu si no el podem escriure com a una composició

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times$$

d'un caràcter de Dirichlet χ' mod n per a algun divisor $n|m$ on $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ és el morfisme natural. Si un caràcter χ no és primitiu podem pensar χ mod m o mod n ja que defineixen essencialment el mateix morfisme. És convenient doncs triar m minimal. De la mínima m en direm el conductor de χ i denotem aquest conductor minimal de χ per f o f_χ.

Com que $(\mathbb{Z}/m\mathbb{Z})^\times \cong Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ podem pensar χ com un morfisme del grup $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ a $\mathbb{C}^\times$. Sigui $ker(\chi)$ nucli de χ, sabem que $ker(\chi)$ és un subgrup de $(\mathbb{Z}/m\mathbb{Z})^\times$ i en particular de $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Aleshores pel teorema fonamental de la teoria de Galois tenim una bijecció entre els subgrups de $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ i els cossos intermitjos de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Sigui K el cos fix que correspon al nucli de χ, llavors podem definir el caràcter de Dirichlet χ com

$$(\mathbb{Z}/f\mathbb{Z})^\times \cong Gal(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \xrightarrow{\varphi} Gal(K/\mathbb{Q}) \longrightarrow \mathbb{C}^\times,$$

del cos K en diem cos associat a χ i l'aplicació φ és la restricció d'un automorfisme a $\mathbb{Q}(\zeta_f)$ a K. Si X és un grup abelià finit format per caràcters de Dirichlet, triem $n = mcm_{\chi\in X}(f_\chi)$ i X és un grup de caràcters de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ a $\mathbb{C}^\times$. Sigui H la intersecció dels nuclis de tots els caràcters de X i K el cos fix corresponent a H. Aleshores K és el cos associat a X i $X = Hom(Gal(K/\mathbb{Q}), \mathbb{C}^\times)$. En particular tenim $X \cong Gal(K/\mathbb{Q})$. Vegem-ho: Pel teorema fonamental dels grups abelians finits, el grup X és suma directa de grups cíclics $\mathbb{Z}/m\mathbb{Z}$. Aleshores $Hom(Gal(K/\mathbb{Q}), \mathbb{C}^\times)$ és producte de grups de la forma $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^\times)$ i per tant només hem de demostrar que $\mathbb{Z}/m\mathbb{Z} \cong Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^\times)$. Sigui $\varphi \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^\times)$ aleshores $\varphi(a \bmod n) = \varphi(a \cdot 1 \bmod n) = \varphi(1)^a$, per ser φ un homomorfisme i $\mathbb{Z}/m\mathbb{Z}$ un grup additiu. Aleshores cada homomorfisme $\varphi \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^\times)$ està determinat pel valor de $\varphi(1 \bmod m)$. Així com que els morfismes de grups envien el neutre del primer grup al neutre del segon, tenim

$$1 = \varphi(m \bmod m) = \varphi(m \cdot 1 \bmod m) = \varphi(1 \bmod m)^m$$

i per tant φ és una arrel m-èssima de la unitat. Així doncs podem escriure un isomorfisme explícit entre $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{C}^\times)$ i $\mathbb{Z}/m\mathbb{Z}$ que envia ζ_m^i a i per a $i \in \{0, 1, \dots, m-1\}$. És important observar que el grau de $K/\mathbb{Q}$ és igual al nombre de caràcters de X.

Exemple 1. *Sigui $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ definit com $\chi(1) = 1, \chi(3) = -1, \chi(5) = 1, \chi(7) = -1$. El nucli d'aquest caràcter és 1 mod 8 i 5 mod 8. L'irreductible de $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ és el vuitè polinomi ciclotòmic $x^4 + 1$ que té arrels $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$. Com que és una extensió simple els automorfismes envien ζ_8 a cada una de les arrels del polinomi irreductible. Posem $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ on $\sigma_0(\zeta_8) = \zeta_8, \sigma_1(\zeta_8) = \zeta_8^3, \sigma_2(\zeta_8) = \zeta_8^5, \sigma_3(\zeta_8) = \zeta_8^7$. Els subgrups de $(\mathbb{Z}/m\mathbb{Z})^\times$ són*

$$\begin{tikzcd}
 & (\mathbb{Z}/(8))^{\times} \cong Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
< 3 > \arrow[dr, dash, "2"'] & < 5 > \arrow[d, dash, "2"] & < 7 > \arrow[dl, dash, "2"] \\
 & < 1 > \cong \{id\} &
\end{tikzcd}$$

on $< 5 >= \{1, 5\}$ *és el grup generat per* 5 *mod* 8 *i forma* $ker(\chi)$*. Busquem el cos fix corresponent a aquest subgrup. Hem de buscar un subconjunt de* $\mathbb{Q}(\zeta_8)$ *que quedi fix per* σ_2*. Tenim*

$$\sigma_2(\zeta_8^4) = (\zeta_8^4)^5 = \zeta_8^4 = -1, \quad \sigma_2(\zeta_8^6) = (\zeta_8^6)^5 = \zeta_8^6 = -i,$$

i per tant el cos intermig K *és* $\mathbb{Q}(i)$*. Esquematicament hem construit* χ *utilitzant la teoria de Galois*

$$\begin{aligned}
1 \ mod \ 8 &\leftrightarrow \sigma_0(\zeta_8) = \zeta_8^1 \mapsto \sigma_0|_{\mathbb{Q}(i)}(i) = (\zeta_8^2)^1 = +i \leftrightarrow +1 \\
3 \ mod \ 8 &\leftrightarrow \sigma_1(\zeta_8) = \zeta_8^3 \mapsto \sigma_1|_{\mathbb{Q}(i)}(i) = (\zeta_8^2)^3 = -i \leftrightarrow -1 \\
5 \ mod \ 8 &\leftrightarrow \sigma_2(\zeta_8) = \zeta_8^5 \mapsto \sigma_2|_{\mathbb{Q}(i)}(i) = (\zeta_8^2)^5 = +i \leftrightarrow +1 \\
7 \ mod \ 8 &\leftrightarrow \sigma_3(\zeta_8) = \zeta_8^7 \mapsto \sigma_3|_{\mathbb{Q}(i)}(i) = (\zeta_8^2)^7 = -i \leftrightarrow -1
\end{aligned}$$

on, en aquest cas, la primera aplicació és l'isomorfisme de $(\mathbb{Z}/m\mathbb{Z})^{\times}$ *a* $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$*, la segona és la restricció dels automorfismes del grup de Galois a* $\mathbb{Q}(i)$ *i l'última és l'aplicació signe.*
Notem que $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$*. Aleshores la restricció de* $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ *a* $Gal(\mathbb{Q}(\zeta_4)/\mathbb{Q})$ *és de fet una aplicació de* $(\mathbb{Z}/8\mathbb{Z})^{\times}$ *a* $(\mathbb{Z}/4\mathbb{Z})^{\times}$*. Si definim un caràcter* χ' *que envia l'1 mod 4 al 1 i el 3 mod 4 al -1, aleshores* $\chi : (\mathbb{Z}/8\mathbb{Z})^{\times} \to (\mathbb{Z}/4\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$*, i està clar que el conductor de* χ *és* $f = 4$*.*

Observem que si considerem $K = \mathbb{Q}(i)$ *com a cos associat a un grup de caràcters de Dirichlet* X*, com que* $\mathbb{Q}(i)$ *és un cos quadràtic, és a dir,* $[\mathbb{Q}(i) : \mathbb{Q}] = 2$*, aleshores* X *només té dos caràcters. Com que* X *és un grup, sempre hi ha d'haver el caràcter trivial (el que sempre té imatge 1) que fa d'element neutre i l'altre caràcter és el que hem calculat. Per a caràcters de Dirichlet amb* $[K : \mathbb{Q}] > 2$ *el procediment per trobar-los explícitament pot ser molt més laboriós.*

Presentem ara la funció L de Dirichlet, i alguna de les seves propietats.
Ens interessa estendre χ a $\chi(a)$ amb $a \in \mathbb{N}$ arbitrari tal que

$$\chi(a) = \begin{cases} \chi(a \text{ mod } m) & \text{per } (a, m) = 1, \\ 0 & \text{per } (a, m) \neq 1. \end{cases}$$

Diem que un caràcter de Dirichlet és parell si compleix $\chi(-1) = 1$ i senar si $\chi(-1) = -1$.

Definició 2 (Sèrie L de Dirichlet). *Sigui χ un caràcter de Dirichlet amb conductor f. Definim la sèrie L associada a χ com*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \textit{per a } Re(s) > 1.$$

Observació 1. *Es pot veure*

$$\prod_p (1 - \chi(p)p^{-s})^{-1}, \quad \textit{per a } Re(s) > 1,$$

on p recorre tots els nombres primers.

Notem que per raons de convergència de sumes i productes de funcions de variable complexa, només hem definit $L(s,\chi)$ per a s amb part real estrictament més gran que 1. El primer objectiu serà extendre analíticament la sèrie L a tot el pla complex.

Definició 3 (Funció L de Dirichlet completada). *Sigui $L(s,\chi)$ la funció L de Dirichlet associada a un caràcter χ, definim*

$$\hat{L}(s,\chi) := f^{s/2}\pi^{-\frac{s+\epsilon(\chi)}{2}}\Gamma\left(\frac{s+\epsilon(\chi)}{2}\right)L(s,\chi), \ \textit{per a } Re(s) > 1,$$

amb

$$\epsilon(\chi) = \begin{cases} 0 \ \textit{si } \chi \ \textit{parell} \\ 1 \ \textit{si } \chi \ \textit{senar}, \end{cases}$$

i on la funció Γ es defineix com

$$\Gamma(s) = \int_0^\infty e^{-t}t^s \frac{dt}{t}, \quad \textit{per a } Re(s) > 0.$$

Fet: la funció $\Gamma(s)$ té continuació analítica a una funció meromorfa a tot el pla complex. Aquesta funció és holomorfa excepte per a $s = -n = 0, -1, -2, -3, \ldots$, amb $n \in \mathbb{Z}_0^+$ on hi té pols d'ordre 1 i residu $(-1)^n/n!$. Veure [1, Capítol 2.4.].

Definim també una altra funció important

Definició 4 (Suma de Gauss). *Sigui χ un caràcter de Dirichlet amb conductor f i ζ_f una arrel f-èssima de la unitat, definim la suma de Gauss com*

$$G(\chi,\zeta_f) = \sum_{a=1}^{f} \chi(a)\zeta_f^a.$$

Definim el caràcter de Dirichlet trivial mòdul m com el caràcter que val $\chi_0(a) = 1$ si $(a,m) = 1$ i $\chi_0(a) = 0$ si $(a,m) \neq 1$.

Teorema 1 (Equació funcional). *Sigui χ un caràcter de Dirichlet diferent del caràcter trivial, aleshores la funció $L(s,\chi)$ té una continuació analítica a tot el pla complex i satisfà l'equació funcional*

$$\hat{L}(s,\chi) = W(\chi)\hat{L}(1-s,\bar{\chi})$$

on $W(\chi) = \frac{G(\chi,\zeta_f)}{i^{\epsilon(\chi)}\sqrt{f}}$ i $\epsilon(\chi) = 0$ si χ és parell i $\epsilon(\chi) = 1$ si χ és senar.

Demostració. Comencem suposant que χ és parell, $\chi(-1) = 1$. Definim

$$\psi_\chi(x) := \frac{1}{2}\sum_{m=-\infty}^{\infty} \chi(m) e^{-\pi x m^2/f} = \sum_{m=1}^{\infty} \chi(m) e^{-\pi x m^2/f},$$

on l'última igualtat és perquè $\chi(m)$ i m^2 són funcions parelles. Enunciem dos proposicions que més tard demostrem, veure pàgina 15.

Proposició 1. *Siguin χ un caràcter de Dirichlet de conductor f, ζ_f una arrel f-èssima de la unitat i $G(\chi, \zeta_f)$ la suma de Gauss. Si n és un enter, tenim*

$$\bar{\chi}(n) G(\chi, \zeta_f) = G(\chi, \zeta_f^n). \tag{1.1}$$

Proposició 2. *Siguin χ un caràcter de Dirichlet de conductor f, ζ_f una arrel f-èssima de la unitat i $G(\chi, \zeta_f)$ la suma de Gauss. Aleshores*

$$|G(\chi, \zeta_f)| = \sqrt{f}. \tag{1.2}$$

A partir de la proposició 1 i utilitzant la fórmula de sumació de Poisson s'obté l'equació

$$G(\bar{\chi}, \zeta_f)\psi_\chi(x) = \left(\frac{f}{x}\right)^{\frac{1}{2}} \psi_{\bar{\chi}}\left(\frac{1}{x}\right), \tag{1.3}$$

veieu [7, fi p.118].
Primer, a la funció Gamma li fem un canvi de variable $t = \pi x m^2/f$

$$\Gamma(s/2) = \int_0^\infty e^{-t} t^{s/2-1} dt = \left(\frac{\pi m^2}{f}\right)^{s/2} \int_0^\infty e^{-\pi x m^2/f} x^{s/2-1} dx$$

Desenvolupant a la funció L completada s'obté

$$\begin{aligned}
\hat{L}(s,\chi) &= \left(\frac{f}{\pi}\right)^{s/2} L(s,\chi)\Gamma(s/2) \\
&= \left(\frac{f}{\pi}\right)^{s/2} \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \left(\frac{\pi m^2}{f}\right)^{s/2} \int_0^\infty e^{-\pi x m^2/f} x^{s/2-1} dx \\
&= \left(\frac{f}{\pi}\right)^{s/2} \left(\frac{\pi}{f}\right)^{s/2} \int_0^\infty \sum_{m=1}^{\infty} \chi(m) e^{-\pi x m^2/f} x^{s/2-1} dx \\
&= \int_0^\infty \psi_\chi(x) x^{s/2-1} dx
\end{aligned}$$

Obtenim:

$$\begin{aligned}
\hat{L}(s,\chi) &= \int_0^1 \psi_\chi(x) x^{s/2-1} dx + \int_1^\infty \psi_\chi(x) x^{s/2-1} dx \\
&= \int_1^\infty \psi_\chi\left(\frac{1}{x}\right) x^{-s/2-1} dx + \int_1^\infty \psi_\chi(x) x^{s/2-1} dx \\
&= \frac{f^{1/2}}{G(\bar{\chi}, \zeta_f)} \int_1^\infty \psi_{\bar{\chi}}(x) x^{(-1-s)/2} dx + \int_1^\infty \psi_\chi(x) x^{s/2-1} dx
\end{aligned}$$

on a la segona igualtat hem fet el canvi de variable x per $1/x$, a la tercera hem fet servir l'equació (1.3) canviant x per $1/x$.

