UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

EL CRITERI DE KUMMER PER A LA REGULARITAT DE PRIMERS

Autor: Eudald Vilar Pagès

Director: Dr. Francesc Fité Naya
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de juny de 2024

Abstract

Fermat's Last Theorem, written in 1637, states that the equation $x^n + y^n = z^n$ has no non-trivial solutions for integer x, y, z and integer $n > 3$. Fermat never wrote down the proof of this theorem, but he did prove the case for $n = 4$ and that it was sufficient to prove the case for prime $n = p$. It was not until 1995 that Andrew Wiles proved the theorem.

During the first 200 years, there were various contributions to the proof, until the mid-19th century when a paradigm shift occurred with Ernst Kummer. Kummer proved that the theorem was true in the case that p does not divide the class number of $\mathbb{Q}(\zeta_p)$. He called primes satisfying this condition regular primes. I take this opportunity to mention that my colleague Pol Plans has proven this case in his work [6].

The case where p is irregular has never been proven, as Wiles' proof does not continue Kummer's proof. Nevertheless, in this work, I prove a statement that Kummer himself already demonstrated, which is the following:

Teorema 0.1. *Let p be an odd prime and $B_1, \ldots, B_p$ be Bernoulli numbers. Then:*

$$p|h(\mathbb{Q}(\zeta_p)) \iff p|B_j, \quad \text{for some } j = 2, 4, \ldots, p-3.$$

To prove this theorem, I separate it into two double implications. These are:

$$p|h(\mathbb{Q}(\zeta_p)) \iff p|h^-(\mathbb{Q}(\zeta_p)) \iff p|B_j, \quad \text{for some } j = 2, 4, \ldots, p-3.$$

I prove both in theorem 7. The one that will take more work is the second. First, I prove a formula for the discriminant of a field in terms of the associated Dirichlet characters. Then, using the generalized Bernoulli numbers, I provide an expression for the relative class number h^-. Finally, with the help of p-adic numbers, fields, and functions, I find a modular p equivalence between h^- and B_j, thus proving the second double implication. With all the work done, a new definition, and a couple of results that I do not prove, I also deduce the first, thus proving theorem 0.2.

For a full understanding of this work, it is assumed that one has taken courses in arithmetic, algebraic structures, and algebraic equations. Additionally, it is recommended to have taken courses in algebraic methods in number theory and analytical methods in number theory. Nevertheless, in the first chapter, I provide a quick summary defining the necessary concepts to introduce the concepts of class number, ramified primes, and discriminant.

In the second chapter, I present Dirichlet characters and define the field associated with one or more Dirichlet characters. Finally, I conclude the chapter by proving the Conductor-Discriminant formula.

In the third chapter, I introduce the various Bernoulli numbers and find the value of the L function at negative integers and also at 1 in terms of the Bernoulli numbers.

In the fourth chapter, I define p-adic fields, first defining valuations and non-Archimedean absolute values, and finally, using completions, I define the p-adic fields.

In the fifth chapter, I define the functions $\exp_p$, $\log_p$, $<>$, H_p, and L_p. These functions are defined in p-adic fields.

Finally, in the sixth and last chapter of the work, I prove Kummer's theorem using Kummer's congruences and the L_p functions

Resum

L'últim teorema de Fermat escrit l'any 1637 afirma que l'equació $x^n + y^n = z^n$ no té solucions no trivials per a x, y, z enters i $n > 3$ enter. Fermat mai va deixar per escrit la demostració d'aquest teorema, però va demostrar el cas $n = 4$ i que n'hi havia prou en demostrar el cas per $n = p$ primer. No va ser fins el 1995 que Andrew Wiles va demostrar el teorema.

Durant els primers 200 anys hi van haver diverses aportacions per a la demostració, fins a mitjans del segle XIX que es va produir un canvi de paradigma amb Ernst Kummer. Kummer va demostrar que el teorema era cert en el cas que p no divideix el nombre de classes de $\mathbb{Q}(\zeta_p)$. Va anomenar primers regulars als que complien aquesta condició. Aprofito l'avinentesa per comentar que el meu company Pol Plans ha demostrat aquest cas al seu treball [6]

El cas que p sigui irregular no s'ha demostrat mai, ja que la demostració de Wiles no continua la demostració de Kummer. Tot i això, en aquest treball demostro un enunciat que el mateix Kummer ja va demostrar, que és la següent:

Teorema 0.2. *Sigui p un primer senar i $B_1, \ldots, B_p$ nombres de Bernoulli. Aleshores són equivalents:*

$$p|h(\mathbb{Q}(\zeta_p)) \Longleftrightarrow p|B_j, \quad \text{per algun } j = 2, 4, \ldots, p-3.$$

Per a la demostració d'aquest teorema ho separo en dues dobles implicacions. Aquestes són:

$$p|h(\mathbb{Q}(\zeta_p)) \Longleftrightarrow p|h^-(\mathbb{Q}(\zeta_p)) \Longleftrightarrow p|B_j, \quad \text{per algun } j = 2, 4, \ldots, p-3.$$

Demostro les dues en el capítol 7. La que portarà més feina és la segona. Primer provo una fórmula pel discriminant d'un cos en funció dels caràcters de Dirichlet que tingui associats. A continuació amb els nombres de Bernoulli generalitzats dono una expressió per al nombre relatiu de classes h^-. Finalment, amb ajuda dels nombres, cossos i funcions p-àdics trobo una equivalència mòdul p entre h^- i B_j, provant així la segona doble implicació. Amb tota la feina feta, una nova definició i un parell de resultats que no demostro, dedueixo també la primera, demostrant així el teorema 0.2.

Per a la plena comprensió d'aquest treball es suposa haver cursat les assignatures d'aritmètica, estructures algebraiques, equacions algebraiques. A més es recomana haver cursat mètodes algebraics en teoria de nombres i mètodes analítics en teoria de nombres. Tot i això, en el primer capítol faig un resum ràpid definint els conceptes necessaris per introduir els conceptes de nombre de classes, primers ramificats i discriminant.

En el segon capítol presento els caràcters de Dirichlet i defineixo el cos associat a un o diversos caràcters de Dirichlet. Finalment, acabo el capítol demostrant la fórmula del Conductor-Discriminant.

En el tercer capítol introdueixo els diversos nombres de Bernoulli i trobo el valor en els enters negatius i també en el 1 de la funció L en funció dels nombres de Bernoulli.

En el quart capítol defineixo els cossos p-àdics, definint primer valoracions i valors absoluts no arquimedians, i finalment mitjançant complecions definir els cossos p-àdics.

En el cinquè capítol defineixo les funcions $\exp_p$, $\log_p$, $<>$, H_p, i L_p. Aquestes funcions estan definides en cossos p-àdics.

Finalment, en el sisè i últim capítol del treball demostrem el teorema de Kummer, utilitzant les congruències de Kummer i les funcions L_p.

2020 Mathematics Subject Classification. 11R29, 11B68, 11D88, 11M20

Agraïments

En primer lloc, vull expressar la meva més profunda gratitud al meu tutor, Francesc Fité, per la seva guia inestimable, suport i encoratjament durant el desenvolupament d'aquest treball de fi de grau. Les seves idees i coneixements han estat essencials per donar forma a aquest treball.

També vull agrair de tot cor als meus companys de la facultat, que han aguantat llargues hores amb mi a la biblioteca. La vostra companyonia i suport han fet aquest viatge més agradable i suportable.

Agrair a la Júlia Vilageliu per les seves meticuloses correccions gramaticals i el seu ull atent per als detalls, que han millorat notablement la claredat i la qualitat d'aquest treball.

Finalment, estic profundament agraït a la meva família, gràcies per la vostra paciència i per escoltar les meves explicacions, tot i que en general no s'entenia res.

Gràcies a tots per les vostres contribucions i suport.

Índex

1 Introducció

1.1 Conceptes previs

Primer de tot, llistem una sèrie de definicions i resultats que no demostrarem. Amb aquesta secció volem definir bé els conceptes necessaris per entendre l'objectiu final del treball. Així doncs, al final de la secció donarem sentit al que enunciarem durant aquesta.

Definició 1.1 (DFU)**.** *Un domini de factorització única (DFU) és un anell íntegre en què tot element descompon totalment de manera única en primers.*

Definició 1.2 (Anell de Dedekind)**.** *Un anell de Dedekind és un domini d'integritat que és noetherià, és íntegrament tancat, no és un cos i tal que tot ideal primer no nul és maximal.*

Observació 1.3. En general un anell de Dedekind no és un DFU, però el grup dels seus ideals compleix el següent resultat.

Proposició 1.4. *En un anell de Dedekind tot ideal no nul descompon de manera única com a producte d'ideals primers no nuls.*

Definició 1.5 (Cos de nombres)**.** *Un cos de nombres algebraics o simplement cos de nombres és una extensió de cos K del cos dels nombres racionals $\mathbb{Q}$ tal que l'extensió $K/\mathbb{Q}$ té grau finit.*

Definició 1.6 (Anell d'enters d'un cos de nombres)**.** *Donat un cos de nombres K, definim el seu anell d'enters o anell d'enters algebraics $\mathcal{O}_K$ com les arrels a K de polinòmics mònics amb coeficients enters.*

Definició 1.7 (Cos ciclotòmic)**.** *Sigui ζ_n una arrel primitiva n-èssima de la unitat. Aleshores definim el n-èssim cos ciclotòmic com $\mathbb{Q}(\zeta_n)$.*

Definició 1.8 (Ideal fraccionari)**.** *Sigui R un domini d'integritat i sigui K el cos de fraccions de R. Definim un ideal fraccionari de R com un R-submòdul I de K tal que existeix un element no nul $a \in A$ de manera que $a\,I \subset R$.*

Definició 1.9 (Grup de classes d'anells)**.** *El grup de classes d'anells d'un cos de nombres K és el grup quocient J_K/P_k, on J_K és el grup d'anells fraccionaris i P_K és el grup d'anells fraccionaris principals.*

Definició 1.10 (Nombre de classes)**.** *Sigui K un cos de nombres. Anomenarem nombre de classes al cardinal del grup de classes d'anells. El denotarem per $h(K)$.*

Aquest nombre ens indica com de l·lluny"està el nostre cos de nombres K de ser un DFU. Com més gran el nombre de classes, més elements irreductibles del cos no són primers.