Ara canviem s per $1-s$ i χ per $\bar{\chi}$

$$\hat{L}(1-s,\bar{\chi}) = \frac{f^{1/2}}{G(\chi,\zeta_f)}\int_1^\infty \psi_\chi(x)x^{s/2-1} + \int_1^\infty \psi_{\bar{\chi}}(x)x^{(-1-s)/2}dx,$$

fem el canvi de variable x per $1/x$ al sumant dret

$$\hat{L}(1-s,\bar{\chi}) = \frac{f^{1/2}}{G(\chi,\zeta_f)}\int_1^\infty \psi_\chi(x)x^{s/2-1} + \int_0^1 \psi_{\bar{\chi}}\left(\frac{1}{x}\right)x^{(s-3)/2}dx$$

i fem servir l'equació 1.3 a l'integral de la dreta

$$\hat{L}(1-s,\bar{\chi}) = \frac{f^{1/2}}{G(\chi,\zeta_f)}\int_1^\infty \psi_\chi(x)x^{s/2-1} + \frac{G(\bar{\chi},\zeta_f)}{f^{1/2}}\int_0^1 \psi_\chi x^{s/2-1}dx. \tag{1.4}$$

A l'equació 1.1 podem canviar χ per $\bar{\chi}$ i posar $n=-1$. Aleshores

$$\chi(-1)G(\bar{\chi},\zeta_f) = G(\bar{\chi},\zeta_f^{-1}) = \sum_{a=1}^{f}\bar{\chi}\zeta_f^{-a} = \sum_{a=1}^{f}\bar{\chi}\overline{\zeta_f^a} = \overline{G(\chi,\zeta_f)}$$

i com que $\chi(-1)=1$, s'obté

$$\frac{G(\bar{\chi},\zeta_f)}{\sqrt{f}} = \frac{\chi(-1)\overline{G(\chi,\zeta_f)}}{\sqrt{f}} = \frac{|G(\chi,\zeta_f)|^2}{\sqrt{f}G(\chi,\zeta_f)} = \frac{\sqrt{f}}{G(\chi,\zeta_f)}, \tag{1.5}$$

on a l'última igualtat fem servir la proposició 1.2. Ara substituim l'equació (1.5) a l'equació (1.4) i obtenim el que voliem

$$\hat{L}(s,\chi) = \frac{G(\chi,\zeta_f)}{\sqrt{f}}\hat{L}(1-s,\bar{\chi}).$$

Cas senar $\chi(-1)=-1$. Definim

$$\varphi_\chi(x) := \frac{1}{2}\sum_{-\infty}^{\infty} m\chi(m)e^{-\pi x m^2/f} = \sum_{m=1}^{\infty} m\chi(m)e^{-\pi x m^2/f}.$$

Igual que en el cas del caràcter de Dirichlet parell tenim una equació amb aquesta funció

$$G(\bar{\chi},\zeta_f)\varphi_\chi(x) = \frac{\sqrt{-1}f^{\frac{1}{2}}}{x^{\frac{3}{2}}}\varphi_{\bar{\chi}}\left(\frac{1}{x}\right). \tag{1.6}$$

Com abans, desenvolupem la funció $\hat{L}$ i dins la funció Gamma fem el canvi de variable t per $-\pi x m^2/f$. Ara observem $\epsilon(\chi)=1$.

$$\begin{aligned}
\hat{L}(s,\chi) &= f^{\frac{s}{2}}\pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi)\\
&= f^{-\frac{1}{2}}\int_0^\infty x^{\frac{s-1}{2}}\sum_{m=1}^{\infty} m\chi(m)e^{\frac{-\pi x m^2}{f}}dx\\
&= f^{-\frac{1}{2}}\int_0^\infty \varphi_\chi(x)x^{\frac{s-1}{2}}dx\\
&= f^{-\frac{1}{2}}\int_1^\infty \varphi_\chi(x)x^{\frac{s-1}{2}}dx + \frac{\sqrt{-1}}{G(\bar{\chi},\zeta_f)}\int_1^\infty \varphi_{\bar{\chi}}(x)x^{-\frac{s}{2}}dx
\end{aligned}$$

i similarment que el cas parell:

$$
\begin{aligned}
\hat{L}(1-s,\bar{\chi}) &= f^{-\frac{1}{2}}\int_1^\infty \varphi_{\bar{\chi}}(x)x^{-\frac{s}{2}}dx + \frac{\sqrt{-1}}{G(\chi,\zeta_f)}\int_1^\infty \varphi_\chi(x)x^{\frac{s-1}{2}}dx \\
&= \frac{\sqrt{-1}}{G(\chi,\zeta_f)}\int_0^1 \varphi_\chi(x)x^{\frac{s-1}{2}}dx + \frac{\sqrt{-1}}{G(\chi,\zeta_f)}\int_1^\infty \varphi_\chi(x)x^{\frac{s-1}{2}}dx \\
&= \frac{\sqrt{-1}f^{\frac{1}{2}}}{G(\chi,\zeta_f)}\bar{L}(s,\chi).
\end{aligned}
$$

Vegem-ne ara la continuació analítica.

Definició 5 (Transformada de mellin)**.** *Sigui $f:\mathbb{R}_{>0}\to\mathbb{C}$ una funció contínua, definim la transformada de Mellin de la funció f com*

$$M(f,s)=\int_0^\infty f(x)x^s\frac{dx}{x}.$$

Es pot trobar una demostració més general del següent teorema a [9, Teorema 1.4.]

Teorema 2. *Siguin $f,g:\mathbb{R}_{>0}\to\mathbb{C}$ funcions contínues tals que*

$$f(x)=O(e^{-cx^\alpha}),\qquad g(x)=O(e^{-cx^\alpha})$$

per $x\to\infty$ i constants positives c,α. Si f,g satisfan l'equació

$$f\left(\frac{1}{x}\right)=Cx^kg(x),$$

per algun nombre complex $C\neq 0$ i $k>0$ real, aleshores $M(f,s)$ i $M(g,s)$ admeten continuació analítica a $\mathbb{C}$.

Hem vist que la funció $\hat{L}$ es pot escriure com

$$\hat{L}(\chi,s)=\begin{cases}\int_0^\infty \psi_\chi(x)x^{\frac{s}{2}-1}dx & \text{si} \quad \chi \text{ parell}\\ \frac{1}{\sqrt{f}}\int_0^\infty \varphi_\chi(x)x^{\frac{s-1}{2}}dx & \text{si} \quad \chi \text{ senar,}\end{cases}$$

i per tant $\hat{L}(\chi,s)$ és una transformada de Mellin de les funcions ψ_χ i φ_χ. Apliquem el teorema 2 pels casos χ parell i senar, per separat. Si χ és parell definim $f(x)=\psi_\chi(x)$ i $g(x)=\psi_{\bar{\chi}}(x)$. Aleshores $f(x)=O(e^{-\pi x/f})$ i $g(x)=O(e^{-\pi x/f})$. Per les equacions (1.3) i (1.5) tenim

$$f\left(\frac{1}{x}\right)=W(\chi)\sqrt{x}g(x).$$

Si χ és senar definim $f(x)=\varphi_\chi(x)$ i $g(x)=\varphi_{\bar{\chi}}(x)$ on $f(x)=O(e^{-\pi x/f})$ i $g(x)=O(e^{-\pi x/f})$. Per les equacions (1.6) i (1.5) obtenim

$$f\left(\frac{1}{x}\right)=-W(\chi)x^{3/2}g(x).$$

Per tant pel teorema 2 la funció $\hat{L}(\chi,s)$ té continuació analítica a tot el pla complex. Ja hem observat que la funció Γ té continuació analítica, aleshores concluim que la funció $L(\chi,s)$ també. □

Observació 2. *Si χ_0 és el caràcter trivial aleshores $L(s, \chi_0) = \zeta(s)$ és la funció zeta de Riemann. Es sap que la funció ζ es pot estendre analíticament a tot el pla complex excepte al punt $s = 1$ on té un pol simple. Aleshores obtenim que la funció L de Dirichlet té un pol simple quan $s = 1$ i χ és el caràcter trivial. veieu per exemple [10, T. 2.5.].*

Vegem ara com obtenim el valor de $L(1-n, \chi)$ en termes de nombre de Bernoulli que sabem calcular.

Definició 6 (Nombres de Bernoulli)**.** *Definim els nombres de Bernoulli ordinaris com els nombres $B_n \in \mathbb{C}$ que satisfan*

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!},$$

del desenvolupament en sèrie en t.

Definició 7 (Nombres de Bernoulli generalitzats)**.** *Sigui χ un caràcter de Dirichlet de conductor f, definim els nombres de Bernoulli generalitzats associats a χ com els nombres $B_{n,\chi} \in \mathbb{C}$ que satisfan*

$$\sum_{a=0}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

Definició 8 (Polinomis de Bernoulli)**.** *Definim els polinomis de Bernoulli $B_n(X) \in \mathbb{C}[X]$ com*

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X) \frac{t^n}{n!}.$$

Tenim tres resultats que ens serveixen per a calcular els nombres de Bernoulli generalitzats, veieu-ne una demostració a [15, p. 32].

Proposició 3. $B_n(1 - X) = (-1)^n B_n(X)$

Proposició 4. $B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$

Proposició 5. *Sigui F un múltiple de f. Aleshores*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

Definició 9 (Funció zeta de Hurwitz)**.** *Sigui s un nombre complex i x un nombre real, definim la funció zeta de Hurwitz com*

$$\zeta(s, x) = \sum_{n=0}^{\infty} \frac{1}{(x+n)^s}.$$

Aquesta sèrie és convergent per $Re(s) > 1$ i $x > 0$, veieu [2, Teorema 12.1.].

Proposició 6. *Tenim*

$$L(s, \chi) = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta(s, \frac{a}{f}), \tag{1.7}$$

on f és el conductor associat a χ.

Demostració. Fem

$$f^{-s}\zeta(s,\frac{a}{f}) = f^{-s}\sum_{n=0}^{\infty}\frac{1}{(\frac{a}{f}+n)^s} = f^{-s}\sum_{n=0}^{\infty}\frac{f^s}{(a+fn)^s} = \sum_{m\equiv a(f)}\frac{1}{m^s}.$$

Aleshores la part dreta de (1.7) queda

$$\sum_{a=1}^{f}\chi(a)\sum_{m\equiv a(f)}\frac{1}{m^s} = \sum_{m=1}^{\infty}\frac{\chi(m)}{m^s} = L(s,\chi), \qquad \text{per a } s>1.$$

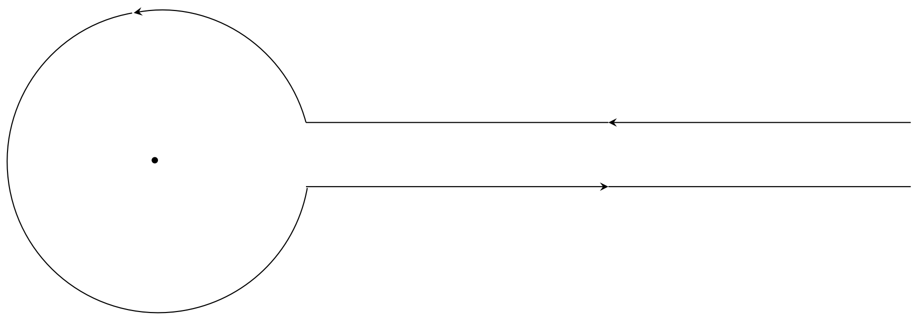
□

Teorema 3 (Funció L de Dirichlet a valors negatius)**.** *Tenim $L(1-n,\chi) = -B_{n,\chi}/n$ i $\zeta(1-n,b) = -B_n(b)/n$, per a $n \geq 1$ i $0 < b \leq 1$.*

Demostració. Sigui

$$F(t) = \frac{te^{(1-b)t}}{e^t-1} = \sum_{n=0}^{\infty}B_n(1-b)\frac{t^n}{n!}$$

la definició dels polinomis de Bernoulli amb $x = 1-b$.
Sigui $H(s) = \int F(z)z^{s-2}dz$ la integral sobre el següent camí orientat positivament



que consisteix en un cercle C_ϵ de radi $\epsilon > 0$ i dues còpies de la recta real positiva. Calculem la integral en tres parts. Per la recta de dalt posem $z^{s-2} = e^{(s-2)log(z)}$ i triem la determinació amb $arg(z) = 2\pi i$. Així la integral sobre la recta de dalt queda

$$\int_\infty^\epsilon F(t)e^{(s-2)(ln(t)+2\pi i)}dt = -e^{2s\pi i}\int_\epsilon^\infty F(t)t^{s-2}dt,$$

Amb les tres integrals tenim

$$H(s) = (e^{2\pi is}-1)\int_\epsilon^\infty F(t)t^{s-2}dt + \int_{C_\epsilon}F(z)z^{s-2}dz.$$

Si suposem $Re(s) > 1$ aleshores

$$\left|\int_{C_\epsilon}F(z)z^{s-2}\right| \leq \int_0^{2\pi}\left|F(\epsilon e^{it})(\epsilon e^{it})^{s-1}\right|dt \xrightarrow{\epsilon\to 0} 0$$

i per tant, per a $\epsilon \to 0$

$$H(s) = (e^{2\pi is}-1)\int_0^\infty F(t)t^{s-2}dt$$

ara fent

$$\sum_{n=0}^{\infty} e^{-(b+n)t} = e^{-bt}\sum_{n=0}^{\infty}(e^{-t})^n = \frac{e^{-bt}}{1-e^{-t}} = \frac{e^{(1-b)t}}{e^t-1} = F(t)/t$$

i per tant

$$\begin{aligned} H(s) &= (e^{2\pi is}-1)\int_0^{\infty} t^{s-1}\sum_{n=0}^{\infty} e^{-(b+n)t}dt \\ &= (e^{2\pi is}-1)\sum_{n=0}^{\infty}\int_0^{\infty} t^{s-1}e^{-(b+n)t}dt \\ &= (e^{2\pi is}-1)\sum_{n=0}^{\infty}\frac{\Gamma(s)}{(n+b)^s} \\ &= (e^{2\pi is}-1)\Gamma(s)\zeta(s,b) \end{aligned}$$

on a la penúltima igualtat hem fet el canvi de variable $u = (b+n)t$. Per tant hem obtingut $\zeta(s,b) = H(s)/(e^{2\pi is}-1)\Gamma(s)$. Com que $H(s)$ és analítica i $\Gamma(s)$ té continuació analítica a $\mathbb{C}$, obtenim que $\zeta(s,b)$ té continuació analítica tret de $s=1$ on Γ no té pol. Assumim ara que $s = 1-n$ amb $n \geq 1$ enter. Aleshores $e^{2\pi is} = 1$ i

$$H(1-n) = \int_{C_\epsilon} F(z)z^{-n-1}dz = \int_0^{2\pi} i\frac{B_n(1-b)}{n!}dt = (2\pi i)\frac{B_n(1-b)}{n!}.$$

Es pot demostrar que

$$\lim_{s\longrightarrow 1-n}(e^{2\pi is}-1)\Gamma(s) = \frac{(2\pi i)(-1)^{n-1}}{(n-1)!}.$$

Amb l'equació anterior, $\zeta(s,b) = H(s)/(e^{2\pi is}-1)\Gamma(s)$ i $B_n(1-x) = (-1)^nB_n(x)$ obtenim

$$\zeta(1-n,b) = (-1)^{n-1}\frac{B_n(1-b)}{n} = -\frac{B_n(b)}{n}.$$

Per acabar, amb la proposició 6 obtenim les igualtats següents:

$$L(1-n,\chi) = \sum_{a=1}^{f}\chi(a)f^{-s}\zeta(1-n,\frac{a}{f}) = -\frac{1}{n}\sum_{a=1}^{f}\chi(a)f^{n-1}B_n\left(\frac{a}{f}\right) = -\frac{B_{n,\chi}}{n},$$

on hem fet servir la proposició 5 a l'última igualtat. □

Observació 3. *Per la proposició 6 la continuació analítica de $\zeta(s,b)$ ens dóna també la contínuació analítica de $L(s,\chi)$.*

Anem a avaluar $L(s,\chi)$ a $s=1$. Per a χ senar, per l'equació funcional

$$\hat{L}(1,\chi) = W(\chi)\hat{L}(0,\bar{\chi}),$$

escrivim

$$\hat{L}(1,\chi) = \left(\frac{f}{\pi}\right)^{1/2}\Gamma\left(\frac{1}{2}\right)L(1,\chi)$$

$$\hat{L}(0,\bar{\chi}) = \left(\frac{f}{\pi}\right)^{0/2} \Gamma\left(\frac{0}{2}\right) L(0,\bar{\chi})$$

$$W(\chi) = \frac{G(\chi,\zeta_f)}{i\sqrt{f}},$$

i obtenim

$$L(1,\chi) = \frac{G(\chi,\zeta_f)\pi}{if} L(0,\bar{\chi})$$

Pel teorema 3:

$$L(1,\chi) = \frac{\pi i G(\chi,\zeta_f)}{f} B_{1,\bar{\chi}}.$$

Per la proposició 4 obtenim

$$B_1(x) = \sum_{i=0}^{1} \binom{1}{i} B_i x^{1-i} = \binom{1}{0} B_0 x + \binom{1}{1} B_1 x^0 = x - \frac{1}{2},$$

i de la proposició 5:

$$B_{1,\bar{\chi}} = \sum_{a=1}^{f} \bar{\chi}(a) B_1\left(\frac{a}{f}\right) = \sum_{a=1}^{f} \bar{\chi}(a)(\frac{a}{f} - \frac{1}{2}) = \frac{1}{f}\sum_{a=1}^{f} \bar{\chi}(a)a,$$

de $\sum_{a=1}^{f} \bar{\chi}(a) = 0$ de ser $\bar{\chi}$ no trivial. Per tant l'expressió de $L(1,\chi)$ per a caràcters de Dirichlet senars queda

$$L(1,\chi) = \pi i \frac{G(\chi,\zeta_f)}{f} \frac{1}{f} \sum_{a=1}^{f} \bar{\chi}(a)a. \tag{1.8}$$

Busquem ara una expressió per a $L(1,\chi)$ amb χ parell.
Evaluem $L(1,\chi)$. Per la proposició 1 tenim $\chi(n) = \frac{\sum_{a=1}^{f} \bar{\chi}(a) e^{2\pi i a n/f}}{G(\bar{\chi},\zeta_f)}$, per tant

$$\begin{aligned} L(1,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{1}{nG(\bar{\chi},\zeta_f)} \sum_{a=1}^{f} \bar{\chi}(a) e^{2\pi i a n/f} \\ &= \frac{1}{G(\bar{\chi},\zeta_f)} \sum_{a=1}^{f} \bar{\chi}(a) \sum_{n=1}^{\infty} \frac{(\zeta_f^a)^n}{n} \end{aligned}$$

ara podem fer servir l'expansió de Taylor $log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$ i queda

$$L(1,\chi) = -\frac{1}{G(\bar{\chi},\zeta_f)} \sum_{a=1}^{f} \bar{\chi}(a) log(1-\zeta_f^a). \tag{1.9}$$

Si fem servir la proposició 1 amb $n=-1$ i canviant χ per $\bar{\chi}$ obtenim

$$\chi(-1)G(\bar{\chi},\zeta_f) = G(\bar{\chi},\zeta_f^{-1}) = G(\bar{\chi},\bar{\zeta_f}) = \overline{G(\chi,\zeta_f)}$$

i per la proposició 2 tenim $\overline{G(\chi,\zeta_f)}G(\chi,\zeta_f) = |G(\chi,\zeta_f)|^2 = (\sqrt{f})^2 = f$ i per tant

$$G(\bar{\chi},\zeta_f) = \chi(-1)f/G(\chi,\zeta_f).$$

Substituint a l'equació 1.9 i, com que χ es parell, obtenim

$$L(1,\chi) = -\frac{G(\chi,\zeta_f)}{f}\sum_{a=1}^{f}\bar{\chi}(a)log(1-\zeta_f^a).$$

Ara fem

$$\begin{aligned} log(1-\zeta_f^a) + log(1-\zeta_f^{-a}) &= log((1-\zeta_f^a)(1-\zeta_f^{-a})) \\ &= log((1-\zeta_f^a)\overline{(1-\zeta_f^a)}) \\ &= log|1-\zeta_f^a|^2 \\ &= 2log|1-\zeta_f^a|. \end{aligned}$$

A la següent suma podem canviar a per $-a$ sense alterar-la

$$\begin{aligned} \sum_{a=1}^{f}\bar{\chi}(a)log(1-\zeta_f^a) &= \sum_{a\in(\mathbb{Z}/f\mathbb{Z})^\times}\bar{\chi}(a)log(1-\zeta_f^a) \\ &= \sum_{a\in(\mathbb{Z}/f\mathbb{Z})^\times}\bar{\chi}(-a)log(1-\zeta_f^{-a}) \\ &= \sum_{a=1}^{f}\bar{\chi}(a)log(1-\zeta_f^{-a}), \end{aligned}$$

ja que $\chi(-a) = \chi(-1)\chi(a) = \chi(a)$. Aleshores

$$\begin{aligned} \sum_{a=1}^{f}\bar{\chi}(a)log|1-\zeta_f^a| &= \frac{1}{2}(\sum_{a=1}^{f}\bar{\chi}(a)log(1-\zeta_f^a) + \sum_{a=1}^{f}\bar{\chi}(a)log(1-\zeta_f^{-a})) \\ &= \sum_{a=1}^{f}\bar{\chi}(a)log(1-\zeta_f^a) \end{aligned}$$

Finalment hem obtingut

$$L(1,\chi) = \frac{-G(\chi,\zeta_f)}{f}\sum_{a=1}^{f}\bar{\chi}(a)log|1-\zeta_f^a|. \tag{1.10}$$

Demostració proposicions 1 i 2

Demostració proposició 1. Si $(n,f)=1$ aleshores $\chi^{-1}(n) = \bar{\chi}(n)$ i fent el canvi de variables $b \equiv an (\mathrm{mod}\ f)$ podem reescriure la part dreta de l'equació (1.1)

$$G(\chi,\zeta_f^n) = \sum_{a=1}^{f}\chi(a)\zeta_f^{an} = \bar{\chi}(n)\sum_{a=1}^{f}\chi(an)\zeta_f^{an} = \bar{\chi}(n)\sum_{b=1}^{f}\chi(b)\zeta_f^{b},$$

on a l'última igualtat es fa servir que tant χ com ζ_f depenen només de les classes mòdul f.

Si n i f no són coprimers, escrivim $1 < d = (n, f)$.
A l'esquerra de l'equació (1.1) $\chi(n) = 0$. Vegem que la dreta també val zero. Suposem que $\chi(y) = 1$ per tot $y \equiv 1(\text{mod } f/d)$ i amb $(y, f) = 1$. Aleshores tindriem la composició

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \longrightarrow (\mathbb{Z}/(f/d)\mathbb{Z})^* \xrightarrow{\chi'} \mathbb{C}^\times$$

on χ' és χ mod f/d i estaria ben definit. Llavors el conductor de χ seria menor o igual que f/d i no podria ser f. Per tant existeix $y \equiv 1(\text{mod } f/d)$ amb $(y, f) = 1$ tal que $\chi(y) \neq 1$. Com que $y \equiv 1(\text{mod } f/d)$ també $dy \equiv d(\text{mod } f)$ i per tant $ny \equiv n(\text{mod } f)$. Multiplicant $G(\chi, \zeta_f^n)$ per $\chi(y)$ obtenim

$$\chi(y)\sum_{a=1}^{f}\chi(a)e^{2\pi i n a/f} = \sum_{a=1}^{f}\chi(ay)e^{2\pi i n y a/f},$$

i fent el canvi de variable $b \equiv ay(\text{mod } f)$ obtenim

$$\chi(y)G(\chi, \zeta_f^n) = G(\chi, \zeta_f^n)$$

i de $\chi(y) \neq 1$ tenim $G(\chi, \zeta_f^n) = 0$. □

Demostració proposició 2. Agafem els quadrats dels valors absoluts de l'equació (1.1)

$$|\bar{\chi}(n)|^2|G(\chi, \zeta_f)|^2 = |G(\chi, \zeta_f^n|^2 = G(\chi, \zeta_f^n)G(\bar{\chi}, \zeta_f^{-n}) = \sum_{a,b}\chi(a)\bar{\chi}(b)\zeta_f^{(a-b)n}$$

i sumem per $n = 1, \ldots, f$:

$$\sum_{n=1}^{f}|\bar{\chi}(n)|^2|G(\chi, \zeta_f)|^2 = \sum_{n=1}^{f}\sum_{a,b}\chi(a)\bar{\chi}(b)\zeta_f^{(a-b)n} = \sum_{a,b}\chi(a)\bar{\chi}(b)\sum_{n=1}^{f}\zeta_f^{(a-b)n}$$

on desapareixen els termes $a \neq b$ de $\zeta_f^{(a-b)f-1} + \cdots + \zeta_f^{(a-b)} + 1 = \frac{\zeta_f^{(a-b)f}-1}{\zeta_f^{(a-b)}-1} = 0$ i d'on

$$\sum_{n=1}^{f}|\bar{\chi}(n)|^2|G(\chi, \zeta_f)|^2 = \sum_{a=1}^{f}|\chi(a)|^2 f$$

perquè $|\bar{\chi}(n)|^2 = \bar{\bar{\chi}}(n)\bar{\chi}(n) = |\chi(n)|^2$. □

Definició 10 (Funció zeta de Dedekind)**.** *Sigui K un cos amb $K/\mathbb{Q}$ finita. Definim la funció zeta associada a K amb $s \in \mathbb{C}$ via*

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} \qquad \text{per a } Re(s) >> 0$$

on $\mathfrak{a}$ recorre els ideals no nuls de l'anell d'enters $\mathcal{O}_K$ de K on $\mathcal{O}_K = \{\alpha \in K | Irr(\alpha, K)[x] \in \mathbb{Z}[x]\}$ i $N(\mathfrak{a})$ és el nombre d'elements de l'anell finit $\mathcal{O}_K/\mathfrak{a}$.

Proposició 7. *Per a $Re(s) \geq 1$ tenim*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}}\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

on $\mathfrak{a}$ recorre els ideals de $\mathcal{O}_K$ i $\mathfrak{p}$ recorre els ideals primers de $\mathcal{O}_K$. A més, $\zeta_K(s)$ té prolongació analítica a tot el plà complex, amb un únic pol en $s = 1$. Veieu [9, capítol 5].

Proposició 8. *L'anell $\mathcal{O}_K$ és un domini de Dedekind, és a dir, tot ideal de $\mathcal{O}_K$ s'escriu de manera única (llevat de l'ordre) com a producte d'ideals primers de $\mathcal{O}_K$. Per aprofundir dominis de Dedekind mireu [8, cap.1]*

Teorema 4. *Sigui X un grup format per caràcters de Dirichlet i K el cos associat. Aleshores*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Demostració. Recordem les definicions de ζ_K i $L(s, \chi)$. Tenim

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

on $\mathfrak{p}$ recorre els ideals primers de $\mathcal{O}_K$. L'expansió multiplicativa d'Euler de la funció L de Dirichlet pel caràcter χ és

$$L(s, \chi) = \prod_{p} (1 - \chi(p)p^{-s})^{-1}$$

on p recorre els nombres primers de $\mathbb{Z}$. Aquests productes d'Euler convergeixen per a $Re(s) > 1$.
Sigui $p \in \mathbb{Z}$ primer. Com $K/\mathbb{Q}$ és una extensió finita i $\mathcal{O}_K$ Dedekind tenim que $p\mathcal{O}_K$ s'escriu com

$$p\mathcal{O}_K = \mathfrak{p}_1^e \dots \mathfrak{p}_g^e \tag{1.11}$$

amb el mateix exponent e per ser $K/\mathbb{Q}$ Galois. Notem que si fixem un primer p podem escriure

$$\prod_{\chi \in X} L(s, \chi) = \prod_{p \text{ primer}} \prod_{\chi \in X} (1 - \chi(p)p^{-s})^{-1},$$

per tant l'equació que volem demostrar és equivalent a provar

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = \prod_{\chi \in X} (1 - \chi(p)p^{-s}),$$

per cada nombre primer p de $\mathbb{Z}$, on $\mathfrak{p}$ són els ideals de $\mathcal{O}_K$ que apareixen en (1.11).

Sigui $N(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i|$ i sigui in_f el grau residual, és a dir, $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p] = in_f$ i de ser $K/\mathbb{Q}$ Galois in_f és igual en tot $\mathfrak{p}_i$ de (1.11). Aleshores com que $\mathcal{O}_K/\mathfrak{p}_i$ és un cos finit, el podem escriure com $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_{p^{in_f}}$ i per tant $N(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| = p^{in_f}$, per a qualsevol $i \in \{1, \dots, g\}$. Aleshores

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}|p} (1 - p^{-in_f s}) = (1 - p^{-in_f s})^g,$$

ja que hi ha g $\mathfrak{p}$'s que divideixen p. Per tant ens queda demostrar

$$\prod_{\chi} (1 - \chi(p)p^{-s}) = (1 - p^{-in_f s})^g$$

amb un nombre primer p fixat.
Tenim

$$\prod_{\chi} (1 - \chi(p)p^{-s}) = \prod_{\chi, \chi(p) \neq 0} (1 - \chi(p)p^{-s}),$$

ja que si $\chi(p) = 0$ per algun p aleshores $(1 - \chi(p)p^{-s}) = 1$ i no influeix en el producte. Usem el següent resultat:

Teorema 5. *Sigui X un grup de caràcters de Dirichlet amb K el cos associat, i sigui p un primer enter fixat. Definim els subgrups de X:*

$$Y = \{\chi \in X | \chi(p) \neq 0\}, \qquad Z = \{\chi \in X | \chi(p) = 1\}.$$

Aleshores $in_f = [Y : Z]$ és el grau residual, $g = [Z : 1]$ és el nombre de primers de $\mathcal{O}_K$ que divideixen p i Y/Z és cíclic d'ordre in_f .