1.2 Ramificació

En aquesta secció introduïm el concepte d'índex de ramificació i de grau residual. Després les usem per

Definició 1.11. *Sigui L/K una extensió de cossos de nombres i siguin $\mathcal{O}_L$ i $\mathcal{O}_K$ els anells d'enters dels cossos L i K respectivament. Sigui $\mathfrak{P}$ un ideal primer de $\mathcal{O}_L$. Sigui $\mathfrak{p} = \mathfrak{P} \bigcap \mathcal{O}_K$. Aleshores la factorització de $\mathfrak{p}$ en ideals primers de $\mathcal{O}_L$ és:*

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}' \subset \mathcal{O}_L} (\mathfrak{P}')^{e_{L/K}(\mathfrak{P}')}.$$

On un dels termes és $\mathfrak{P}^{e_{L/K}(\mathfrak{P})}$. Direm que $\mathfrak{P}$ està sobre $\mathfrak{p}$. Definim l'índex de ramificació de $\mathfrak{P}$ com $e_{L/K}(\mathfrak{P})$ i definim el grau residual $f_{L/K}(\mathfrak{P})$ com $f_{L/K}(\mathfrak{P}) = [\mathcal{O}_L/\mathfrak{P}\mathcal{O}_K/\mathfrak{p}]$.

L'índex de ramificació i el grau residual són multiplicatius. És a dir, compleixen la següent proposició.

Proposició 1.12. *Siguin $K \subseteq K' \subseteq K''$ tres cossos de nombres i sigui $\mathfrak{p}''$ un primer de K''. Definim $\mathfrak{p}' = \mathfrak{p}'' \bigcap \mathcal{O}_{K'}$ i $\mathfrak{p} = \mathfrak{p}' \bigcap \mathcal{O}_K$. Aleshores*

$$f_{K''/K}(\mathfrak{p}'') = f_{K''/K'}(\mathfrak{p}'') f_{K'/K}(\mathfrak{p}'),$$
$$e_{K''/K}(\mathfrak{p}'') = e_{K''/K'}(\mathfrak{p}'') e_{K'/K}(\mathfrak{p}').$$

Definició 1.13. *Sigui $\mathfrak{p}$ un ideal de $\mathcal{O}_K$ amb descomposició en ideals primer de $\mathcal{O}_L$*

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}' \subset \mathcal{O}_L} (\mathfrak{P}')^{e_{L/K}(\mathfrak{P}')}.$$

Direm que $\mathfrak{p}$ no ramifica en L si $e_{L/K}(\mathfrak{P}') = 1$ per tot $\mathfrak{P}'$ en la factorització de $\mathfrak{p}$. Altrament, direm que $\mathfrak{p}$ ramifica en L. A més, si $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P})^{e_{L/K}(\mathfrak{P})}$, direm que p ramifica totalment en L.

Proposició 1.14. *Sigui L/K una extensió abeliana, és a dir, de Galois i amb grup de Galois abelià. Sigui $\mathfrak{p}$ un ideal de $\mathcal{O}_K$ amb la següent descomposició en ideals primer de $\mathcal{O}_L$:*

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}' \subset \mathcal{O}_L} (\mathfrak{P}')^{e_{L/K}(\mathfrak{P}')}.$$

Aleshores per qualsevol $\mathfrak{P}', \mathfrak{P}''$ per sobre de $\mathfrak{p}$, tenim que $e_{L/K}(\mathfrak{P}') = e_{L/K}(\mathfrak{P}'')$.

Demostració. Es dedueix del fet que tot grup abelià descompon com a producte directe de p-subgrups i aquests com a producte directe de subgrups cíclics. □

Per tant, en extensions abelianes no cal fer distincions entre els índexs de ramificació dels $\mathfrak{P}'$. Aleshores, fent un abús de notació, parlem de $e_{L/K}(\mathfrak{p})$, ja que és independent del $\mathfrak{P}$ escollit. Per raonaments similars, també es té el mateix cas amb el grau residual $f_{L/K}(\mathfrak{p})$. Aprofitant aquests fets, podem definir ramificació per extensions cossos de nombres de la següent manera:

Definició 1.15. *Sigui L/K una extensió de cossos de nombres abeliana tal que cap ideal primer de K és ramificat en L. Diem aleshores que L/K és una extensió no ramificada.*

Un resultat de teoria de nombres que no en veiem la demostració relaciona el grup de Galois de la màxima extensió abeliana no ramificada de K amb el seu anell d'enters.

Teorema 1.16. *Sigui K un cos de nombres. Sigui L/K la màxima extensió abeliana no ramificada de K. Aleshores*

$$Gal(L/K) \simeq \mathrm{Cl}_K.$$

On Cl_K és el grup de classes d'anells de K.

Directament del teorema tenim el següent corol·lari.

Corołari 1.17. *Per tota extensió abeliana $L/\mathbb{Q}$, existeix un primer p de $\mathbb{Q}$ ramificat en L.*

Demostració. Tenim que $h(\mathbb{Q})$ és un grup amb un sol element, ja que és un DFU, i el grup $\mathrm{Gal}(L/\mathbb{Q})$ té sempre més d'un element si $L \neq \mathbb{Q}$. Per tant com no són isomorfs, tenim pel teorema que existeix un primer de $\mathbb{Q}$ ramificat en L. □

Anem a veure un exemple per una extensió abeliana de $\mathbb{Q}$, per deixar clar quan un primer ramifica en K i quan un primer no hi ramifica.

Exemple 1.18. Sigui $K = \mathbb{Q}(\zeta_3)$. Anem a veure que 7 no ramifica a K. Per fer-ho hem de trobar la descomposició en ideals primers de $7\mathcal{O}_K$. Primer, busquem un element de K que tingui norma 7.

$$\begin{aligned} N(a+b\zeta_3) &= 7, \\ (a+b\zeta_3)(a+b\zeta_3^2) &= 7, \\ a^2+ab\zeta_3^2+ab\zeta_3+b^2 &= 7, \\ a^2-ab+b^2 &= 7. \end{aligned}$$

Escollint $a = 2$ i $b = -1$ obtenim la igualtat. Per tant hem vist que

$$7\mathcal{O}_K = (2-\zeta_3)(2-\zeta_3^2).$$

Com els dos ideals són diferents, aleshores 7 no ramifica en K. Ara veiem que 3 sí que ramifica en K. Novament, trobem la descomposició en ideals primer de $3\mathcal{O}_K$ buscant primer un element de K que tingui norma 3.

$$\begin{aligned} N(a+b\zeta_3) &= 3, \\ a^2-ab+b^2 &= 3. \end{aligned}$$

Escollint $a = 1$ i $b = -1$ obtenim la igualtat. Aleshores ens queda:

$$3\mathcal{O}_K = (1-\zeta_3)(1-\zeta_3^2).$$

Però com les arrels 3-èssimes primitives de la unitat són les següents:

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2}, \quad \zeta_3^2 = \frac{-1-\sqrt{-3}}{2}.$$

Observem que:

$$-\zeta_3 - 1 = \frac{1-\sqrt{-3}}{2} - \frac{2}{2} = \frac{-1-\sqrt{-3}}{2} = \zeta_3^2.$$

I per tant hem obtingut:

$$3\mathcal{O}_K = (1-\zeta_3)(1-\zeta_3^2) = (1-\zeta_3)(1-(-\zeta_3-1)) = (1-\zeta_3)^2.$$

Així doncs, 3 ramifica en $\mathbb{Q}(\zeta_3)$.

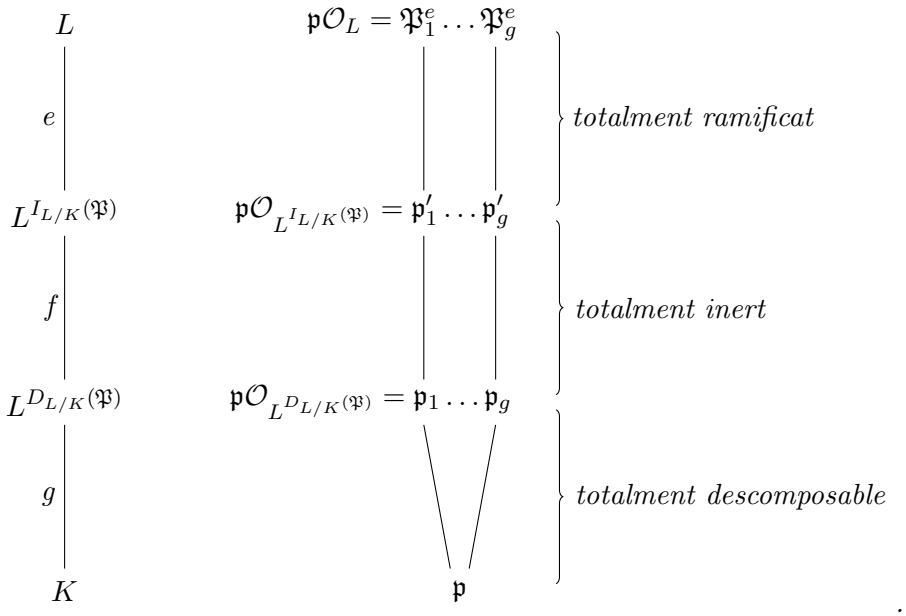
Anem a veure una equivalència per saber quan un primer ramificarà en el cos ciclotòmic. També comentem un cas més general que no involucra cossos ciclotòmics, però no entra dins dels objectius del treball i per tant no el demostrem.

Més endavant parlarem dels subgrups de descomposició i inèrcia d'una extensió abeliana L/K. Els definim ara i justifiquem tant els seus graus com les ramificacions entre les subextensions.

Definició 1.19. *Sigui L/K una extensió de cossos de nombres de Galois. Sigui $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$ i $\mathfrak{P}$ un ideal primer sobre $\mathfrak{p}$ de $\mathcal{O}_L$. Aleshores definirem el grup de descomposició $D_{L/K}(\mathfrak{P})$ i el grup d'inèrcia $I_{L/K}(\mathfrak{P})$ com:*

$$\begin{aligned} D_{L/K}(\mathfrak{P}) &:= \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{P}) = \mathfrak{P}\}, \\ I_{L/K}(\mathfrak{P}) &:= \left\{\sigma \in D_{L/K}(\mathfrak{P}) | \sigma(x) = x \pmod{\mathfrak{P}}, \quad \forall x \in \mathcal{O}_L\right\}. \end{aligned}$$

Teorema 1.20. *Sigui K/L una extensió de cossos de nombres de Galois tal que $[K : L] = efg$. Sigui $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \dots \mathfrak{P}_g^e$. Aleshores obtenim el següent diagrama:*



On $\mathfrak{P} = \mathfrak{P}_i$ per algun i qualsevol, totalment descomposable indica que els primers $\mathfrak{p}_i$ no tornaran a descomposar-se i totalment inert indica que ni es ramifiquen ni es descomposen.