La prova d'aquest teorema es pot trobar a [15, teorema 3.7].

Prenem aleshores Z i Y com en el teorema 5. Si ψ són els caràcters de Dirichlet de Z i χ els de Y, les classes d'equivalència de Y/Z serien doncs

$$[\chi] = \{\chi\psi_1, \chi\psi_2, \dots, \chi\psi_g\}$$

que té g elements de X. Com que Y/Z és cíclic podem triar-ne un generador $< [\chi'] >$. Notem que $[\chi']^{in_f} = [\chi_0]$ és el caràcter trivial. Ara sigui χ un caràcter de X. Si pensem χ com un caràcter de Galois tenim que cada χ envia p a una de les in_f arrels in_f-èssimes de la unitat. Aleshores $\chi'\psi_i(p) = \chi'(p)\psi_i(p) = \zeta_{in_f}^a \cdot 1$, per alguna $0 \leq a \leq in_f - 1$ i alguna $i = 1, \dots, g$. D'aquí obtenim que $[\chi'](p) = \zeta_{in_f}^a$ per alguna $0 \leq a \leq in_f - 1$. Com que $[\chi']$ genera Y/Z tenim

$$\begin{aligned}\prod_{\chi, \chi(p) \neq 0} (1 - \chi(p)p^{-s}) &= \prod_{j=0}^{in_f - 1} (1 - [\chi'(p)]^j p^{-s})^g \\ &= \prod_{j=0}^{in_f - 1} (1 - \zeta_{in_f}^{aj} p^{-s})^g,\end{aligned}$$

ja que cada classe lateral té g elements. Per tant només queda demostrar

$$\prod_{j=0}^{in_f - 1} (1 - \zeta_{in_f}^{aj} p^{-s}) = 1 - p^{-in_f s}.$$

Sabem que

$$\prod_{j=0}^{in_f - 1} (x - \zeta_{in_f}^{aj}) = x^{in_f} - 1,$$

i multiplicant per p^{-sf} als dos costats

$$\prod_{j=0}^{in_f - 1} (p^{-s}x - p^{-s}\zeta_f^{aj}) = p^{-in_f s (x^{in_f} - 1)}.$$

Si definim $y := p^{-s}x$ queda

$$\prod_{j=0}^{in_f - 1} (y - p^{-s}\zeta_{in_f}^{aj}) = p^{-in_f s}((yp^s)f - 1) = y^{in_f} - p^{-in_f s},$$

i si posem $y = 1$ aleshores

$$\prod_{j=0}^{in_f - 1} (1 - p^{-s}\zeta_{in_f}^{aj}) = p^{-in_f s}((p^s)in_f - 1) = 1 - p^{-in_f s}.$$

Tenim la igualtat per $Re(s) > 1$, per continuació analítica es compleix per tot $s \in \mathbb{C}$. $\square$

Corol·lari 1. *Sigui χ un caràcter de Drichlet cos associat K i conductor f, aleshores $L(1,\chi) \neq 0$.*

Demostració. Es sap que la funció ζ_K té un pol simple a $s = 1$. Com hem vist a la demostració del teorema 4 podem escriure

$$\zeta_K(s) = \prod_{a=0}^{f-1} L(s,\chi^a) = \zeta(s) \prod_{a=1}^{f-1} L(s,\chi^a),$$

ja que $L(s,\chi_0) = \zeta(s)$. Com que $\zeta(s)$ també té un únic pol simple a $s = 1$, el producte $\prod_{a=1}^{f-1} L(s,\chi^a)$ no pot valer zero i en particular tampoc cada $L(s,\chi^a)$ quan $s = 1$. $\square$

Teorema 6 (Dirichlet)**.** *Siguin $a, n \in \mathbb{Z}$ fixats amb $(a,n) = 1$, aleshores hi ha infinits nombres primers p que compleixen $p \equiv a(mod\ n)$.*

Demostració. Per $Re(s) > 1$ tenim

$$\begin{aligned}
log(L(s,\chi)) &= log(\prod_p (1-\chi(p)p^{-s})^{-1}) \\
&= -\sum_p log(1-\chi(p)p^{-s}) \\
&= \sum_p \sum_{n=1}^{\infty} \frac{\chi^n(p)p^{-sn}}{n} \\
&= \sum_p \frac{\chi(p)}{p^s} + O\left(\sum_p \frac{1}{p^{2s}}\right) \\
&= \sum_p \frac{\chi(p)}{p^s} + O(1),
\end{aligned}$$

la tercera igualtat per l'expansió de la funció $log(1-x)$ en sèrie de Taylor i l'útima perquè la sèrie $\sum_p \frac{1}{p^{2s}}$ convergeix.
Ja sabem que si $(a,n) = 1$ i $a \not\equiv 1(\text{mod } n)$ aleshores $\sum_{\chi \in X} \chi(a) = 0$, per algun grup X format per caràcters de Dirichlet χ. Aleshores sigui X el grup format pels caràcters de Dirichlet mòdul n, fem

$$\begin{aligned}
\sum_{\chi \in X} \chi(a^{-1}) log(L(s,\chi)) &= \sum_{\chi \in X} \sum_p \frac{\chi(pa^{-a})}{p^s} + \sum_{\chi \in X} \chi(a^{-1}) \\
&= \sum_{p \equiv a(n)} \frac{\sum_{\chi \in X} \chi(1)}{p^s} + 0 \\
&= \sum_{p \equiv a(n)} \frac{\phi(n)}{p^s},
\end{aligned}$$

on hem fet servir que $|X| = |Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, la funció phi d'Euler. A la segona igualtat els termes tals que $pa^{-1} \not\equiv 1(\text{mod } n)$ desapareixen i només queden els $p \equiv a(\text{mod } n)$.

Si χ_0 és el caràcter trivial, tenim el límit $\lim_{s\to 1} log(L(s,\chi_0)) = log(\lim_{s\to 1}\zeta(s)) = \infty$ ja que $\zeta(s)$ té un pol a $s = 1$. Notem que pel corol·lari 1 $L(1,\chi) \neq 0$ i per tant si $s \to 1$, la funció $log(L(s,\chi))$ es manté acotada si $\chi \neq \chi_0$. Finalment obtenim

$$\lim_{s\to 1} \sum_{p\equiv a(n)} \frac{\phi(n)}{p^s} = \infty,$$

i aquesta suma no pot tenir finits termes. Per tant hi ha infinits primers $p \equiv a(\bmod\ n)$. □

2 La fórmula del nombre de classes

Definició 11 (Ideals fraccionaris i grup d'ideals fraccionaris)**.** *Sigui K un cos de nombres algebraics és a dir $K/\mathbb{Q}$ una extensió finita. Si existeix un element c a $\mathcal{O}_K$ tal que $c\mathfrak{a}$ és un ideal no nul de $\mathcal{O}_K$, per a un subconjunt $\mathfrak{a}$ de K, aleshores $\mathfrak{a}$ s'anomena ideal fraccionari de $\mathcal{O}_K$.*

Proposició 9. *Siguin $\mathfrak{a}, \mathfrak{b}$ ideals fraccionaris de K, definim el producte $\mathfrak{ab}$ com l'ideal format pels elements $\sum_{i=1}^{n} a_i b_i$, on $n \geq 1$ i $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$. Amb aquest producte, el conjunt de tots els ideals fraccionaris de $\mathcal{O}_K$ és un grup.*

Definició 12 (Classes d'ideals)**.** *Sigui K un cos de nombres algebraics. El grup de classes d'ideals $Cl(K)$ de K és el quocient del grup d'ideals fraccionaris de $\mathcal{O}_K$ pel subgrup dels ideals fraccionaris principals.*

Teorema 7. *Si $K/\mathbb{Q}$ és un cos de nombres, $Cl(k)$ és un grup finit i denotem per h_K a $|Cl(K)|$ que anomenem nombre de classes de K.*

Una demostració del teorema 7 es pot trobar a [9, capítol 2, teorema 6.3].

Definició 13 (Places reals i places complexes de K)**.** *Sigui K un cos de nombres, és a dir $K/\mathbb{Q}$ finita, existeix α on $K = \mathbb{Q}(\alpha)$ i*

$$Irr(\alpha,\mathbb{Q})[x] = \prod_{i=1}^{r_1}(x-\alpha_i)\prod_{j=r_1+1}^{r_1+r_2}(x-\alpha_j)(x-\overline{\alpha_j}) \in \mathbb{C}[x],$$

on r_1 és el nombre d'arrels reals i r_2 el nombre d'arrels complexes i no reals (identificadaes via la conjugació complexa). Observem $[K:\mathbb{Q}] = r_1 + 2r_2$. Es veu que no depèn de α on $K = \mathbb{Q}(\alpha)$, r_1 s'anomena el nombre de places reals de K i r_2 el nombre de places complexes de K. Si S és el conjunt de totes les places reals i complexes de K aleshores les places $v \in S$ diem que divideixen ∞ i escriurem $v|\infty$.

Definició 14 (Norma i traça)**.** *Siguin L/K una extensió de cossos. Sigui $\beta \in L$, definim l'aplicació K-lineal multiplicació per β com $L \to L$ tal que $x \mapsto \beta x$. Aleshores el determinant i la traça d'aquesta aplicació com K-espais vectorials són la norma $N_{L/K}$ i la traça $Tr_{L/K}$, respectivament.*

Si tenim una extensió de Galois $K/\mathbb{Q}$ on K és un cos de nombres, la norma i la traça es poden calcular via

$$N(\beta) = \prod_{\sigma\in Gal(K/\mathbb{Q})} \sigma(\beta) \qquad Tr_{K/\mathbb{Q}}(\beta) = \sum_{\sigma\in Gal(K/\mathbb{Q})} \sigma(\beta),$$

veieu [3, prop 2.1.6.].

Definició 15 (Discriminant)**.** *Sigui K un cos de nombres algebraics. Sigui $n = [K : \mathbb{Q}]$, triem una base $\alpha_1, \ldots, \alpha_n$ per l'anell d'enters $\mathcal{O}_K$ com a $\mathbb{Z}$ mòdul. Definim el discriminant de K com*

$$D_K = det((Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j}).$$

Es demostra que D_K és independent de la base triada de $\mathcal{O}_K$ com a grup abelià ($\mathbb{Z}$-mòdul).

Demostrem ara un resultat important que relaciona el discriminant d'un cos K amb el conductor d'un grup de caràcters de Dirichlet associats a K.

Teorema 8 (Fórmula del conductor-discriminant)**.** *Sigui K un cos de nombres algebraics associat a un grup X format per caràcters de Dirichlet. Aleshores*

$$D_K = (-1)^{r_2} \prod_{\chi \in X} f_\chi.$$

Demostració. Sigui $K/\mathbb{Q}$ una extensió finita i separable, tenim $K = \mathbb{Q}(\alpha)$, escrivim

$$p(x) \in Irr(\alpha, \mathbb{Q})[x] \quad \text{on} \quad p(x) = \prod_{i=1}^{r_1}(x - \alpha_i) \prod_{j=r_1+1}^{r_1+r_2} (x - \alpha_j)(x - \overline{\alpha_j}),$$

amb α_i reals per $1 \leq i \leq r_1$ i $r_1 + 1 \leq j \leq r_1 + r_2$ α_j complexes i no reals. Tenim

$$\begin{aligned} \sigma_i : K &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto \alpha_i \end{aligned} \qquad\qquad \begin{aligned} \sigma_j : K &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto \alpha_j \\ \alpha &\longmapsto \overline{\alpha_j} \end{aligned}$$

donen places reals i complexes on $N = [K : \mathbb{Q}] = r_1 + 2r_2$. Com $K/\mathbb{Q}$ és Galois $\exists \sigma \in Gal(K/\mathbb{Q})$ complint $\sigma(\alpha_i) = \alpha_k$ per $i \neq k$, d'aquí $r_1 = 0$ ó $r_2 = 0$.

Suposem que $r_2 = 0$ aleshores $r_1 = N$. Notem també que quan $r_2 = 0$, la conjugació complexa deixa els elements de K invariants i per tant el morfisme $\zeta \mapsto \zeta^{-1}$ ha d'estar al nucli del caràcter de Dirichlet que té K associat i per tant tenim $\chi(-1) = 1$. Es sap que la funció zeta de Dedekind satisfà una equació funcional

$$A^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s) = A^{1-s} \Gamma\left(\frac{1-s}{2}\right)^{r_1} \Gamma(1-s)^{r_2} \zeta_K(1-s),$$

on

$$A = 2^{-r_2} \pi^{-N/2} \sqrt{|D_K|}.$$

Agafem també l'equació funcional de la funció L de Dirichlet i sumem per tot $\chi \in X$. Queda

$$(\prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right))^{s/2} \Gamma\left(\frac{s}{2}\right)^N \sum_{\chi \in X} L(s, \chi) = W_\chi(\prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right))^{(1-s)/2} \Gamma\left(\frac{1-s}{2}\right)^N \prod_{\chi \in X} L(1-s, \bar{\chi}),$$

que pel teorema 4 obtenim

$$(\prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right))^{s/2} \Gamma\left(\frac{s}{2}\right)^N \zeta_K(s) = W_\chi(\prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right))^{(1-s)/2} \Gamma\left(\frac{1-s}{2}\right)^N \zeta_K(1-s),$$

que podem comparar amb l'equació funcional de ζ_K amb $r_2 = 0$ i $r_1 = N$

$$A^s\Gamma\left(\frac{s}{2}\right)^N \zeta_K(s) = A^{1-s}\Gamma\left(\frac{1-s}{2}\right)^N \zeta_K(1-s),$$

i ràpidament ens adonem que per força

$$A^2 = \prod_{\chi\in X}\left(\frac{f_\chi}{\pi}\right)$$

i

$$\prod_{\chi\in X} W_\chi = 1.$$

Per tant amb l'expressió d'A obtenim el resultat que voliem

$$|D_K| = \prod_{\chi\in X} f_\chi.$$

Per a $r_1 = 0$ i $r_2 = N/2$ es fa de manera similar. Utilitzant la identitat

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = 2^{1-s}\sqrt{\pi}\Gamma(s),$$

podem tornar a comparar les equacions funcionals de L i ζ_K, però ara els caràcters són la meitat parells i la meitat senars i per tant el signe del discriminant depèn de r_2. $\square$

Observació 4. *Si $K/\mathbb{Q}$ és una extensió de grau 2, podem calcular fàcilment f si tenim el discriminant.*

Definició 16 (Xarxa a $\mathbb{R}^n$)**.** *Sigui $e_1, \dots, e_n \in \mathbb{R}^n$ una base per $\mathbb{R}^n$ com a espai vectorial sobre $\mathbb{R}$. Aleshores $e_1, \dots, e_n$ també forma una base per un $\mathbb{Z}$-mòdul lliure de rang n*

$$\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n,$$

i diem que Λ és una xarxa a $\mathbb{R}^n$.