Demostració. El primer que demostrem és que $\#D(\mathfrak{P}) = ef$. Per veure-ho cal observar que $\mathrm{Gal}(L/K)$ actua transitivament sobre els primers $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ i que els grup de descomposició és l'estabilitzador. El primer fet és clar, doncs per qualsevol dos $\mathfrak{P}_i, \mathfrak{P}_j$ existeix una $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, doncs els elements de $\mathrm{Gal}(L/K)$ permuten els $\mathfrak{P}_l$. El segon fet també ho és, doncs els elements de $\mathrm{Gal}(L/K)$ actuen trivialment sobre PP_i. Aleshores, tenim que

$$\#D(\mathfrak{P}) = \#(\mathrm{Est}_{\mathfrak{P}}(\mathrm{Gal}(L/K))) = \frac{\#\mathrm{Gal}(L/K)}{\#\grave{\mathrm{O}}\mathrm{rb}(\mathfrak{P})} = \frac{efg}{g} = ef.$$

L'òrbita té g elements, doncs la imatge d'un $\mathfrak{P}$ per una σ de $\mathrm{Gal}(L/K)$ poden ser qualsevol dels g elements $\mathfrak{P}_j$. El següent que veurem és que el grau residual de $\mathfrak{P}$ és f. Per definició tenim que

$$f_{L/K}(\mathfrak{P}) = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [\mathbb{F}_{q^f} : \mathbb{F}_q].$$

La segona igualtat surt de que $\mathcal{O}_L/\mathfrak{P}$ i $\mathcal{O}_K/\mathfrak{p}$ són finits, per tant existeix un primer q tal que ho compleix. Ara, com el grau de l'extensió $\mathbb{F}_{q^f}/\mathbb{F}_q$ és igual al cardinal del grup $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$, tenim que per l'automorfisme de Frobenius,

$$[\mathbb{F}_{q^f} : \mathbb{F}_q] = \#\mathrm{Gal}\left(\mathbb{F}_{q^f}/\mathbb{F}_q\right) = f.$$

Per acabar, demostrem que $\#I_{L/K}(\mathfrak{P}) = e$. En tenim prou, doncs ja sabem que $[L^{D_{L/K}(\mathfrak{P})} : K] = g$ ja que $[l : L^{D_{L/K}(\mathfrak{P})}] = ef$. Per fer-ho considerem la següent successió

$$1 \to I_{L/K}(\mathfrak{P}) \to D_{L/K}(\mathfrak{P}) \to \mathrm{Gal}\left(\mathbb{F}_{q^f}/\mathbb{F}_q\right) \to 1.$$

Si veiem que la successió és exacte, ja tindrem que $\#I_{L/K}(\mathfrak{P}) = e$, doncs $[l : L^{D_{L/K}(\mathfrak{P})}] = ef$ i $\#\mathrm{Gal}\left(\mathbb{F}_{q^f}/\mathbb{F}_q\right) = f$. L'aplicació entre $I_{L/K}(\mathfrak{P})$ i $D_{L/K}(\mathfrak{P})$ té per imatge $\mathfrak{P}$, i com l'aplicació entre $D_{L/K}(\mathfrak{P})$ i $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$ té per nucli $\mathfrak{P}$, la successió és exacte. □

Havent acabat aquesta demostració, veiem ara la definició de discriminant. Amb aquesta definició podrem caracteritzar quins primers ramifiquen al cos en el que estiguem treballant i també quins no.

Definició 1.21 (Discriminant)**.** *Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Sigui $b_1, \ldots, b_n$ una base de $\mathcal{O}_K$ i $\sigma_1, \ldots, \sigma_n$ el conjunt del les immersions de K en els complexos. Es defineix doncs el discriminant de K com el quadrat del determinant de la matriu $(\sigma_i(b_j))_{j=1,\ldots,n}^{i=1,\ldots,n}$. És a dir:*

$$d(K) = \begin{vmatrix} \sigma_1(b_1) & \ldots & \sigma_1(b_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(b_1) & \ldots & \sigma_n(b_n) \end{vmatrix}^2.$$

Separarem les immersión amb reals i no reals. Anomenarem r_1 el cardinal d'immersions reals i $2r_2$ el d'immersions no reals. Per tant, seguint la notació del teorema, tindrem que $n = r_1 + 2r_2$. El signe del determinant es pot obtenir usant el següent resultat:

Proposició 1.22. *Sigui K un cos de nombres i r_2 el nombre de parelles d'immersions complexes. Aleshores $d(K)$ té signe $(-1)^{r_2}$.*

Demostració. Sigui $\alpha_1, \ldots, \alpha_m$ una base de $\mathcal{O}_K$. Aleshores $d(K) = (\det(\sigma(\alpha_i)_i^\sigma))^2$. Si σ és una immersió no real, aleshores $\bar{\sigma}$ és una altre immersió, on la barra indica la conjugació complexa. Per tant

$$\overline{\det(\sigma(\alpha_i))} = (-1)^{r_2} \det(\sigma(\alpha_i)),$$

ja que r_2 files han estat intercanviades. Si r_2 és parell, aleshores el determinant és real i per tant $d(K) > 0$. Si r_2 és senar, aleshores el determinant és imaginari i per tant $d(K) < 0$. □

El següent teorema ens dona una equivalència entre ramificació de primers i divisibilitat respecte el discriminant. És un teorema que no demostrarem en aquest treball.

Teorema 1.23. *Sigui K un cos de nombres i p un primer senar. Aleshores:*

$$p \text{ ramifica a } K \iff p \big| d(K).$$

Pel cas $\mathbb{Q}(\zeta_p)$ tenim que no és complicat calcular el discriminant i gràcies al teorema, també saber quins són els primers que hi ramifiquen.

Proposició 1.24. *Al cos de nombres $\mathbb{Q}(\zeta_p)$, p és l'únic primer ramificat.*

Demostració. En virtut del teorema anterior, en tindrem prou en calcular el discriminant de $K = \mathbb{Q}(\zeta_p)$. Tenim que una base de $\mathcal{O}_K$ és $1, \zeta_p, \ldots, \zeta_p^{p-2}$, i les immersions són $\sigma_1, \ldots, \sigma_{p-1}$ tals que $\sigma_j(\zeta_p) = \zeta_p^j$. Aleshores tenim que:

$$d(\mathbb{Q}(\zeta_p)) = \begin{vmatrix} \sigma_1(1) & \sigma_2(\zeta_p) & \ldots & \sigma_1(\zeta_p^{p-3}) & \sigma_1(\zeta_p^{p-2}) \\ \sigma_2(1) & \sigma_2(\zeta_p) & \ldots & \sigma_2(\zeta_p^{p-3}) & \sigma_2(\zeta_p^{p-2}) \\ \vdots & & \ddots & & \vdots \\ \sigma_{p-2}(1) & \sigma_{p-2}(\zeta_p) & \ldots & \sigma_{p-2}(\zeta_p^{p-3}) & \sigma_{p-2}(\zeta_p^{p-2}) \\ \sigma_{p-1}(1) & \sigma_{p-1}(\zeta_p) & \ldots & \sigma_{p-1}(\zeta_p^{p-3}) & \sigma_{p-1}(\zeta_p^{p-2}) \end{vmatrix}^2,$$

$$= \begin{vmatrix} 1 & \zeta_p & \ldots & \zeta_p^{p-3} & \zeta_p^{p-2} \\ 1 & \zeta_p^2 & \ldots & \left(\zeta_p^{(p-3)}\right)^2 & \left(\zeta_p^{(p-2)}\right)^2 \\ \vdots & & \ddots & & \vdots \\ 1 & \zeta_p^{(p-2)} & \ldots & \left(\zeta_p^{(p-3)}\right)^{(p-2)} & \left(\zeta_p^{(p-2)}\right)^{(p-2)} \\ 1 & \zeta_p^{(p-1)} & \ldots & \left(\zeta_p^{(p-3)}\right)^{(p-1)} & \left(\zeta_p^{(p-2)}\right)^{(p-1)} \end{vmatrix}^2.$$

Ens queda una matriu Vandermonde, per tant podem aplicar la fórmula per a determinants de matrius Vandermonde i obtenim el següent resultat:

$$d(\mathbb{Q}(\zeta_p)) = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 = (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{\substack{1 \le i,j \le p-1 \\ i \ne j}} (\zeta_p^i - \zeta_p^j)$$

Ara, per propietats de les arrels de la unitat i separant per la classe de p mòdul 4:

$$d(\mathbb{Q}(\zeta_p)) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2} = \begin{cases} p^{p-2} & \text{si } p \equiv 1 \pmod 4 \\ -p^{p-2} & \text{si } p \equiv 3 \pmod 4 \end{cases}.$$

Per tant, l'únic primer que divideix el discriminant és p. □

Més generalment, es pot veure que $L = \mathbb{Q}(\zeta_p^a)$ és totalment ramificat a p. Nogensmenys, hem provat una fórmula per a calcular el discriminant del cos ciclotòmic p-èssim. En el següent capítol veiem una fórmula més general.

2 Fórmula del Conductor-Discriminant

L'objectiu d'aquesta secció serà demostrar la fórmula del Conductor-Discriminant. La fórmula donarà un valor pel discriminant d'un cos qualsevol. Per la fórmula necessitarem les definicions de Caràcters de Dirichlet i el seu cos associat.

2.1 Caràcters de Dirichlet

En aquesta secció introduirem el concepte de caràcter de Dirichlet i del seu conductor, i definirem el cos associat a un grup de caràcters de Dirichlet. També en comentarem algunes propietats que usarem en les properes seccions.

Definició 2.1 (Caràcter de Dirichlet)**.** *Un caràcter de Dirichlet mòdul m és una aplicació*

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C},$$

tal que, existeix un homomorfisme

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

que compleix les següents condicions:

(1) $\chi(n) = \tilde{\chi}(n)$ *si* $(n, m) = 1$*,*

(2) $\chi(n) = 0$ *altrament.*

Direm que χ està associat a $\tilde{\chi}$.

Definició 2.2 (Conductor)**.** *Sigui χ un caràcter de Dirichlet mòdul m associat a un homomorfisme $\tilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. El conductor de χ és el menor $n \in \mathbb{N}$ tal que $n|m$ i existeix un diagrama commutatiu*

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times & \longrightarrow & \mathbb{C}^\times \\ & {\scriptstyle p}\searrow \quad \nearrow & \\ & (\mathbb{Z}/n\mathbb{Z})^\times & \end{array},$$

on p és la projecció natural. En altres paraules, el conductor de χ és el període de $\tilde{\chi}$. Anotarem per f_χ el conductor de χ.

Exemple 2.3. Sigui $n = 8$. Com $\#(\mathbb{Z}/8\mathbb{Z})^\times = 4$, tenim 4 caràcters de Dirichlet diferents, $\chi_0, \chi_1, \chi_2, \chi_3$, que estan definits de la següent manera:

χ_0: $\chi_0(1) = 1, \chi_0(3) = 1, \chi_0(5) = 1, \chi_0(7) = 1, \qquad f_{\chi_0} = 2,$

χ_1: $\chi_1(1) = 1, \chi_1(3) = -1, \chi_1(5) = -1, \chi_1(7) = 1, \qquad f_{\chi_1} = 8,$

χ_2: $\chi_2(1) = 1, \chi_2(3) = 1, \chi_2(5) = -1, \chi_2(7) = -1, \qquad f_{\chi_2} = 8,$

χ_3: $\chi_3(1) = 1, \chi_3(3) = -1, \chi_3(5) = 1, \chi_3(7) = -1, \qquad f_{\chi_3} = 4.$

El caràcter més simple és el següent:

$$\chi(m) = \begin{cases} 0 & \text{si } \gcd(n, m) \neq 1 \\ 1 & \text{si } \gcd(n, m) = 1 \end{cases}.$$

L'anomenarem caràcter principal i el denotarem per χ_0.

Definició 2.4. *Sigui χ un caràcter de Dirichlet. Si $\chi(-1) = 1$, direm que χ és parell. Altrament si $\chi(-1) = -1$ direm que és senar.*

Amb aquesta definició finalitzem la introducció als caràcters de Dirichlet. Com cada caràcter de Dirichlet mòdul n està associat a un homomorfisme de $(\mathbb{Z}/n\mathbb{Z})^\times$, i tenim l'equivalència $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, és natural pensar χ com un caràcter de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Definició 2.5 (Cos pertanyent a un caràcter de Dirichlet)**.** *Sigui χ un caràcter de Dirichlet mòdul m associat a $\tilde{\chi}$. Sigui τ l'isomorfisme entre $(\mathbb{Z}/m\mathbb{Z})^\times$ i $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Sigui $\tilde{\tilde{\chi}}$ la composició $\tilde{\chi} \circ \tau^{-1}$. Sigui $H \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ el nucli de $\tilde{\tilde{\chi}}$. Sigui $K = \mathbb{Q}(\zeta_m)^H$ el cos fix per H. Observem que K depèn únicament de χ i l'anomenarem cos pertanyent a χ.*

Més generalment, podem considerar un grup de caràcters de Dirichlet. En cas que no coincideixin en mòdul, considerarem tots els caràcters de Dirichlet mòdul el mínim comú múltiple. Observem que seguiran mantenint el seu conductor i els seus valors.

Definició 2.6. *Sigui X un grup de caràcters de Dirichlet mòdul m. Escrivim els elements de X com χ_i, amb $i = 1, \ldots, r$ associats cadascun a $\tilde{\chi}_i$. Sigui τ l'isomorfisme entre $(\mathbb{Z}/m\mathbb{Z})^\times$ i $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Sigui $\tilde{\tilde{\chi}}_i$ la composició $\tilde{\chi}_i \circ \tau^{-1}$. Siguin $H_i \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ el nucli de $\tilde{\tilde{\chi}}_i$ i anomenem $H = \bigcap_{i=1}^r H_i$ a la seva intersecció. Sigui $K = \mathbb{Q}(\zeta_m)^H$ el cos fix per H. Aleshores K depèn únicament de X i l'anomenem cos pertanyent a X.*

Observació 2.7. Es compleixen les següents propietats:

(1) X és un subgrup de caràcters de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

(2) X és el conjunt de homomorfismes de $\mathrm{Gal}(K/\mathbb{Q})$ a $\mathbb{C}^\times$.

(3) $K = \mathbb{Q}(\zeta_m)^H = K_1 \ldots K_r$, on K_i són els cossos pertanyent a χ_i.

(4) $\deg(K/\mathbb{Q}) = \#X = r$, i a més $X = \mathrm{Gal}(K/\mathbb{Q})^\vee$, el dual del grup de Galois.

(5) Si X és cíclic generat per χ, aleshores K és el cos associat a χ.

(6) El cos associat a χ es real si i només si χ és parell.

Exemple 2.8. Sigui X el conjunt de caràcters de $(\mathbb{Z}/n\mathbb{Z})^\times$. Aleshores com X és un grup cíclic generat per un χ_m tal que $\gcd(m, n) = 1$ i $m \neq 1$, tenim que L és el grup associat a χ_m. Per tant $K = \mathbb{Q}(\zeta_n)$.

Exemple 2.9. Sigui X el conjunt de caràcters parells de $(\mathbb{Z}/n\mathbb{Z})^\times$. Aleshores la conjugació complexa ($\zeta_n \mapsto \zeta_n^{-1}$) és el nucli de cada $\chi \in X$. El cos associat a X és doncs $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, que és el màxim subcòs real de $\mathbb{Q}(\zeta_n)$.

2.2 Fórmula del Conductor-Discriminant

El següent objectiu és demostrar la Fórmula del Conductor-Discriminant, que és la següent:

Teorema 2.10 (Fórmula del Conductor-Discriminant)**.** *Sigui K el cos de nombres associat al grup de caràcters de Dirichlet X. Aleshores el discriminant de K ve donat per*

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

Per a la demostració d'aquesta fórmula, necessitarem les següents definicions i resultats.

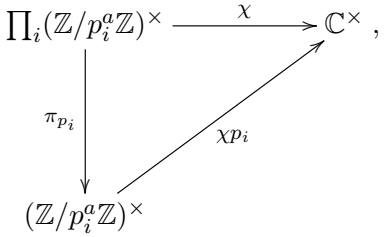
Definició 2.11. *Sigui $n = \prod_i p_i^{a_i}$. Aleshores podem escriure un caràcter de Dirichlet mòdul n qualsevol com*

$$\chi = \prod_i \chi_{p_i},$$

on χ_{p_i} és un caràcter de Dirichlet mòdul $p_i^{a_i}$, degut a l'equivalència:

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_i (\mathbb{Z}/p_i^a\mathbb{Z})^\times.$$

I a que el següent diagrama commuta:



on π_{p_i} és la projecció de la component i-èssima del productori. Sigui X un grup de caràcters de Dirichlet, aleshores definim

$$X_p = \{\chi_p | \chi \in X\}.$$

Definició 2.12. *Sigui K un cos de nombres i X el grup de caràcters de Dirichlet associat. Sigui $L \subseteq K$ un subcòs de K. Aleshores*

$$\mathrm{Gal}(L/Q)^\vee = \left\{\chi \in X \middle| \chi(g) = 1, \forall g \in \mathrm{Gal}(K/L)\right\} = Y.$$

Notarem per $G_Y = \mathrm{Gal}(K/L)$.

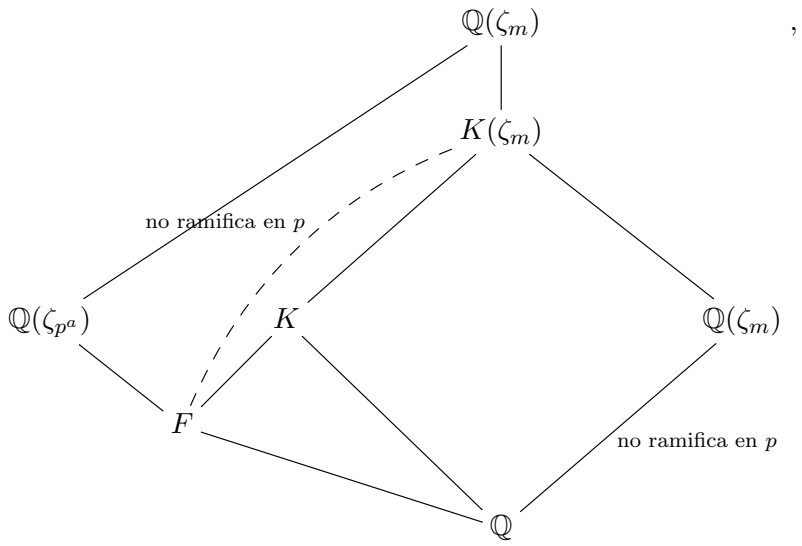
Observació 2.13. Amb la notació de la definició, tenim que $L = K^{G_Y}$.

El següent teorema caracteritza l'índex de ramificació amb els grups χ_p.