Definició 17 (Domini fonamental)**.** *Sigui Λ una xarxa a $\mathbb{R}^n$ definim el domini fonamental d'Λ com el conjunt*

$$F = \{x \in \mathbb{R} : x = \sum_{i=1}^{n} a_i e_i, \quad 0 \le a_i < 1\}.$$

Per entendre-ho podem pensar el cas més familiar on e_1 i e_2 són vectors linealment independents al pla $\mathbb{R}^2$. Llavors F és el paral·lelogram de costats e_1 i e_2.

Observació 5. *En general, cada punt de $\mathbb{R}^n$ és congruent mòdul Λ a un únic punt de F, per tant $\mathbb{R}^n$ és l'unió disjunta de conjunts $\lambda + F$ amb $\lambda \in \Lambda$.*

Definició 18 (Covolum)**.** *Sigui μ la mesura de Lebesgue i Λ una xarxa a $\mathbb{R}^n$, aleshores el volum $\mu(F)$ del domini fonamental F el denotarem per covol(Λ).*

Si com abans e_1 i e_2 són vectors linealment independents al pla, aleshores el covolum de la xarxa de base (e_1, e_2) és l'àrea del paral·lelogram generat per e_1, e_2.

Definició 19 (Valor absolut)**.** *Un valor absolut en un cos K és una aplicació $|| : K \to \mathbb{R}$ tal que per cada $x, y \in K$ es té*

1. $|x| \geq 0$ *amb igualtat si i només si* $x = 0$,
2. $|xy| = |x||y|$,
3. $|x+y| \leq |x| + |y|$ *o 3'.* $|x+y| \leq \max(|x|, |y|)$,

on si es compleix $1, 2, 3$ *i* $3'$ *en diem valor absolut no-arquimedià i si només es compleix* $1, 2, 3$ *en diem valor absolut arquimedià.*
Diem que dos valors absoluts $||_1$ *i* $||_2$ *de* K *són equivalents si i només si per a tot* $x \in K$ *existeixen constants* c_1, c_2 *tals que* $|x|_1 \leq c_2|x|_2$ *i* $|x|_2 \leq c_1|x|_1$.

Definició 20 (Valoració discreta). *Una valoració discreta a* K *és una aplicació exhaustiva* $v : K \to \mathbb{Z} \cup \{\infty\}$, *tal que per a cada* $x, y \in K$,

1. $v(x) = \infty$ *si i només si* $x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x+y) \geq \min(v(x), v(y))$.

La valoració discreta indueix un valor absolut no-arquimedià via $|x|_v = c^{v(x)}$ *amb c constant* $0 < c < 1$.

Definició 21 (Espai mètric complet i completació d'un espai mètric). *Diem que un espai mètric* X *és complet si tota successió de Cauchy convergeix a* X.
Siguin $(x_n), (y_n)$ *successions de Cauchy en* X, *definim la següent relació* $(x_n) \sim (y_n)$ *si* $d(x_n, y_n) \to 0$ *quan* $n \to \infty$. *Aquesta relació és d'equivalència i les classes* $[(x_n)]$ *defineixen un espai mètric* $\hat{X}$ *amb mètrica* $d([(x_n)], [(y_n)]) = \lim_{n\to\infty} d(x_n, y_n)$. *Si* X *és induït per un valor absolut* $||$, *extenem el valor absolut* $||$ *a un valor absolut a* $\hat{X}$ *via* $|[(x_n)]| := \lim_{n\to\infty} |x_n|$ *i en aquest cas* $\hat{X}$ *és un cos. Si* $||_v = c^{v(x)}$, $c \in (0,1)$ *llavors extenem* v *a* $\hat{X}$ *com* $v([x_n]) := \lim_{n\to\infty} v(x_n) \in \mathbb{Z}$. *Aleshores tenim* $|[(x_N)]| := c^{v([x_n])}$.

Per aprofundir en el tema de les valoracions discretes i les completacions veieu les notes [14, capítol 8.1.].

Definició 22. *Sigui* K *un cos amb un valor absolut* $||$. *Aleshores* K *és un espai mètric amb la mètrica* $d(x,y) = |x - y|$ *induïda per* $||$. *Si* S *és el conjunt de les places de* K, *aleshores denotem per* K_v *la completació de* K *respecte* v. *Del valor absolut a* K_v *induït per* $||$ *en diem* $||_{K_v}$.

Observació 6. *Sigui* $K/\mathbb{Q}$ *finita, tots els valors absoluts no-equivalents a* K *provenen de places* $v|\infty$ *(donant valors absoluts arquimedians) i per a cada ideal primer* β *de* $\mathcal{O}_K$, *l'anell d'enters de* K, *es defineix* $|x|_\beta = q^{-i}$ *on* $(x) = \beta^i \beta_1^{i_1} \dots \beta_n^{i_n}$ *és la descomposició en ideals primers de l'ideal generat per* x *en* $\mathcal{O}_K$, *i* $q = \#\mathcal{O}_K/\beta$ *on* $\mathcal{O}_K/\beta \cong \mathbb{F}_q$ *és un cos finit* ($K/\mathbb{Q}$ *finita). Aquest* $||_\beta$ *és no-arquimedià i no equivalent per a 2 ideals primers diferents de* $\mathcal{O}_K$.

Definim l'espai vectorial real $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ i el seu grup d'unitats $K_\mathbb{R}^\times = \prod_{v|\infty} K_v^\times \simeq \prod_{\text{real } v|\infty} \mathbb{R}^\times \times \prod_{\text{complex } v|\infty} \mathbb{C}^\times$.
Definim també el conjunt $\mathbb{R}_0^{r_1+r_2} := \{x \in \mathbb{R}^{r_1+r_2} : x_1 + x_2 + \cdots + x_{r_1+r_2} = 0\}$. Sigui π la projecció $x_{r_1+r_2} \mapsto x_1 + x_2 + \cdots + x_{r_1+r_2-1}$ aleshores tenim l'isomorfisme $\mathbb{R}_0^{r_1+r_2} \overset{\pi}{\cong} \mathbb{R}^{r_1+r_2-1}$.

Proposició 10. *Si pensem* $\mathcal{O}_K$ *com a xarxa a* $K_\mathbb{R} \simeq \mathbb{R}^{r_1+2r_2}$ *tenim*

$$|D_K|^{1/2} = covol(\mathcal{O}_K).$$

Podeu trobar una demostració a [11, prop.14.12].

Definició 23. *Definim el següent morfisme continu de grups*

$$\begin{aligned} Log : K_{\mathbb{R}}^{\times} &\longrightarrow \mathbb{R}^{r_1+r_2} \\ (x_v) &\mapsto (log|x_v|_{K_v}). \end{aligned}$$

Proposició 11. *El conjunt* $\Lambda_K := Log(\mathcal{O}_K^{\times})$ *és una xarxa en* $\mathbb{R}_0^{r_1+r_2}$.

Definició 24 (Regulador)**.** *Sigui* K *un cos de nombres amb* r_1 *places reals i* r_2 *places complexes. Ja hem vist que* Λ_K *és una xarxa a* $\mathbb{R}_0^{r_1+r_2}$ *i que* $\mathbb{R}_0^{r_1+r_2} \overset{\pi}{\cong} \mathbb{R}^{r_1+r_2-1}$*, on* π *és l'aplicació* $x_{r_1+r_2} \mapsto x_1 + x_2 + \cdots + x_{r_1+r_2-1}$ *amb* $x = (x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}_0^{r_1+r_2}$ *. De fet* $\pi : \mathbb{R}^{r_1+r_2} \to \mathbb{R}^{r_1+r_2-1}$ *pot ser una projecció de coordenades qualsevol. Definim el regulador* R_K *com*

$$R_K := covol(\pi(Log(\mathcal{O}_K^{\times}))) \in \mathbb{R}_{>0},$$

on la mesura μ *del covolum és la mesura Euclidiana a* $\mathbb{R}^{r+s-1}$.

Proposició 12. *El valor de* R_K *no depèn de la projecció* π *escollida, veure [12, def 15.14.]. Sigui* $e_1, \ldots, e_{r_1+r_2-1}$ *una base de* $\mathcal{O}_K^{\times}/\mu_K$ *(pel teorema 11 és un* $\mathbb{Z}$*-mòdul lliure), on* μ_K *és el grup de les arrels de la unitat a* K*. Aleshores* R_K *es calcula com el valor absolut del determinant de qualsevol menor* $(r_1+r_2-1)\times(r_1+r_2-1)$ *de la matriu* $(r_1+r_2)\times(r_1+r_2-1)$ *que té per columnes vectors* $Log(e_i) \in \mathbb{R}^{r_1+r_2}$*. veieu [7, def 7.9.] per més detalls.*

Teorema 9 (Fórmula del nombre de classes per a cossos de nombres algebraics)**.** *Sigui* K *un cos de nombres. El residu en* $s = 1$ *per a* $\zeta_K(s)$ *ve donat per*

$$\lim_{s\longrightarrow 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K|D_K|^{\frac{1}{2}}},$$

on h_K *és el nombre de classes,* R_K *el regulador,* w_K *el nombre d'arrels de la unitat a* K*,* r_1 *el nombre de places reals, i* r_2 *de places complexes de* K*.*

També és útil definir la fórmula en termes de productes de funcions L fent servir el teorema 4. Així tenim

$$\begin{aligned} \lim_{s\longrightarrow 1^+}(s-1)\zeta_K(s) &= \lim_{s\longrightarrow 1^+}(s-1)\prod_{\chi\in X} L(s,\chi) \\ &= \lim_{s\longrightarrow 1^+}(s-1)\zeta(s)\prod_{\chi\in X,\chi\neq\chi_0} L(s,\chi) \\ &= \prod_{\chi\in X,\chi\neq\chi_0} L(1,\chi), \end{aligned}$$

ja que la funció zeta de Riemann té un pol simple al $s = 1$ amb residu 1. La fórmula del nombre de classes es pot descriure per

$$\prod_{\chi\in X,\chi\neq\chi_0} L(1,\chi) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K|D_K|^{\frac{1}{2}}},$$

que depèn de les funcions $L(1,\chi)$ que hem vist fórmules per a calcular-les segons si χ és parell o senar.

Proposició 13. *Sigui K un cos quadràtic $K = \mathbb{Q}(\sqrt{m})$ on m és un enter lliure de quadrats, aleshores tenim*

$$\zeta_K(s) = \zeta(s)L(s, \chi_m)$$

on χ_m és el caràcter no trivial associat a K.

Demostració. És un cas especial del teorema 4 amb K un cos quadràtic. En aquest cas el grup X format pels caràcters de Dirichlet amb cos associat K només té dos caràcters: el trivial i un altre que en direm χ_m. Com que $L(s, \chi_0) = \zeta_K(s)$ tenim el resultat. $\square$

De la proposició anterior $\zeta_{\mathbb{Q}}(\sqrt{m})(s) = \zeta(s)L(s, \chi_m)$ i $\lim_{s \longrightarrow 1}(s-1)\zeta(s) = 1$ obtenim

$$\lim_{s \longrightarrow 1^+}(s-1)\zeta_{\mathbb{Q}}(\sqrt{m})(s) = L(1, \chi_m).$$

Sabem que $w_{\mathbb{Q}(\sqrt{m})} = 2$, $r_1 = 2$ i $r_2 = 0$ si $\mathbb{Q}(\sqrt{m})$, $m > 0$ és un cos quadràtic real i $R_{\mathbb{Q}(\sqrt{m})} = 1$, $r_1 = 0$ i $r_2 = 1$ si $\mathbb{Q}(\sqrt{m})$, $m < 0$ és un cos quadràtic imaginari. Aleshores per la fórmula del nombre de classes per a cossos de nombres algebraics, obtenim

$$h_{\mathbb{Q}(\sqrt{m})} = |D_{\mathbb{Q}(\sqrt{m})}|^{\frac{1}{2}} \frac{L(1, \chi_m)}{2R_{\mathbb{Q}(\sqrt{m})}} \qquad (m > 0) \tag{2.1}$$

$$h_{\mathbb{Q}(\sqrt{m})} = \frac{w_{\mathbb{Q}(\sqrt{m})}}{2\pi} |D_{\mathbb{Q}(\sqrt{m})}|^{\frac{1}{2}} L(1, \chi_m) \qquad (m < 0) \tag{2.2}$$

Idees de la demostració del teorema 9

Anem ara a donar alguns detalls per a una demostració de la fórmula del nombre de classes per a cossos de nombres. Seguim la demostració de [13].
Tenim

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \sum_{t \geq 1, t \in \mathbb{Z}} a_t t^{-s}, \quad \text{per a} \quad Re(s) > 1.$$

on $\mathfrak{a}$ recorre els ideals no nuls de $\mathcal{O}_K$ i $a_t := \#\{\mathfrak{a} \subseteq \mathcal{O}_K : N(\mathfrak{a}) = t\}$ amb $t \in [1, \infty) \cap \mathbb{Z}$. Enunciem ara dos resultats que són clau per a la demostració del teorema 9, veieu traces de la demostració del teorema 10 a partir de la pàgina 26.

Teorema 10. *Sigui K un cos de nombres on $n = [K : \mathbb{Q}]$. Quan $t \to \infty$, el nombre d'ideals no nuls $\mathfrak{a}$ de $\mathcal{O}_K$ amb norma acotada $N(\mathfrak{a}) \leq t$ és*

$$\left(\frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |D_K|^{1/2}} \right) t + O(t^{t-1/n})$$

on $h_K, R_K, D_K, w_K, r_1 i\, r_2$ com abans.

Lema 1. *Sigui $b_1, b_2, \ldots$ una successió de nombres complexos que satisfà*

$$b_1 + \cdots + b_t = \rho t + O(t^\sigma)$$

quan $t \longrightarrow \infty$, per algun $\sigma \in [0, 1)$ i $\rho \in \mathbb{C}^\times$.Llavors la sèrie de Dirichlet $\sum_{n=1}^{\infty} b_n n^{-s}$ convergeix per a $Re(s) > 1$ i té una continuació meromorfa a $Re(s) > \sigma$ i té un únic pol simple a $s = 1$ amb residu ρ.

Observació 7. *El lema 1 és un resultat d'anàlisi complexa, podeu veure detall de la demostració en [13, lema 19.11].*

Ja estem a punt per a acabar la demostració de la fórmula del nombre de classes. Pel teorema 10 tenim

$$a_1 + \cdots + a_t = \sum_{j=1}^{t} \#\{\mathfrak{a} : N(\mathfrak{a}) = j\} = \#\{\mathfrak{a} : N(\mathfrak{a}) \leq t\} = \rho_K t + O(t^{1-1/n})$$

quan $t \longrightarrow \infty$. Aplicant el lema amb $\sigma = 1 - 1/n$ observem que $\zeta_K(s) = \sum a_t t^{-s}$ la podem extendre a una funció meromorfa a $Re(s) > 1 - 1/n$ que té un únic pol simple a $s = 1$ amb residu ρ_K.

Idees de la demostració del teorema 10

Volem comptar els ideals no nuls $\mathfrak{a}$ de $\mathcal{O}_k$ tals que $N(\mathfrak{a}) \leq t$.

Teorema 11 (Teorema de les unitats de Dirichlet). *El grup $\mathcal{O}_K^\times$ d'unitats d'un cos de nombres K és un grup abelià finitament generat. Més concretament, si $r = r_1 + r_2 - 1$, aleshores tenim*

$$\mathcal{O}_K^\times \cong \mathbb{Z}^r \times \mu_K,$$

on μ_K és el conjunt de les arrels de la unitat en K i $\mathbb{Z}^r$ és un grup lliure de rang $r_1 + r_2 - 1$ i que,per tant, en podem trobar una base.

Podeu consultar una demostració del teorema 11 en [9, teorema 7.4.].
Definim ara el conjunt

$$S := \nu^{-1}(Log^{-1}(F))$$

on F és un domini fonamental de la xarxa Λ_K i ν és el morfisme exhaustiu

$$\begin{aligned} \nu : K_{\mathbb{R}}^\times &\longrightarrow K_{\mathbb{R},1}^\times \\ x &\mapsto xN(x)^{-1/n} \end{aligned}$$

on $K_{\mathbb{R},1}^\times$ és els elements de $K_{\mathbb{R}}^\times$ de norma 1. Sigui pel teorema 11 $\mathcal{O}_K^\times \cong U \times \mu_K$, U grup lliure de rang $r_1 + r_2 - 1$. Podem pensar S com les classes laterals del quocient $K_{\mathbb{R}}^\times / U$.

Finalment definim el conjunt

$$S_{\leq t} := \{x \in S : N(x) \leq t\}.$$

Ara necessitem una proposició que discutirem més tard.

Proposició 14. *Es compleix*

$$\#(S_{\leq t} \cap \mathcal{O}_K) = \left(\frac{2^{r_1}(2\pi)^{r_2} R_K}{|D_K|^{1/2}} \right) t + O(t^{1-1/n}).$$

Ja podem començar a comptar els ideals no nuls $\mathfrak{a}$ de $\mathcal{O}_k$ tals que $N(\mathfrak{a}) \leq t$. Considerem primer la classe trivial de $Cl(K)$ composta pels ideals principals de $\mathcal{O}_K$. Hi ha un ideal principal per cada $\alpha \in \mathcal{O}_K / \mathcal{O}_K^\times$ amb $N(\alpha) \leq t$. Prenem l'aplicació

$$S_{\leq t} \cap \mathcal{O}_K \longrightarrow (K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/\mathcal{O}_K^\times$$

que envia w_K elements del conjunt de l'esquerra a un element de la dreta. Per tant per calcular la cardinalitat del conjunt de la dreta calcularem la cardinalitat del de l'esquerra i dividirem per w_K. Amb la proposició 14 queda

$$\#\{(\alpha) \subseteq \mathcal{O}_K | N(\alpha) \leq t\} = \left(\frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K |D_K|^{1/2}} \right) t + O(t^{1-1/n}) \tag{2.3}$$

Ara volem calcular la cardinalitat del conjunt anterior per a la resta de classes de $Cl(K)$. Veurem que obtenim la mateixa expressió d'abans per a cada classe.
Fixem una classe d'ideals $[\mathfrak{a}]$ amb $\mathfrak{a} \subseteq \mathcal{O}_K$ no nul i $N(\mathfrak{a} \leq t)$. Com que $Cl(K)$ té estructura de grup podem agafar l'element simètric $[\mathfrak{a}^{-1}]$ i aleshores si prenem $\mathfrak{b} \in [\mathfrak{a}^{-1}]$ el producte $\mathfrak{ba}$ és un ideal principal de $\mathcal{O}_K$. Llavors l'aplicació multiplicació per $\mathfrak{a}$ ens dóna una bijecció

$$\begin{aligned} \{\mathfrak{b} \in [\mathfrak{a}^{-1}] : N(\mathfrak{b} \leq t)\} &\xrightarrow{\times \mathfrak{a}} \{(\alpha) \subseteq \mathfrak{a} : N(\alpha) \leq tN(\alpha)\} \\ &\longrightarrow \{\alpha \in \mathfrak{a} : N(\alpha) \leq tN(\mathfrak{a})\}/\mathcal{O}_K^\times \end{aligned}$$

on hem fet servir $N(\alpha) = N(\mathfrak{ba}) = N(\mathfrak{b})N(\mathfrak{a}) \leq tN(\mathfrak{a})$.
Definim $S_{[\mathfrak{a}],\leq t} := \{\alpha \in \mathfrak{a} : N(\alpha) \leq tN(\mathfrak{a})\}/\mathcal{O}_K^\times$. Quan fem la demostració de la proposició 14 a les properes pàgines veurem que de fet es pot aplicar a qualsevol xarxa a $K_\mathbb{R}$ i no només a $\mathcal{O}_K$. Observem que l'ideal fraccionari $\mathfrak{a} \subseteq \mathcal{O}_K$ és un $\mathcal{O}_\mathbb{K}$-submòdul ja que per definició $c\mathfrak{a}$ és un ideal de $\mathcal{O}_K$, per algun $c \in \mathcal{O}_K$. Aleshores com que $\mathcal{O}_K$ és una xarxa a $K_\mathbb{R}$, en particular $\mathfrak{a}$ també és una xarxa a $K_\mathbb{R}$. Llavors podem canviar $\mathcal{O}_K$ per $\mathfrak{a}$ a l'equació (2.3). Substituim també t per $tN(\mathfrak{a})$ a l'equació (2.3) i obtenim

$$\begin{aligned} \#S_{[\mathfrak{a}],\leq t} &= \left(\frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K covol(\mathfrak{a})} \right) tN(\mathfrak{a}) + O(t^{1-1/n}) \\ &= \left(\frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K covol(\mathcal{O}_K)N(\mathfrak{a})} \right) tN(\mathfrak{a}) + O(t^{1-1/n}) \\ &= \left(\frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K |D_K|^{1/2}} \right) t + O(t^{1-1/n}) \end{aligned}$$

on hem fet servir la proposició 10 i el fet que $covol(\mathfrak{a}) = N(\mathfrak{a})covol(\mathcal{O}_K)$ com a xarxes a $K_\mathbb{R}$. Veieu [11, Corol·lari 14.13]. La clau per veure com surt el nombre de classes h_K a la fórmula és notar que la dreta de l'equació anterior no depèn de la classe d'ideals $[\mathfrak{a}]$. Aleshores si sumem totes les classes d'ideals obtenim

$$\begin{aligned} \#\{\mathfrak{b} \subseteq \mathcal{O}_K : N(\mathfrak{b}) \leq t\} &= \sum_{[\mathfrak{a}] \in Cl(K)} \#S_{[\mathfrak{a}],\leq t} \\ &= h\#S_{[\mathfrak{a}],\leq t} \\ &= \left(\frac{2^{r_1}(2\pi)^{r_2} h R_K}{w_K |D_K|^{1/2}} \right) t + O(t^{1-1/n}). \end{aligned}$$

Idees de la demostració de la proposició 14

Hem d'establir una condició que limiti el creixament de S quan t creix a l'infinit.

Definició 25 (Lipschitz parametritzable)**.** *Sigui B un conjunt en un espai mètric X. Una funció f és Lipschitz contínua si existeix $c > 0$ tal que per tot $x_1 \neq x_2 \in X$ es té $d(f(x_1), f(x_2)) \leq cd(x_1, x_2)$. Diem que B és Lipschitz parametritzable si és la unió de les imatges d'un nombre finit de funcions Lipschitz contínues $f_i : [0,1]^d \longrightarrow B$.*

Farem la demostració de la proposició 14 mitjançant alguns lemes.

Lema 2. *Sigui* $A \subseteq \mathbb{R}^n$ *amb frontera* $(n-1)$*-Lipschitz parametritzable. Llavors*

$$\#(tA \cap \mathbb{Z}^n) = \mu(A)t^n + O(t^{n-1})$$

quan $t \longrightarrow \infty$ *i* μ *és la mesura de Lebesgue a* $\mathbb{R}^n$*.*

Demostració. El primer pas és partir $\mathbb{R}^n$ en cubs mig oberts

$$c(a_1, \ldots, a_n) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \in [a_i, a_i + 1)\}$$

amb $a_1, \ldots, a_n \in \mathbb{Z}$.
Sigui C el conjunt de tots els cubs c. Per cada t definim

$$B_0(t) := \#\{c \in C : c \subseteq tA\}$$
$$B_1(t) := \#\{c \in C : c \cap tA \neq \emptyset\}$$

que són respectivament els cubs totalment dins de tA i els cubs total o parcialment dins de tA.
Com que cada cub conté un sol enter de $\mathbb{Z}^n$ tenim $B_0(t) \leq \#(tA \cap \mathbb{Z}^n) \leq B_1(t)$.
Notem que cada $c(a_1, \ldots, a_n) \in B_1(t) - B_2(t)$ conté un punt dins d'una esfera de radi $\sqrt{n}$ i centre un punt de ∂tA.
Ara fem servir la condició de que A és $(n-1)$-Lipschitz parametritzable. Siguin $f_1, \ldots, f_m$ funcions Lipschitz $[0,1]^{n-1} \longrightarrow \partial A$ tals que les seves imatges cobreixen ∂A i siguin $c_1, \ldots, c_n$ constants tals que $d(f_i(x_1), f_i(x_2)) \leq c_i d(x_1, x_2)$ per tot $x_1, x_2 \in [0,1]^{n-1}$. Per qualsevol $y \in \partial A$ podem triar $f_i(x_1, \ldots, x_{n-1}) = y$. Sigui $r_j = \lfloor tx_j \rfloor$ la part entera de tx_j, llavors $0 \leq tx_j - r_j < 1 \implies 0 \leq x_j - r_j/t < 1/t$. Aleshores

$$d(y, f_i(\frac{r_1}{t}, \ldots, \frac{r_{n-1}}{t})) \leq c_i d((x_1, \ldots, x_{n-1}), (\frac{r_1}{t}, \ldots, \frac{r_{n-1}}{t})) \leq c_i \sqrt{n}/t \leq c/t$$

on $c := \sqrt{n} \cdot \max_i(c_i)$. Per tant $y \in \partial A$ està a distància menor que c/t que un punt del conjunt

$$P = \{f_i(\frac{r_1}{t} \ldots \frac{r_{n-1}}{t}) : 1 \leq i \leq m, 0 \leq r_1, \ldots, r_{n-1} \leq t\}$$

que té cardinalitat $m(t+1)^{n-1} = O(t^{n-1})$. Per tant cada punt la distància entre cada punt de ∂tA i tP és menor que c i el nombre de punts de la xarxa entera a distància menor que $\sqrt{n}$ de un punt de $t\partial A$ és $O(t^{n-1})$. Així doncs podem acotar $B_1(t) - B_0(t) = O(t^{n-1})$.
Com que $B_0(t) \leq \mu(tA) \leq B_1(t)$ i $\mu(tA) = t^n \mu(A)$ tenim

$$\#(tA \cap \mathbb{Z}^n) \leq B_1(t) - B_0(t) + B_0(t) \leq O(t^{n-1}) + t^n \mu(A)$$
$$\#(tA \cap \mathbb{Z}^n) \geq B_0(t) - B_1(t) + B_1(t) \geq O(t^{n-1}) + t^n \mu(A)$$

i per tant quan $t \longrightarrow \infty$ tindrem la igualtat del lema.

□

Anem a veure un corol·lari del lema

Corol·lari 2. *Sigui* Λ *una xarxa en un espai vectorial real* V *i sigui* $A \subseteq V$ *un conjunt amb frontera* $(n-1)$*-Lipschitz parametritzable. Si* μ *és la mesura de Lebesgue, aleshores*

$$\#(tA \cap \Lambda) = \frac{\mu(A)}{covol(\Lambda)} t^n + O(t^{n-1}).$$

Demostració. Si $\Lambda \subseteq \mathbb{Z}^n$ aleshores es compleix pel lema. Notem que si el corol·lari és cert per a $s\Lambda$, $s>0$, aleshores també és cert per a Λ ja que $tA \cap s\Lambda = (t/s)A \cap \Lambda$. Sigui $(v_1,\ldots,v_m)$ una base de la xarxa Λ on cada v_i és un vector de components reals. Aquests vectors reals els podem aproximar per vectors de nombres racionals i prenent $s = mcm(\text{denominadors de } v_i)$ obtenim una base d'una xarxa a $\mathbb{Z}^n$. $\square$

Amb aquest corol·lari si demostrem que $\mu(S_{\leq 1}) = 2^{r_1}(2\pi)^{r_2}R_K$ i que la frontera de S és $(n-1)$-Lipschitz parametritzable, haurem acabat. En efecte si agafem $\Lambda = \mathcal{O}_K$, $A = S_{\leq 1}$ i $t = t^{1/n}$ tenim

$$\#(t^{1/n}S_{\leq 1} \cap \mathcal{O}_K) = \left(\frac{\mu(S_{\leq 1})}{covol(\mathcal{O}_K)}\right) t + O(t^{n-1/n})$$

i com que $S_{\leq t} = t^{1/n}S_{\leq 1}$ i $|D_K|^{1/2} = covol(\mathcal{O}_K)$

$$\#(S_{\leq t} \cap \mathcal{O}_K) = \left(\frac{\mu(S_{\leq 1})}{|D_K|^{1/2}}\right) t + O(t^{1-1/n})$$

on $\mu(S_{\leq 1}) = 2^{r_1}(2\pi)^{r_2}R_K$.