Teorema 2.14. *Sigui X un grup de caràcters de Dirichlet i K el cos associat. Sigui p un primer amb índex de ramificació e en K. Aleshores $e = \#(X_p)$.*

Demostració. Sigui n el mínim comú múltiple dels caràcters de X. Sigui doncs $n = p^a m$ tal que $p \not| m$. Sigui F el cos associat al grup de caràcters de Dirichlet X_p i considerem el

següent diagrama:



,

on $K(\zeta_m) = K \cdot \mathbb{Q}(\zeta_m)$. Aleshores tenim que:

$$\mathrm{Gal}(K/\mathbb{Q})^\vee = X = X_p \times \left(X \bigcap \prod_{q \neq p} (\mathbb{Z}/q^{a_q}\mathbb{Z})^\times \right).$$

D'altra banda obtenim de la igualtat:

$$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q})^\vee = X_p \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})^\vee.$$

I deduïm que:

$$K(\zeta_m) = F \times \mathbb{Q}(\zeta_m).$$

Per la multiplicitat de l'índex de ramificació, obtenim

$$e_{K(\zeta_m)/\mathbb{Q}}(p) = e_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(p) \cdot e_{K/\mathbb{Q}}(p) = e_{K/\mathbb{Q}}(p),$$

$$e_{K(\zeta_m)/\mathbb{Q}}(p) = e_{F/\mathbb{Q}}(p) \cdot e_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(p) = e_{F/\mathbb{Q}}(p).$$

Per tant serà suficient veure que $e_{F/\mathbb{Q}}(p) = X_p$. Per acabar utilitzarem que $\mathbb{Q}(\zeta_{p^a}/\mathbb{Q})$ està totalment ramificat. Per una demostració veure [1][Teorema 2.13]. Com $\mathbb{Q}(\zeta_p^a/\mathbb{Q})$ està totalment ramificat, aleshores F també està totalment ramificat i per tant:

$$e_{F/\mathbb{Q}}(p) = [F : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p^a})^{G_{X_p}} : \mathbb{Q}] = \frac{\#X}{\#G_{X_p}} = \#X_p.$$

□

Usem la proposició anterior per a provar una nova equivalència per a la ramificació d'un primer. Anteriorment hem provat la relació amb el discriminant d'un cos, i ara ho fem amb el caràcter de Dirichlet associat al cos.

Proposició 2.15. *Sigui χ un caràcter de Dirichlet i K el seu cos associat. Aleshores:*

$$p \text{ ramifica en } K \iff \chi(p) = 0.$$

Més generalment, sigui K el cos associat a un grup de caràcters de Dirichlet X. Aleshores:

$$p \text{ no ramifica en } K \iff \chi(p) \neq 0 \quad \forall \chi \in X.$$

Demostració. p ramifica en $K \leftrightarrow e_{K/\mathbb{Q}}(p) > 1 \leftrightarrow \#X_p > 1 \leftrightarrow \exists \chi \in X$ tal que $\chi_p \neq 1 \leftrightarrow \exists \chi \in X$ tal que $p \big| f_\chi \leftrightarrow \exists \chi \in X$ tal que $\chi(p) = 0$. □

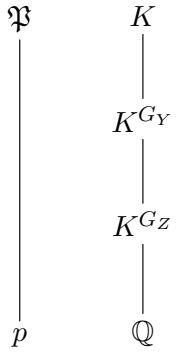
En el capítol 1 hem definit el grup de descomposició i el grup d'inèrcia d'una extensió de cossos de nombres de Galois. La proposició següent demostrem que el grau entre els dos grups és el grau de la classe residual, que en la notació del teorema 1.20 és f.

Proposició 2.16. *Sigui X un grup de caràcters de Dirichlet i K el seu cos associat. Siguin:*

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

Aleshores $f = [Y : Z]$ és el grau de la classe residual i Y/Z és un grup cíclic d'ordre f.

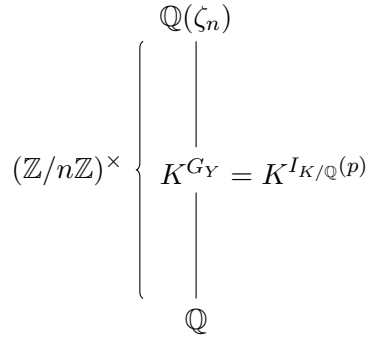
Demostració. Sigui p un primer de $\mathbb{Q}$ i $\mathfrak{P}$ un primer de K per sobre de p. Siguin $G_Y^\vee = Y$ i $G_Z^\vee = Z$. Aleshores considerem l'extensió de cossos següent



Per 2.16, com l'extensió $K^{G_Y}/\mathbb{Q}$ és la màxima subextenció en la qual p és no ramificat, G_y és el grup d'inèrcia. A més, el seu grau és:

$$[X : Y] = \frac{\#X}{\#Y} = \#G_Y = e.$$

Ara, sigui $n = \operatorname{lcm}_{\chi \in Y}(f_\chi)$. Ens fixem ara en la següent l'extensió:



,

on $(\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ i $\mathbb{Q}(\zeta_m) \subseteq K$. Tenim doncs una aplicació $(\mathbb{Z}/n\mathbb{Z})^\times \to {}^{\mathrm{Gal}(K/\mathbb{Q})}/_{I_{K/\mathbb{Q}}(\mathfrak{p})}$. Per altra banda, per l'aplicació $p \pmod n$ tenim un isomorfisme amb l'isomorfisme de Frobenius $< x \mapsto x^p >$. Seguidament observem que:

$$< x \mapsto x^p >= \mathrm{Gal}\left(\mathbb{F}_{p^f}/\mathbb{F}\right) = {}^{D_{K/\mathbb{Q}}(\mathfrak{p})}/_{I_{K/\mathbb{Q}}(\mathfrak{p})} \subseteq {}^{\mathrm{Gal}(K/\mathbb{Q})}/_{I_{K/\mathbb{Q}}(\mathfrak{p})}.$$

Per veure que són iguals, en tindrem prou en veure que un element de $\mathrm{Gal}\left(K^{G_Z}/\mathbb{Q}\right)^\vee$ també està en $\mathrm{Gal}\left(K^{D_{K/\mathbb{Q}}(\mathfrak{p})}/\mathbb{Q}\right)^\vee$. Aleshores obtenim les següents equivalències:

$$\chi \in \mathrm{Gal}\left(K^{G_Z}/\mathbb{Q}\right)^\vee \leftrightarrow \chi \in Z \leftrightarrow \chi(p) = 1 \leftrightarrow \chi\big|_{D_{K/\mathbb{Q}}(p)} = 1 \leftrightarrow \chi \in \mathrm{Gal}\left(K^{D_{K/\mathbb{Q}}(\mathfrak{p})}/\mathbb{Q}\right)^\vee.$$

Per tant $K^{G_Z} = K^{D_{K/\mathbb{Q}}(\mathfrak{p})}$. Aleshores $G_Z = D_{K/\mathbb{Q}}(\mathfrak{p})$ i $\#G_Z = ef$. Finalment, com $[Y : Z] = \#Y/\#Z = f$, hem vist que Y/Z és un grup cíclic d'ordre f. □

Definició 2.17 (Funció zeta de Dedekind de K)**.** *Sigui K un cos de nombres. Aleshores per $s > 1$ definim la funció zeta de Dedekind de K de la següent manera:*

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

on $\mathfrak{p}$ són els ideals primers de K.

Teorema 2.18. *Sigui X un grup de caràcters de Dirichlet, K el cos associat i $\zeta_K(s)$ la funció zeta de Dedekind de K. Aleshores*

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

Demostració. Per una banda, considerem un primer qualsevol i sigui $(p) = (\mathcal{P}_1, \ldots, \mathcal{P}_g)^e$ la factorització en primers de p en K, amb cada $\mathcal{P}$ amb grau de la classe residual f, per tant $N(\mathcal{P}) = p^f$. Aleshores $\zeta_K(s)$ conté el següent factor:

$$\prod_{\mathcal{P}|p} (1 - (N(\mathcal{P}))^{-s})^{-1} = (1 - p^{-fs})^{-g}.$$

Per altra banda, tenim que la funció L és:

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

No tenim en compte els $\chi \in X$ tals que $\chi(p) = 0$, ja que no contribueixen en el productori. Pel 2.16, Y/Z és cíclic d'ordre f, amb la notació $Y = \{\chi \in X | \chi(p) \neq 0\}$, $\quad Z = \{\chi \in X | \chi(p) = 1\}$. A mesura que χ passa pels representants de Y/Z, $\chi(p)$ passa per les arrels f-èssimes de la unitat. Cada conjunt té g elements. Ara, com:

$$\prod_{a=0}^{f-1} (1 - \zeta_f^a p^{-s}) = (1 - p^{-sf}),$$

doncs ja ho tenim. □

Ja hem provat totes les propietats que necessitarem per a la demostració de la fórmula del Discriminant-Conductor. Ens falten per definir les equacions funcionals de la funció ζ_K de Dedekind i de la funció L.

Proposició 2.19 (Equació funcional de ζ_K)**.** *Sigui Γ la funció gamma. La funció zeta de Dedekind de K compleix la 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

$$A = 2^{-r_2} \pi^{-N/2} \sqrt{|d(K)|},$$

amb $N = \deg(K/\mathbb{Q})$.

Demostració. Veure [2, p. 254]. □

Proposició 2.20 (Equació funcional de $L(s,\chi)$)**.** *Sigui* $\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a)e^{2\pi ia/f_\chi}$ *una suma de Gauss. La funció* L *compleix la següent equació funcional:*

$$\left(\frac{f_\chi}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi) = W_\chi \left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\overline{\chi}),$$

on $\delta = 0$ *si* $\chi(-1) = 1$ *i* $\delta = 1$ *si* $\chi(-1) = -1$ *i també:*

$$W_\chi = \frac{\tau(\chi)}{i^\delta \sqrt{f_\chi}},$$

amb $\prod_\chi W_\chi = 1$.

Demostració. Veure [1, p. 29]. □

Teorema 2.21 (Fórmula del Conductor-Discriminant)**.** *Sigui* K *el cos de nombres associat al grup de caràcters de Dirichlet* X*. Aleshores el discriminant de* K *ve donat per la següent fórmula:*

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

Demostració. Com $K/\mathbb{Q}$ és de Galois, tenim que o bé $r_1 = 0$ o bé $r_2 = 0$. Suposem primer que $r_2 = 0$. Per tant el cos K és totalment real i $\chi(-1) = 1$ per tot $\chi \in X$ i $N = r_1$. Expressant la equació funcional de ζ_K amb el canvi del 2.18 i aplicant que $r_2 = 0$, tenim:

$$\begin{aligned} A^s\Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2}\zeta_K(s) &= A^{1-s}\Gamma\left(\frac{1-s}{2}\right)^{r_1} \Gamma(1-s)^{r_2}\zeta_K(1-s), \\ A^s\Gamma\left(\frac{s}{2}\right)^{N} \prod_{\chi\in X} L(s,\chi) &= A^{1-s}\Gamma\left(\frac{1-s}{2}\right)^{N} \prod_{\chi\in X} L(1-s,\chi). \end{aligned} \tag{2.1}$$

En l'equació funcional de L, fem el productori a cada costat perquè passi per totes les χ de X i apliquem que $\delta = 0$.

$$\begin{aligned} \left(\frac{f_\chi}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi) &= W_\chi \left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\overline{\chi}), \\ \prod_{\chi\in X}\left(\frac{f_\chi}{\pi}\right)^{s/2} \Gamma\left(\frac{s}{2}\right) L(s,\chi) &= \prod_{\chi\in X} W_\chi \left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s}{2}\right) L(1-s,\overline{\chi}), \\ \Gamma\left(\frac{s}{\pi}\right)^{N} \prod_{\chi\in X}\left(\frac{f_\chi}{2}\right)^{s/2} L(s,\chi) &= \Gamma\left(\frac{1-s}{2}\right)^{N} \prod_{\chi\in X}\left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} L(1-s,\chi). \end{aligned} \tag{2.2}$$

Dividint l'expressió (2.1) per (2.2), obtenim:

$$\frac{A^s}{\prod_{\chi\in X}\left(\frac{f_\chi}{\pi}\right)^{s/2}} = \frac{A^{1-s}}{\prod_{\chi\in X}\left(\frac{f_\chi}{\pi}\right)^{(1-s)/2}}.$$

Aleshores, operant i simplificant arribem a veure que:

$$A^{2(s-1/2)} = \prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right)^{s-1/2},$$
$$A^2 = \prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right).$$

Finalment, substituint per l'expressió de A i simplificant, deduïm:

$$(\pi^{-N/2}\sqrt{|d(K)|})^2 = \prod_{\chi \in X} \left(\frac{f_\chi}{\pi}\right),$$
$$|d(K)| = \prod_{\chi \in X} f_\chi.$$

Per tant ja hem comprovat el cas que $r_2 = 0$. Sigui ara $r_1 = 0$. Aleshores $r_2 = N/2$ i observem que tenim el mateix nombre de χ parells que senars. Anem ara a tractar les equacions funcionals per separat i després dividirem com hem fet per l'altre cas. Per una banda, per l'equació funcional de ζ_K tenim

$$A^s\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s) = A^{1-s}\Gamma\left(\frac{1-s}{2}\right)^{r_1}\Gamma(1-s)^{r_2}\zeta_K(1-s)$$
$$A^s\Gamma(s)^{N/2}\prod_{\chi \in X} L(s,\chi) = A^{1-s}\Gamma(1-s)^{N/2}\prod_{\chi \in X} L(1-s,\chi) \tag{2.3}$$

Per altra banda, com en aquest cas tenim que hi ha el mateix nombre de caràcters de Dirichlet parells que senars, podem separar els productoris depenent dels valors de delta. Per tant partint de l'equació funcional de la funció L

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

El costat esquerre de la igualtat és igual a:

$$\prod_{\chi \in X}\left(\frac{f_\chi}{\pi}\right)^{s/2}\prod_{\chi \text{ parell}}\Gamma\left(\frac{s}{2}\right)L(s,\chi)\prod_{\chi \text{ senar}}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi).$$

De manera similar, el costat dret de la igualtat és:

$$\prod_{\chi \in X} W_\chi\left(\frac{f_\chi}{\pi}\right)^{(1-s)/2}\prod_{\chi \text{ parell}}\Gamma\left(\frac{1-s}{2}\right)L(1-s,\overline{\chi})\prod_{\chi \text{ senar}}\Gamma\left(\frac{2-s}{2}\right)L(1-s,\overline{\chi}).$$

Ara traiem les funcions Gamma fora dels productoris apliquem la fórmula de la duplicació, que diu el següent:

$$\Gamma(s) = \Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right).$$

Per tant la banda esquerra ens queda:

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

I la banda dreta:

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

Finalment aplicant que $\prod_{\chi\in X} W_\chi = 1$:

$$\left(\frac{f_\chi}{\pi}\right)^{Ns/2} 2^{N(1-s)/2}\Gamma(s)^{N/2} \prod_{\chi\in X} L(s,\chi) = \left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} 2^{SN/2}\Gamma(1-s)^{N/2} \prod_{\chi\in X} L(1-s,\overline{\chi}). \tag{2.4}$$

Dividint l'equació (2.3) per (2.4), aplicant la definició de A i eliminant termes comuns obtenim finalment:

$$\frac{\pi^{-Ns/2}|d(K)|^{s/2}}{\left(\frac{f_\chi}{\pi}\right)^{Ns/2}} = \frac{\pi^{-N(1-s)/2}|d(K)|^{(1-s)/2}}{\left(\frac{f_\chi}{\pi}\right)^{N(1-s)/2}\prod_{\chi\in X} W_\chi}$$

$$|d(K)| = \prod_{\chi\in X} f_\chi.$$

□

Directament del teorema obtenim el següent corol·lari:

Corołari 2.22.

$$\prod_{\chi\in X} \tau(\chi) = \begin{cases} \sqrt{|d(K)|} & \textit{si } K \textit{ és totalment real} \\ i^{[K:\mathbb{Q}]/2}\sqrt{|d(K)|} & \textit{Si } K \textit{ és complex} \end{cases}$$

3 Funció $L(s,\chi)$

L'objectiu d'aquest capítol és calcular el valor de $L(1,\chi)$ quan χ és parell. El primer que veiem és quan s'anul·la la funció $L(s,\chi)$ depenent de la paritat del caràcter de Dirichlet. Després definim els nombres de Bernoulli i les seves variants, i les relacionem entre elles. També en veiem les seves propietats principals. Aquesta primera secció serà perquè donarem el valor de $L(1,\chi)$ en funció dels nombres de Bernoulli.

Comencem doncs veient quan s'anul·la la funció $L(s,\chi)$ en els enters negatius depenent de la paritat de χ.

Proposició 3.1. *Sigui $n\in\mathbb{Z}$ tal que $n\geq 1$. Aleshores tenim que:*

(1) $L(1-n,\chi)\neq 0$ *si n i χ tenen paritats diferents.*

(2) $L(1-n,\chi)=0$ *si n i χ tenen la mateixa paritat.*

Demostració. Reescrivim l'equació funcional de la funció L de la següent manera

$$\Gamma(s)\cos\left(\frac{\pi(s-\delta)}{2}\right)L(s,\chi) = \frac{\tau(\chi)}{2i^\delta}\left(\frac{2\pi}{f_\chi}\right)^s L(1-s,\bar{\chi})$$

Sigui χ parell. Aleshores $\chi(-1)=\chi(1)$ i $\delta=0$. Per tant el cosinus s'anul·la en n senar. En conclusió, $L(1-n,\chi)=0$ si n és senar i $L(1-n,\chi)\neq 0$ si n és parell.

Sigui ara χ senar. Aleshores $\chi(-1)=(-1)\chi(1)$ i $\delta=1$. Per tant el cosinus s'anul·la en n parell. En conclusió, $L(1-n,\chi)=0$ si n és parell i $L(1-n,\chi)\neq 0$ si n és senar. □

3.1 Nombres de Bernoulli

Comencem la secció definint els nombres de Bernoulli i veient les relacions entre ells. També definim els polinomis de Bernoulli i trobem les seves relacions amb els nombres de Bernoulli.

Definició 3.2 (Nombres de Bernoulli)**.** *Els nombres de Bernoulli són els termes B_n de la següent sèrie*

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

A més, els nombres de Bernoulli generalitzats són els termes $B_{n,\chi}$ de la següent sèrie

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

On f_χ és el conductor del caràcter de Dirichlet χ.

Observació 3.3. Sigui χ un caràcter de Dirichlet no principal. Aleshores

$$B_{0,\chi}=0.$$

Demostració. Es deu al fet que $\sum_{a=1}^{f_\chi}\chi(a)=0$. □

Els nombres de Bernoulli i els nombres de Bernoulli generalitzats estan relacionats de la següent manera.

Proposició 3.4. *Sigui $\chi=1$ el caràcter principal. Aleshores tenim que $B_{n,1}=B_n$ per $n\neq 1$, ja que per $n=1$, $B_{1,1}=\frac{1}{2}$ i $B_1=-\frac{1}{2}$.*

Els nombres de Dirichlet generalitzats es comporten diferent depenent de si χ es parell o senar. Això en porta a pensar que podran estar relacionats amb els valors de la funció $L(s,\chi)$ d'alguna manera.

Proposició 3.5. *Sigui $n>1$. Si χ és un caràcter de Dirichlet senar, aleshores*

$$B_{n,\chi}=0 \quad \textit{si } n \textit{ és parell.}$$

Altrament, si χ és un caràcter de Dirichlet parell, aleshores

$$B_{n,\chi}=0 \quad \textit{si } n \textit{ és senar.}$$

Demostració. Demostrem el primer cas i l'altre es veu anàlogament. De la definició dels nombres de Bernoulli generalitzats, denotem per $F_\chi(t)$ a

$$F_\chi(t)=\sum_{a=1}^{f_\chi}\frac{\chi(a)te^{at}}{e^{f_\chi t}-1}.$$

El que volem veure ara és que la funció F_χ és una funció senar quan χ és senar (anàlogament serà parella si χ és parell). Per fer-ho multipliquem i dividim $F_\chi(-t)$ per $-e^{f_\chi t}$ i obtenim:

$$F_\chi(-t)=\sum_{a=1}^{f_\chi}\frac{\chi(a)(-t)e^{-at}}{e^{-f_\chi t}-1}\cdot\frac{-(e^{f_\chi t})}{-(e^{f_\chi t})}=\sum_{a=1}^{f_\chi}\frac{\chi(a)te^{(f_\chi-a)t}}{e^{tf_\chi}-1}.$$

Com que χ és un caràcter de Dirichlet de conductor f_χ, podem aplicar que $\chi(a) = \chi(-1)\chi(f_\chi - a)$, i ens queda el següent:

$$\sum_{a=1}^{f_\chi} \frac{\chi(a)te^{(f_\chi-a)t}}{e^{f_\chi t}-1} = \sum_{a=1}^{f_\chi} \frac{\chi(-1)\chi(f_\chi-a)te^{(f_\chi-a)t}}{e^{f_\chi t}-1} = \chi(-1)F_\chi(t) = -F_\chi(t).$$

Hem vist doncs que $F_\chi(t)$ és una funció senar respecte t. Finalment aplicant la definició dels nombres de Bernoulli generalitzats obtenim

$$F_\chi(-t) = -F_\chi(t) \Rightarrow \sum_{n=0}^{\infty} B_{n,\chi}\frac{(-t)^n}{n!} = -\sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!} \Rightarrow \begin{cases} B_{n,\chi} = -B_{n,\chi} & \text{si } n \text{ és parell} \\ B_{n,\chi} = B_{n,\chi} & \text{si } n \text{ és senar} \end{cases}.$$

Per tant per χ senar $B_{n,\chi} = 0$ si n és parell. Anàlogament es veu que per χ parell $B_{n,\chi} = 0$ si n és senar. □

Per finalitzar la secció, definim els polinomis de Bernoulli i els relacionem amb els nombres de Bernoulli i també amb els nombres de Bernoulli generalitzats.