La demostració del fet que $\mu(S_{\leq 1}) = 2^{r_1}(2\pi)^{r_2}R_K$ es pot trobar a les notes [13, pàgina 6]. La demostració del fet que $S_{\leq 1}$ és $(n-1)$-Lipschitz parametritzable es pot trobar a [13, meitat inferior pàgina 5].

3 Càlcul de h_K per a $[K:\mathbb{Q}]=2$

Anem a calcular el nombre de classes per a cossos quadràtics amb algun exemple concret.

Tot cos quadràtic sobre $\mathbb{Q}$ és de la fórma $K = \mathbb{Q}(\sqrt{m})$ on m és un enter lliure de quadrats.

L'anell $\mathcal{O}_K = \{\alpha \in K : Irr(\alpha, \mathbb{Q}[x]) \in \mathbb{Z}[x]\}$ es demostra que és

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \text{ si } m \equiv 1 (\text{mod } 4) \\ \mathbb{Z}[\sqrt{m}] \text{ si } m \not\equiv 1 (\text{mod } 4), \end{cases}$$

veure [4, Proposició 13.1.1]. Provem ara la següent proposició

Proposició 15. *La norma d'un element α de $\mathbb{Z}[\sqrt{m}]$ on m és un enter lliure de quadrats és $N(\alpha) = \alpha\bar{\alpha} \in \mathbb{Z}$. Un element $\mathcal{O}_K$ compleix $\alpha \in \mathcal{O}_K^\times \iff N(\alpha) = \pm 1$, i això val per a tots els cossos de nombres algebraics.*

Demostració. Estudiem primer la norma per un element α de l'extensió $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$. Com que $\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{Q}(\sqrt{m})$ la norma serà la mateixa.
Ja hem vist que els automorfismes del grup de galois en aquest cas són la identitat i el que envia $\sqrt{m}$ a $-\sqrt{m}$. Aleshores per $a, b \in \mathbb{Q}$, $\alpha = a + b\sqrt{m}$ és un element qualsevol de $\mathbb{Q}(\sqrt{m})$ i

$$N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = \alpha\bar{\alpha}.$$

Vegem la segona part de la proposició. Si suposem que $\alpha \in \mathcal{O}_K$ aleshores $\alpha\alpha^{-1} = 1$ i $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = 1$. Com que les normes són nombres enters, obtenim $N(\alpha) = \pm 1$. $\square$

Si $m \equiv 2, 3 (\text{mod } 4)$ aleshores els elements de $\mathcal{O}_K$ són de la forma $\alpha = a + b\sqrt{m}$ per alguns $a, b \in \mathbb{Z}$. Si $m \equiv 1 (\text{mod } 4)$ aleshores els elements de $\mathcal{O}_K$ són de la forma $\alpha = (a + b\sqrt{m})/2$ per alguns $a, b \in \mathbb{Z}$.

Amb la proposició 15 escrivim $\alpha\bar{\alpha} = N(\alpha) = \pm 1$ i obtenim l'anomenada equació de Pell

$$a^2 - mb^2 = \pm\sigma, \qquad \sigma = \begin{cases} 4 \text{ si } m \equiv 1 (\text{ mod } 4) \\ 1 \text{ si } m \equiv 2, 3 (\text{ mod } 4). \end{cases} \tag{3.1}$$

Aquesta equació és una equació diofàntica que està molt estudiada, veure, per exemple, [5].

Calculem ara el discriminant D_K. Si $m \equiv 1 (\text{ mod } 4)$ sabem que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Aleshores $(1, \frac{1+\sqrt{m}}{2})$ és una base de $\mathcal{O}_K$ com a $\mathbb{Z}$ mòdul. El grup de Galois de $K/\mathbb{Q}$ ja sabem que té dos automorfismes σ_0, σ_1 que envien $\sqrt{m}$ a $\sqrt{m}$ i $-\sqrt{m}$, respectivament. Aleshores les traces són

$$Tr(1 \cdot 1) = \sigma_0(1) + \sigma_1(1) = 2$$

$$\begin{aligned} Tr\left(1 \cdot \frac{1+\sqrt{m}}{2}\right) = Tr\left(\frac{1+\sqrt{m}}{2} \cdot 1\right) &= \sigma_0\left(\frac{1+\sqrt{m}}{2}\right) + \sigma_1\left(\frac{1+\sqrt{m}}{2}\right) \\ &= \frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} = 1 \end{aligned}$$

$$\begin{aligned} Tr\left(\frac{1+\sqrt{m}}{2}\frac{1+\sqrt{m}}{2}\right) &= \sigma_0\left(\frac{1+2\sqrt{m}+m}{4}\right) + \sigma_1\left(\frac{1+2\sqrt{m}+m}{4}\right) \\ &= \frac{1+2\sqrt{m}+m}{4} + \frac{1-2\sqrt{m}+m}{4} = \frac{1+m}{2}. \end{aligned}$$

i el discriminant és

$$D_K = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+m}{2} \end{vmatrix} = 2\frac{1+m}{2} - 1 \cdot 1 = m.$$

Si ara $m \equiv 2, 3 (\text{ mod } 4)$ i $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. Aleshores $(1, \sqrt{m})$ és una base de $\mathcal{O}_K$ com a $\mathbb{Z}$ mòdul. Les traces són

$$\begin{aligned} &Tr\,(1 \cdot 1) = \sigma_0(1) + \sigma_1(1) = 2 \\ &Tr(1 \cdot \sqrt{m}) = Tr(\sqrt{m} \cdot 1) = \sigma_0(\sqrt{m}) + \sigma_1(\sqrt{m}) = \sqrt{m} - \sqrt{m} = 0 \\ &Tr(\sqrt{m} \cdot \sqrt{m}) = \sigma_0(m) + \sigma_1(m) = 2m, \end{aligned}$$

i en aquest cas el discriminant queda

$$D_K = \begin{vmatrix} 2 & 0 \\ 0 & 2m \end{vmatrix} = 4m.$$

En resum:

$$D_K = \begin{cases} m \text{ si } m \equiv 1(\mod 4) \\ 4m \text{ si } m \equiv 2,3(\mod 4). \end{cases} \tag{3.2}$$

Estudiem ara el grup de caràcters de Dirichlet associat a K.

Si $m<0$, per la fórmula del conductor-discriminant 8, com que $r_2 = 1$ i al grup X format per caràcters de Dirichlet només hi ha el caràter trivial i un altre caràcter amb conductor f, obtenim

$$D_K = -f.$$

Pel cas $m>0$, aquí $r_2=0$ i per la fórmula del conductor-discriminant tenim

$$D_K = f.$$

Com que acabem de calcular el discriminant, ja tenim també una expressió pel conductor

$$f = \begin{cases} |m| \text{ si } m \equiv 1(\mod 4) \\ |4m| \text{ si } m \equiv 2,3(\mod 4). \end{cases} \tag{3.3}$$

per a qualsevol cos quadràtic.

Càlcul del nombre de classes en cossos quadràtics imaginaris sobre $\mathbb{Q}$

Volem calcular el nombre de classes h_K per a $K=\mathbb{Q}(\sqrt{m})$ amb $m<0$ i m lliure de quadrats. Per fer-ho farem servir la fórmula del nombre de classes 2.1

$$h_K = \frac{w_K |D_K|^{1/2}}{2\pi} L(1,\chi).$$

Comencem estudiant el nombre d'arrels de la unitat dins de K. Pel teorema 11 tenim

$$\mathcal{O}_K^\times = \mu(K)\times\mathbb{Z}^{1+0-1} = \mu(K).$$

Per tant podem calcular el nombre d'elements de $\mathcal{O}_K^\times$.

Ja hem vist que els elements de $\mathcal{O}_K^\times$ compleixen l'equació 3.1. Si $m\equiv 2,3(\text{mod } 4)$ i $m<0$, obtenim $a^2+b^2|m| = \pm 1$ i si $m\neq -1$ l'única opció és $a=\pm 1$ i $b=0$. Si $m=-1$ aleshores $a^2+b^2=\pm 1$ i les úniques solucions enteres són $a=\pm 1$ i $b=0$ o $a=0$ i $b=\pm 1$. Si $m\equiv 1(\text{mod } 4)$ aleshores els elements de $\mathcal{O}_K^\times$ compleixen

$$a^2+b^2|m| = \pm 4,$$

i per tant per $m=-3$ tenim les possibilitats $a=\pm 2$ i $b=0$ ó $a=\pm 1$ i $b=\pm 1$. Si $m>3$ les úniques opcions són $a=\pm 2$ i $b=0$.

En resum: si K és un cos quadràtic imaginari el nombre d'arrels de la unitat w_K a K és

$$w_K = \begin{cases} 4 \text{ si } m=-1, \\ 6 \text{ si } m=-3, \\ 2 \text{ si } m\neq -1,-3. \end{cases}$$

El discriminant D_K el dóna (3.2).

Només queda calcular el valor de $L(1,\chi)$ que es pot trobar segons si el caràcter χ és parell o senar utilitzant les dues fórmules 1.10 i 1.8. El caràcter no trivial χ s'ha de calcular i té conductor donat per (3.3).

Exemple 2. *Volem calcular el nombre de classes h_K del cos $K = \mathbb{Q}(\sqrt{-5})$ fent servir la fórmula del nombre de classes. Hem demostrat que el nombre d'arrels de la unitat en cossos quadràtics imaginaris és $w_K = 2$ sempre que $m \neq -1, -3$. També hem vist que el determinant és $D_K = -20$ ja que $-5 \equiv 3(mod\ 4)$. El conductor del caràcter de Dirichlet associat a K és $f = 20$ per la fórmula del conductor-discriminant. Calculem el caràcter de Dirichlet.*
Vegem una manera de trobar la restricció dels automorfismes de $Gal(\mathbb{Q}(\zeta_{20})/\mathbb{Q})$ a K. Volem escriure $\sqrt{5}$ en termes de ζ_{20}. Tenim que

$$2^{-1}(\sqrt{5}-1) = \zeta_5 + \zeta_5^{-1} = \zeta_{20}^4 + \zeta_{20}^{-4} \Rightarrow \sqrt{-5} = i(\zeta_{20}^4 + \zeta_{20}^{-4})2 + i = \zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5.$$

Aleshores χ es calcula de manera detallada com:

$$\begin{aligned}
1\ mod\ 20 &\leftrightarrow \sigma_0(\zeta_{20}) = \zeta_{20}^1 \to \sigma_0|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^1 = +\sqrt{-5} \leftrightarrow +1\\
3\ mod\ 20 &\leftrightarrow \sigma_1(\zeta_{20}) = \zeta_{20}^3 \to \sigma_1|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^3 = +\sqrt{-5} \leftrightarrow +1\\
7\ mod\ 20 &\leftrightarrow \sigma_2(\zeta_{20}) = \zeta_{20}^7 \to \sigma_2|_K((\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^7 = +\sqrt{-5} \leftrightarrow +1\\
9\ mod\ 20 &\leftrightarrow \sigma_3(\zeta_{20}) = \zeta_{20}^9 \to \sigma_3|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^9 = +\sqrt{-5} \leftrightarrow +1\\
11\ mod\ 20 &\leftrightarrow \sigma_4(\zeta_{20}) = \zeta_{20}^{11} \to \sigma_4|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^{11} = -\sqrt{-5} \leftrightarrow -1\\
13\ mod\ 20 &\leftrightarrow \sigma_5(\zeta_{20}) = \zeta_{20}^{13} \to \sigma_5|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^{13} = -\sqrt{-5} \leftrightarrow -1\\
17\ mod\ 20 &\leftrightarrow \sigma_6(\zeta_{20}) = \zeta_{20}^{17} \to \sigma_6|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^{17} = -\sqrt{-5} \leftrightarrow -1\\
19\ mod\ 20 &\leftrightarrow \sigma_7(\zeta_{20}) = \zeta_{20}^{19} \to \sigma_7|_K(\sqrt{-5}) = (\zeta_{20}^5(\zeta_{20}^4 + \zeta_{20}^{-4})2 + \zeta_{20}^5)^{19} = -\sqrt{-5} \leftrightarrow -1.
\end{aligned}$$

Ara podem calcular la suma de Gauss

$$G(\chi, \zeta_{20}) = \sum_{a=1}^{20} \chi(a)\zeta_f^a = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9 - \zeta_{20}^{11} - \zeta_{20}^{13} - \zeta_{20}^{17} - \zeta_{20}^{19} = 2\sqrt{-5},$$

i la funció L amb l'expressió que hem trobat abans amb $s = 1$ i χ senar

$$\begin{aligned}
L(1,\chi) &= \pi i \frac{G(\chi,\zeta_f)}{f}\frac{1}{f}\sum_{a=1}^{f}\chi(a)a\\
&= \pi i \frac{2\sqrt{-5}}{20}\frac{1}{20}\sum_{a\in(\mathbb{Z}/20\mathbb{Z})^\times}\chi(a)a\\
&= \frac{-\pi\sqrt{5}}{200}(1+3+7+9-11-13-17-19)\\
&= \frac{\pi}{\sqrt{5}}.
\end{aligned}$$

Finalment el nombre de classes de K és

$$h_K = \frac{w_K|D_K|^{1/2}}{2\pi}L(1,\chi) = \frac{2\sqrt{20}}{2\pi}\frac{\pi}{\sqrt{5}} = 2.$$

Càlcul del nombre de classes en cossos quadràtics reals sobre $\mathbb{Q}$

Sigui $K=\mathbb{Q}(\sqrt{m})$ on $m>0$, la fórmula del nombre de classes 2.2 és

$$h_K=\frac{|D_K|^{1/2}}{2R_K}L(1,\chi).$$

Ja hem vist quant val el discriminant D_K a (3.2) i com calcular $L(1,\chi)$ amb les fórmules (1.10), (1.8) i (3.3). Vegem com calcular el regulador. Definim el concepte d'unitat fonamental

Definició 26. *Una unitat fonamental ϵ és una unitat d'ordre infinit tal que cada unitat és de la forma $\zeta\epsilon^n$, on ζ és una arrel de la unitat i $n\in\mathbb{Z}$.*

En tots els cossos quadràtics existeix una unitat fonamental. La demostració d'aquest fet es pot trobar en [4, prop.17.5.2]. Pel teorema de les unitats de Dirichlet si $K=\mathbb{Q}(\sqrt{m})$ i $m>0$, tenim

$$\mathcal{O}_K^\times=\{\pm1\}\times\epsilon^{\mathbb{Z}},$$

ja que les úniques arrels de la unitat reals són ±1.