Definició 3.6 (Polinomis de Bernoulli)**.** *Els polinomis de Bernoulli $B_n(X)$ són els coeficients de la següent sèrie*

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

on $e^{Xt} = \sum_{n\geq 1} x^n \frac{t^n}{n!}$

Observació 3.7. Els polinomis de Bernoulli compleixen $B_n(1-X) = (-1)^n B_n(X)$.

Demostració. Amb un procediment similar al de la demostració anterior es veu aquesta propietat. □

Per començar amb les relacions entre nombres i polinomis de Bernoulli, relacionem els polinomis de Bernoulli amb els nombres de Bernoulli.

Proposició 3.8.

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

Demostració. Per la definició dels polinomis de Bernoulli tenim que:

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

Traient factor comú i aplicant les definicions dels nombres de Bernoulli i de l'exponencial següents:

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

obtenim:

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

Finalment unint els sumatoris:

$$\sum_{n=1}^{\infty}\sum_{i=0}^{n}\binom{n}{i}B_i X^{n-i}\frac{t^n}{n!}.$$

Per tant obtenim la igualtat desitjada. □

Ara anem a relacionar els polinomis de Bernoulli amb els nombres de Bernoulli generalitzats.

Proposició 3.9. *Sigui F un múltiple qualsevol de f_χ. Aleshores*

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

Demostració. Per veure la igualtat, comencem per la definició dels nombres de Bernoulli generalitzats i els substituïm per l'enunciat. Aleshores operant volem arribar a veure que són iguals.

$$\sum_{n=0}^{\infty}F^{n-1}\sum_{a=1}^{F}\chi(a)B_n\left(\frac{a}{F}\right)\frac{t^n}{n!} = \sum_{a=1}^{F}\chi(a)\frac{te^{(a/F)Ft}}{e^{Ft}-1}.$$

Sigui $g = F/f_\chi$ i $a = b + cf_\chi$. Per tant ens queda

$$\sum_{b=1}^{f_\chi}\sum_{c=0}^{g-1}\chi(b)\frac{te^{(b+cf_\chi)t}}{e^{f_\chi gt}-1} = \sum_{b=1}^{f_\chi}\chi(b)\frac{te^{bt}}{e^{f_\chi t}-1} = \sum_{n=0}^{\infty}B_{n,\chi}\frac{t^n}{n!}.$$

□

Observació 3.10. En el cas $n = 1$, com tenim que $B_1(X) = X - \frac{1}{2}$, si χ no principal, observem que

$$B_{1,\chi} = \frac{1}{f_\chi}\sum_{a=1}^{f_\chi}\chi(a)a.$$

3.2 $L(s,\chi)$ avaluada en $s = 1$

Per trobar el valor de $L(1,\chi)$ en funció dels nombres de Bernoulli, avaluem primer la funció L en $s = n-1$ i després mitjançant l'equació funcional de la funció L trobem el resultat. Primer de tot trobem el valor de $Ł(s,\chi)$ en els enters negatius en funció dels nombres de Bernoulli generalitzats.

Teorema 3.11. *$L(1-n,\chi) = -B_{n,\chi}/n$, per $n \geq 1$.*

Demostració. Sigui $F_\chi(z)$ la següent funció meromorfa.

$$F_\chi(z) = \sum_{a=1}^{f_\chi}\frac{\chi(a)ze^{az}}{e^{f_\chi z}-1}.$$

Aleshores considerem $F_\chi(z)z^{-n-1}$. Aquesta nova funció té un pol a $z = 0$ per tot $n \geq 1$ amb residu

$$-\frac{L(1-n,\chi)}{\Gamma(n)}.$$

Per un argument sobre aquest resultat, veure [4][Apèndix]. Seguint amb la demostració, obtenim que:

$$F_\chi(z) = \sum_{a=1}^{f_\chi} \frac{\chi(a) z e^{az}}{e^{f_\chi z} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{z^n}{n!}.$$

I per tant ja queda demostrada la fórmula. □

Ja podem demostrar la següent fórmula,, que ens dona el valor de la funció L en $s = 1$ per un caràcter de Dirichlet senar.

Teorema 3.12. *Sigui χ un caràcter de Dirichlet senar, aleshores*

$$L(1, \chi) = \pi i \frac{\tau(\chi)}{f_\chi} B_{1,\bar{\chi}},$$

on $B_{1,\chi}$ és un nombre de Bernoulli generalitzat i $\tau(\chi)$ és una suma de Gauss.

Demostració. Sigui χ un caràcter de Dirichlet senar. Avaluem en $s = 1$ l'equació funcional de L, vista en 2.20 i substituïm δ per 1, doncs χ és senar.

$$\begin{aligned}
\left(\frac{f_\chi}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi) &= W_\chi \left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\overline{\chi}),\\
\left(\frac{f_\chi}{\pi}\right)^{1/2} \Gamma\left(\frac{1+1}{2}\right) L(1,\chi) &= \frac{\tau(\chi)}{\sqrt{f_\chi} i^1} \left(\frac{f_\chi}{\pi}\right)^{(1-1)/2} \Gamma\left(\frac{1-1+1}{2}\right) L(1-1,\overline{\chi}),\\
\left(\frac{f_\chi}{\pi}\right)^{1/2} 1 L(1,\chi) &= \frac{\tau(\chi)}{\sqrt{f_\chi} i} \sqrt{\pi} L(0,\overline{\chi}),\\
L(1,\chi) &= \frac{\tau(\chi)\pi}{f_\chi i} L(0,\overline{\chi}),\\
L(1,\chi) &= -\pi i \frac{\tau(\chi)}{f_\chi} L(0,\overline{\chi}).
\end{aligned}$$

Ara, pel 3.11 agafant $n = 1$, tenim

$$L(1,\chi) = -\pi i \frac{\tau(\chi)}{f_\chi} \left(-\frac{B_{1,\bar{\chi}}}{1}\right) = \pi i \frac{\tau(\chi)}{f_\chi} B_{1,\bar{\chi}}.$$

□

Finalment comentem el que val la funció $L(s,\chi)$ en $s = 1$ quan χ és un caràcter parell. No usarem aquest resultat, per tant tampoc el demostrem. Per una prova, veure [1, Pàgina 37]

Observació 3.13. Si χ un caràcter de Dirichlet parell, tenim que

$$L(1,\chi) = -\frac{\tau(\chi)}{f_\chi} \sum_{a=1}^{f_\chi} \bar{\chi}(a) \log|1 - \zeta_{f_\chi}^a|.$$

4 Fórmula del nombre de classes

L'objectiu d'aquest capítol és trobar una fórmula per a calcular el nombre de classes relatiu d'un cos CM. En la primera secció definim que és un cos CM i definim que és el nombre de classes relatiu d'un cos. En la segona secció definim la noció de regulador d'un cos, demostrem un resultats previs i finalment demostrem la fórmula del nombre de classes.

4.1 Nombre de classes relatiu

Com hem dit, en aquesta secció volem definir el nombre relatiu de classes. Aquest resultarà de la divisió del nombre de classes d'un cos CM entre el nombre de classes del seu cos totalment real maximal. El resultat important d'aquesta secció serà veure que aquesta és una divisió que dona un enter. També veurem que els cossos protagonistes ($\mathbb{Q}(\zeta_p$ i $\mathbb{Q}(\zeta_p^{-1}))$) compleixen aquestes condicions. Comencem doncs amb la secció definit cos totalment real i cos CM.

Definició 4.1 (Cos totalment real)**.** *Un cos de nombres F es totalment real si totes les immersions de F en els complexos són reals. És a dir, si σ és una immersió de F en $\mathbb{C}$, aleshores $\sigma(F) \subseteq \mathbb{R}$.*

Observació 4.2. Comprovem que $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ és totalment real. Sigui σ una immersió de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ a $\mathbb{C}$. Aleshores

$$\zeta_n + \zeta_n^{-1} = e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}} \overset{\sigma}{\longmapsto} e^{\frac{2\pi i}{n}j} + e^{-\frac{2\pi i}{n}j}, \qquad j \in \mathbb{N}.$$

La j ve definida per la σ. Ara bé, per tot j tenim que $e^{\frac{2\pi i}{n}j} + e^{-\frac{2\pi i}{n}j} \in \mathbb{R}$, per tant $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ és totalment real.

Per a la definició de cos CM, primer necessitem definir què és un cos totalment imaginari.

Definició 4.3 (Cos totalment imaginari)**.** *Un cos de nombres F és totalment imaginari si totes les immersions de F en els complexos són no reals. És a dir, si σ és una immersió de F en $\mathbb{C}$, aleshores $\sigma(F) \not\subseteq \mathbb{R}$.*

Exemple 4.4. Comprovem que $\mathbb{Q}(\zeta_n)$ és totalment imaginari. Sigui σ una immersió de $\mathbb{Q}(\zeta_n)$ a $\mathbb{C}$. Aleshores

$$\zeta_p = e^{\frac{2\pi i}{n}} \overset{\sigma}{\longmapsto} e^{\frac{2\pi i}{n}j} = \zeta_n^j, \qquad j = 1, \ldots, \phi(n).$$

Com p és un primer senar, tenim que $\zeta_p^j \notin \mathbb{R}$ per $j = 1, \ldots, p-1$. Per tant, $\mathbb{Q}(\zeta_p)$ és un cos totalment imaginari.