L'irreductible de $\mathbb{Q}(\sqrt{m})$ als racionals és x^2-m, per tant el conjunt de places només conté els elements σ_0 i σ_1 tals que $\sigma_0(\sqrt{m})=\sqrt{m}$ i $\sigma_1(\sqrt{m})=-\sqrt{m}$.

Si el grup d'unitats de K és subconjunt de $\mathbb{Z}[\sqrt{m}]$ aleshores seus elements tenen forma $a+b\sqrt{m}$ per alguns $a,b\in\mathbb{Z}$. La definició de R_K requereix que la suma dels logarítmes dels elements de $\mathbb{Z}[\sqrt{m}]$ per la imatge de cada plaça sigui 0. Per a qualsevol element $a+b\sqrt{m}$ de $\mathcal{O}_K^\times$ aquesta suma és

$$\begin{aligned}log(\sigma_0(a+b\sqrt{m}))+log(\sigma_1(a+b\sqrt{m}))&=log(a+b\sqrt{m})+log(a-b\sqrt{m})\\&=log((a+b\sqrt{m})(a-b\sqrt{m}))\\&=log(N(a+b\sqrt{m}))=log(1)=0,\end{aligned}$$

per certs $a,b,n\in\mathbb{Z}$ i per ser $a+b\sqrt{m}$ element de $\mathcal{O}_K^\times$.

Aleshores el regulador és per definició el determinant del valor absolut de la matriu que s'obté de treure una plaça al conjunt S de le places infinites de K. Ara notem que $log(\sigma_1(\epsilon))=log(\bar{\epsilon})=log(\epsilon^{-1})=-log(\epsilon)$, i per tant $|log(\sigma_0(\epsilon))|=|log(\sigma_1(\epsilon))|$. Per tant la tria de la plaça que treiem no efecta al resultat. Finalment ens queda el determinant de la matriu de dimensió 1 $(log(\epsilon))$ que és $R=log(\epsilon)$.
Ara el problema és trobar unitats fonamentals ϵ. Aquest problema es redueix en trobar la solució més petita de l'equació de Pell que obenim posant $\alpha=a+b\sqrt{m}$ i $N(\alpha)=1$,

$$a^2-mb^2=\pm\sigma,\qquad \sigma=\begin{cases}1 \text{ si } m\equiv 1(\mod 4)\\ 4 \text{ si } m\equiv 2,3(\mod 4)\end{cases}$$

La manera estàndard de resoldre l'equació amb una solució fonamental és utilitzant fraccions continuades. Farem servir un algorisme que podem trobar a [5, capítol 3.3] tot i que en aquesta referència hi ha un error en la definició de q_{i+1} on en el denominador hi ha d'haver Q_{i+1} i no pas Q_i.

Algorisme 1 (Solució fonamental de l'equació de Pell)**.** *Sigui $m>0$, definim*

$$s=\begin{cases}2 \;si\; m\equiv 0,1(\;mod\;4)\\ 1 \;altrament,\end{cases}\qquad q=\begin{cases}0\;si\; m\not\equiv 1(\;mod\;4)\\ 1\;si\; m\equiv 1(\;mod\;4)\end{cases}$$

$$\delta = \frac{q+\sqrt{m}}{s}$$

Siguin $P_0 = q, Q_0 = s, q_0 = \lfloor(\sqrt{m}+q)/s\rfloor, B_{-1} = 0, B_0 = 1, G_{-1} = s, G_0 = sq_0 - q$, *iterem les següents equacions*

$$\begin{aligned} P_{i+1} &= q_i Q_i - P_i \\ Q_{i+1} &= \frac{m - P_{i+1}^2}{Q_i} \\ q_{i+1} &= \lfloor \frac{P_{i+1} + \lfloor\sqrt{m}\rfloor}{Q_{i+1}} \rfloor \\ G_{i+1} &= q_{i+1} G_i + G_{i-1} \\ B_{i+1} &= q_{i+1} B_i + B_{i-1}, \end{aligned}$$

amb $i = 0, 1, 2, \ldots, p-1$ *on* p *és la mínima* $i+1$ *tal que* $Q_p = s$. *Llavors*

$$\epsilon = \frac{G_{p-1} + \sqrt{m} B_{p-1}}{s}.$$

Exemple 3. *Calculem el nombre de classes de* $K = \mathbb{Q}(\sqrt{2})$. *Com que* $2 \equiv 2(4)$ *el conductor del caràcter de Dricichlet associat a* K *és* 8 *i el discriminant* D_K *també. Els morfismes del grup de Galois envien* ζ_8 *a* ζ_8^a *on* a *pren tots els valors de* $(\mathbb{Z}/8\mathbb{Z})^\times$. *Notem que* $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ *i per tant podem escriure la restricció dels automorfismes a* K *i obtenim el caràcter de Dirichlet*

$$\begin{aligned} 1 \ mod \ 8 \leftrightarrow \sigma_0(\zeta_8) = \zeta_8^1 \to \sigma_0|_{\mathbb{Q}(\sqrt{2})}(\zeta_8 + \zeta_8^{-1}) = (\zeta_8 + \zeta_8^{-1})^1 = +\sqrt{2} \leftrightarrow +1 \\ 3 \ mod \ 8 \leftrightarrow \sigma_1(\zeta_8) = \zeta_8^3 \to \sigma_1|_{\mathbb{Q}(\sqrt{2})}(\zeta_8 + \zeta_8^{-1}) = (\zeta_8 + \zeta_8^{-1})^3 = -\sqrt{2} \leftrightarrow -1 \\ 5 \ mod \ 8 \leftrightarrow \sigma_2(\zeta_8) = \zeta_8^5 \to \sigma_2|_{\mathbb{Q}(\sqrt{2})}(\zeta_8 + \zeta_8^{-1}) = (\zeta_8 + \zeta_8^{-1})^5 = -\sqrt{2} \leftrightarrow -1 \\ 7 \ mod \ 8 \leftrightarrow \sigma_3(\zeta_8) = \zeta_8^7 \to \sigma_3|_{\mathbb{Q}(\sqrt{2})}(\zeta_8 + \zeta_8^{-1}) = (\zeta_8 + \zeta_8^{-1})^7 = +\sqrt{2} \leftrightarrow +1 \end{aligned}$$

Ara podem calcular la suma de Gauss $G(\chi, \zeta_f)$. *Recordem que* $\chi(a) = 0$ *si* $(a, f) \neq 1$.

$$G(\chi, \zeta_8) = \sum_{a=1}^{f} \chi(a)\zeta_8^a = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 = 2\sqrt{2}.$$

Utilitzant l'expressió de $L(1, \chi)$ *quan* χ *és senar*

$$\begin{aligned} L(1,\chi) &= \frac{-G(\chi,\zeta_8)}{8} \sum_{a=1}^{8} \bar{\chi}(a) log|1 - \zeta_8^a| \\ &= \frac{-\sqrt{2}}{4}(log|1-\zeta_8| - log|1-\zeta_8^3| - log|1-\zeta_8^5| + log|1-\zeta_8^7|) \\ &= \frac{-\sqrt{2}}{4} log\left(\frac{2-\sqrt{2}}{2+\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}} log(1+\sqrt{2}). \end{aligned}$$

Només ens queda calcular el regulador R. Hem demostrat que per a cossos quadràtics reals el regulador és $R = log(\epsilon)$ on ϵ és una unitat fonamental de $\mathcal{O}_K$. Per a calcular-la farem servir l'algorisme 1, tenim

$$s = 1, q = 0, \delta = \sqrt{2}$$

n	P_n	Q_n	q_n	G_n	B_n
-1				1	0
0	0	1	1	1	1
1	1	1	2	3	0

Taula 1: Càlcul de ϵ quan $m = 2$.

parem l'algorisme a $i = 0$ on $Q_1 = 1 = s$ i aleshores

$$\epsilon = \frac{G_0 + \sqrt{2}B_0}{s} = 1 + \sqrt{2},$$

i el regulador és $R = log(1+\sqrt{2})$. Finalment el nombre de classes del cos $K = \mathbb{Q}(\sqrt{2})$ és

$$h_K = \frac{\sqrt{D_K}}{2R}L(1,\chi) = \frac{\sqrt{8}}{2log(1+\sqrt{2})}\frac{1}{\sqrt{2}}log(1+\sqrt{2}) = 1.$$

Exemple 4. *Fem un altre exemple amb $m = 115$. Notem que en aquest cas tenim $f = 460$ i els càlculs poden ser llarguíssims. Com que tot el que hem fet per a cosssos quadràtics, tret del càlcul del caràcter de Dirichlet, es pot programar, farem aquest exemple amb SageMath. Dins del SageMath hi ha funcions programades que et retornen directament el nombre de classes:* `K.class_number()` *on* `K=QuadraticField(115)`*, però nosaltres ho calcularem amb el que hem explicat fins ara. L'única funció predeterminada de SageMath que farem servir serà la de* `DirichletCharacter()` *ja que no tenim cap algorisme que ens permeti trobar $\sqrt{m}$ en funció de ζ_f per a fer la restricció*

$$Galois(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \twoheadrightarrow Galois(\mathbb{Q}(\sqrt{m})/\mathbb{Q}),$$

(veure observació 8). A l'apèndix A hi ha el codi fet servir en aquest exemple. La unitat fonamental trobada és

$$\frac{105\sqrt{115}}{1126}.$$

I el nombre de classes és $h_K = 2$.

Observació 8. *Existeix un algorisme per a calcular el caràcter de Dirichlet per a cossos quadràtics imaginaris sobre $\mathbb{Q}$ que es pot trobar a [6, pàgina 124]. Vegem-lo. Sigui $K = \mathbb{Q}(\sqrt{m})$ amb $m < 0$ i lliure de quadrats. Sigui f com a 3.3 aleshores el caràcter χ es pot expressar com*

$$\chi(a \ mod \ f) = \left(\prod_{l|m, l \ primer, l \neq 2} \left(\frac{a}{l}\right) \right) \cdot \theta(a), \tag{3.4}$$

on $\theta(a)$ es definiex com

n	P_n	Q_n	q_n	G_n	B_n
-1				1	0
0	0	1	1	1	1
1	1	1	2	3	0
2	5	6	2	32	3
3	7	11	1	43	4
4	4	9	1	75	7
5	5	10	1	118	11
6	5	9	1	193	18
7	4	11	1	311	29
8	7	6	2	815	76
9	5	15	1	1126	105
10	10	1	20	23335	2176

Taula 2: Càlcul de ϵ quan $m = 115$.

1. *Si* $m \equiv 1$ *mod* 4, *aleshores* $\theta(a) = 1$.
2. *Si* $m \equiv 3$ *mod* 4 *i* $a \equiv 1$ *mod* 4, *aleshores* $\theta(a) = 1$. *Si* $m \equiv 3$ *mod* 4 *i* $a \equiv 3$ *mod* 4, *llavors* $\theta(a) = -1$.
3. *Si* m *és parell, llavors* $\theta(a) = 1$ *per* $a \equiv 1, 1 - m$ *mod* 8 *i* $\theta(a) = -1$, *altrament.*

Bibliografia

[1] Lars V Ahlfors. Complex analysis: an introduction to the theory of analytic functions of one complex variable. *New York, London*, 177, 1953. Third edition.

[2] Tom M Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 1998. First edition.

[3] Robert B Ash. *A course in algebraic number theory*. Courier Corporation, 2010. First edition.

[4] Kenneth Ireland and Michael Rosen. A classical introduction to modern number theory. *Grad. Texts in Math*, 84, 1982. First edition.

[5] Michael J Jacobson and Hugh C Williams. *Solving the Pell equation*. Springer, 2009. First edition.

[6] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saitō. *Number Theory: Fermat's dream*. American Mathematical Society, 2000. First edition.

[7] Kazuya Kato, Nobushige Kurokawa, Takeshi Saitō, and Masato Kurihara. *Number Theory: introduction to class field theory*, volume 186. American Mathematical Society, 2011. First edition.

[8] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9. American Mathematical Society, 2021. First edition.

[9] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013. First edition.

[10] Miquel Raïch Regue. La funció ζ de riemann, diverses meravelles de la funció. `https://mat.uab.cat/~francesc/mates/MiquelRaichTFG.pdf`, 2011.

[11] Andrew V Sutherland. 14 the minkowski bound and finiteness results. `https://math.mit.edu/classes/18.785/2017fa/LectureNotes14.pdf`, 2019.

[12] Andrew V Sutherland. 15 dirichlet's unit theorem. `https://math.mit.edu/classes/18.785/2017fa/LectureNotes15.pdf`, 2019.

[13] Andrew V Sutherland. 19 the analytic class number formula. `https://math.mit.edu/classes/18.785/2017fa/LectureNotes19.pdf`, 2019.

[14] Andrew V Sutherland. 8 complete fields and valuation rings. `https://math.mit.edu/classes/18.785/2017fa/LectureNotes8.pdf`, 2019.

[15] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997. Second edition.

Apèndix A

Codi Sage exemple 4

Listing A.1: Càlcul del nombre de classes del cos $\mathbb{Q}(\sqrt{15})$.

```
m=115
if(m%4 == 1): D=m
else: D=4*m
f=abs(D)
from sage.modular.dirichlet import DirichletCharacter
H = DirichletGroup(f, QQ)
M = H._module
chi = DirichletCharacter(H, M([1,1,1]))
K=chi.kernel()
Zn=Zmod(f)
U = [a for a in Zn if gcd(a,f) == 1]
r=e^(2*i*pi/f)
def h(a):return(chi(a)*r^a)
G=sum(h(a) for a in U)
def g(a):return(chi(a)*log(abs(1-r^a)))
L=-G/f*(sum(g(a) for a in U))
if(m%4 == 1): s=2; q=1
else: s=1;q=0
delta= (q+sqrt(m))/s
qi=list();Q=list();P=list();G=list();B=list()
P.append(q);Q.append(s);qi.append(floor((sqrt(m)+q)/s))
G.append(s*qi[0]-q);Bm1=0;B.append(1);Gm1=s
P.append(qi[0]*Q[0]-P[0])
Q.append((m-(P[1])^2)/Q[0])
qi.append(floor((P[1]+floor(sqrt(m)))/Q[1]))
G.append(qi[1]*G[0]+Gm1)
B.append(qi[1]*B[0]+Bm1)
t=1
while(Q[t]!=s):
    P.append(qi[t]*Q[t]-P[t])
    Q.append((m-(P[t+1])^2)/Q[t])
    qi.append(floor((P[t+1]+floor(sqrt(m)))/Q[t+1]))
    G.append(qi[t+1]*G[t]+G[t-1])
    B.append(qi[t+1]*B[t]+B[t-1])
    t+=1
epsilon=(G[t-1]+sqrt(m)*B[t-1])/s;epsilon
R=log(epsilon)
hk=sqrt(D)/(2*R)*L;numerical_approx(hk)
```