Definició 4.5 (Cos CM)**.** *Un cos de nombres F és un cos CM si és una extensió quadràtica d'un cos totalment real i F és totalment imaginari.*

Proposició 4.6. *L'extensió $\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ té grau 2.*

Demostració. Comencem observant que $\mathbb{Q}(\zeta_n) \not\subseteq \mathbb{R}$ i que $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{R}$. Aleshores com a mínim serà una extensió de grau 2. Com $x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ és irreductible en $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, té grau 2 i és reductible en $\mathbb{Q}(\zeta_n)$ doncs $x^2 - (\zeta_n + \zeta_n^{-1})x + 1 = (x - \zeta_n)(x - \zeta_n^{-1})$, ja ho tenim. □

Observació 4.7. $\mathbb{Q}(\zeta_n)$ és un cos CM.

Ja hem definit els conceptes necessaris i hem vist que en el cas que estem treballant es compleixen les mateixes condicions. Ara veiem el següent teorema, que ens dirà que els respectius nombres de classes es poden dividir.

Teorema 4.8. *Siguin K un cos CM, K^+ el seu subcòs real maximal i siguin h i h^+ els nombres de classes respectivament. Aleshores h^+ divideix h.*

Demostració. Necessitem el següent lema:

Lema 4.9. *Sigui K/L una extensió de cossos de nombres tal que no hi ha cap subextensió no trivial no ramificada F/L amb* $\mathrm{Gal}(F/L)$ *abelià. Aleshores el nombre de classes de L divideix el nombre de classes de K.*

Demostració. Siguin K i L cossos de nombres com a la hipòtesi. Sigui H l'extensió maximal no ramificada i abeliana de L. Per teoria de classes, el grup $\mathrm{Gal}(H/L)$ és isomorf al grup de classes d'ideals de L, és a dir $\mathcal{O}_L$. Per una demostració, veure [2][Teorema 2.2]. Com hem suposat K/L, aleshores $H \bigcap K = L$. Per tant $[KH : K] = [H : L]$. Ara, com KH/K és abelià i no ramificat, està contingut en l'extensió abeliana maximal no ramificada de K. En conclusió, el nombre de classes de $L = [H : L] = [KH : K]$ divideix el nombre de classes de K. □

Seguim amb la demostració del teorema. Com l'extenció K/K^+ és totalment ramificada en els primers arquimedians, no existeix cap subcòs F de K no trivial i no ramificat tal que $\mathrm{Gal}(F/L)$ sigui abelià. Per tant podem aplicar la proposició i hem demostrat que $h^+|h$. □

Aquest era un fet que en principi no tenia per a què ser cert. Per tant ara que sabem que $h/h^+ \in \mathbb{Z}$, podem donar-li un nom, que serà nombre de classes relatiu.

Definició 4.10 (Nombre de classes relatiu)**.** *Siguin K un cos CM i K^+ el seu subcós real maximal. Siguin h i h^+ els nombres de classes de K i K^+ respectivament. Aleshores definim el nombre de classes relatiu $h^- = h/h^+$.*

4.2 Fórmula del nombre de classes

La fórmula del nombre de classes serà una fórmula per h^-. Per veure-la comencem definint la $\mathcal{Q}$. $\mathcal{Q}$ pren valors diferents depenent del cos CM sobre el qual treballem. Per acabar, donarem una fórmula per al nombre de classes relatiu, anomenada fórmula del nombre de classes.

Teorema 4.11. *Sigui K un cos CM i E el seu grup d'unitats. Sigui E^+ el grup d'unitats de K^+ i sigui W el grup d'arrels de la unitat en K.*

$$[E : WE^+] = 1 \ o \ 2.$$

Anomenarem $\mathcal{Q} = [E : WE^+]$.

Demostració. Sigui $\phi : E \to W$ tal que $\phi(\epsilon) = \epsilon/\bar{\epsilon}$, amb ϵ una unitat de K. Veiem primer que ϕ està ben definida.

Com K és CM, tenim que $\overline{\epsilon^\sigma} = \bar{\epsilon}^\sigma$. Per tant $|\phi(\epsilon)^\sigma| = |(\epsilon/\bar{\epsilon})^\sigma| = |\epsilon^\sigma|/|\overline{\epsilon^\sigma}| = 1/1 = 1$ per tot immersió σ. Aleshores hem vist que $\phi(\epsilon)$ és una arrel de la unitat de K, per tant $\phi(\epsilon) \in W$ i la funció ϕ està ben definida.

Sigui ara $\psi : E \to W/W^2$ la funció induïda per ϕ que envia ζ^2 a 1. Tenim 2 casos. El primer cas és $\epsilon = \zeta\epsilon_1$ amb $\zeta \in W$ i $\epsilon_1 \in E^+$ i el segon cas és $\epsilon = \zeta^2 \in W^2$. Si tenim el primer cas, aleshores

$$\phi(\epsilon) = \frac{\epsilon}{\bar{\epsilon}} = \frac{\zeta\epsilon_1}{\overline{\zeta\epsilon_1}} = \frac{\zeta\epsilon_1}{\zeta^{-1}\epsilon_1} = \frac{\zeta}{\zeta^{-1}} = \zeta^2.$$

I per tant $\epsilon \in \mathrm{Ker}(\psi)$. Aleshores $\phi(E) = W^2$ i $\mathcal{Q} = 1$.

En el segon cas tenim que

$$\epsilon/\bar{\epsilon} = \zeta^2 \to \epsilon\zeta^{-1} = \bar{\epsilon}\zeta \to \overline{\epsilon\zeta^{-1}} = \overline{\bar{\epsilon}\zeta} \to \bar{\epsilon}\zeta = \epsilon\zeta^{-1}.$$

Per tant $\epsilon\zeta^{-1}$ és real i és una unitat de E^+. Aleshores $\mathrm{Ker}(\psi) = WE^+$. Per tant el nucli de ψ té grau WE^+. I com $[W : W^2] = 2$, hem vist que si $\phi(E) = W$ aleshores $\mathcal{Q} = 1$. □

Finalment trobem el valor per $\mathcal{Q}$ quan $K = \mathbb{Q}(\zeta_p)$. Aquest valor serà important en la demostració de la fórmula del nombre de classes.

Corołari 4.12. *Sigui $K = \mathbb{Q}(\zeta_p)$ amb $p > 2$. Aleshores $\mathcal{Q} = 1$.*

Demostració. Veurem que $\phi(E) = W^2$. Primer demostrem que $\phi(E) \subseteq W^2$. Sigui $\epsilon \in E$, aleshores $\epsilon = \zeta_p^k$, per alguna $k = 0, 1, \ldots, p-1$ o $\epsilon = -1$, ja que el grup d'unitats de $\mathbb{Q}(\zeta_p)$ és $E = \mathbb{Z}[\zeta_p]^\times$. Si $\epsilon = -1$, $\phi(-1) = 1 \in W^2$. Ara, si $\epsilon = \zeta_p^k$ llavors:

$$\phi(\epsilon) = \frac{\epsilon}{\bar{\epsilon}} = \frac{\zeta_p^k}{\zeta_p^{-k}} = \zeta_p^{2k} \in W^2.$$

Veiem ara que $W^2 \subseteq \phi(E)$. Sigui ζ_p^{2k} un element qualsevol de W^2. Aleshores:

$$\zeta_p^{2k} = \frac{\zeta_p^k}{\zeta_p^{-k}} \in \phi(E).$$

Per tant com $\phi(E) = W^2$, tenim que $\mathcal{Q} = 1$. □

Es pot veure també que $\mathcal{Q} = 1$ si $K = \mathbb{Q}(\zeta_n)$ amb n una potència d'un nombre primer. Altrament si $K = \mathbb{Q}(\zeta_n)$ i n no és una potència d'un primer, aleshores $\mathcal{Q} = 2$.

Ara definim el regulador, l'últim concepte que ens falta per presentar la Fórmula del nombre de classes.

Definició 4.13 (Regulador)**.** *Siguin K un cos de nombres, $r = r_1 + r_2 - 1$ i $\epsilon_1, \ldots, \epsilon_r$ un conjunt d'unitats independents de K. Siguin $\sigma_1, \ldots, \sigma_{r_1}$ les immersions reals de K a $\mathbb{C}$ i siguin $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}} \ldots, \sigma_{r_1+r_2} = \sigma_{r+1}, \overline{\sigma_{r+1}}$ les immersions complexes no reals de L a $\mathbb{C}$. Aleshores sigui $\delta_j = 1$ si σ_j és real i $\delta_j = 2$ si σ_j és no real. Finalment definim el regulador de K associat a $\epsilon_1, \ldots, \epsilon_r$ com*

$$R_K(\epsilon_1, \ldots, \epsilon_r) = \left| \det(\delta_i \log |\sigma_i(\epsilon_j)|)_{1 \le i,j \le r} \right|.$$

Si $\epsilon_1, \ldots, \epsilon_r$ és una base pel grup d'unitats de K mòdul arrels de la unitat, aleshores anomenem a $R_K(\epsilon_1, \ldots, \epsilon_r) = R_K$ el regulador de K.

Tenim $r+1$ immersions però hem definit el regulador amb un determinant $r \times r$. Per tant hem de no usar una de les immersions. Agafem el valor absolut del determinant perquè així no sigui rellevant quina columna obviem. Ara anem a relacionar els valors dels reguladors d'un cos CM K i del seu cos real maximal K^+.

Proposició 4.14. *Sigui K un cos CM i K^+ el seu màxim subcòs totalment real. Siguin $\epsilon_1, \ldots, \epsilon_r$ una base de les unitats de K^+ mòdul ± 1. Aleshores*

$$R_K(\epsilon_1, \ldots, \epsilon_r) = 2^r R_{K^+}.$$

Demostració. Sigui $\epsilon_1, \ldots, \epsilon_r$ una base de K^+ mòdul ± 1. Aleshores $\epsilon_1, \ldots, \epsilon_r$ forma una base per a un subgrup d'índex $\mathcal{Q}$ en les unitats de K mòdul arrels de la unitat. Recordem que $\mathcal{Q} = 1$ o 2 depenent de K. Nogensmenys cada $\delta_i = 1$ en K^+ i cada $\delta_i = 2$ en K. Per tant

$$R_K(\epsilon_1, \ldots, \epsilon_r) = 2^r R_{K^+}(\epsilon_1, \ldots, \epsilon_r) = 2^r R_{K^+}.$$

□

Hem vist una relació entre el regulador de K i el de K^+ amb unes bases específiques. Volem relacionar els reguladors de K i K^+ independentment de les bases. La relació ve donada pel següent teorema:

Teorema 4.15. *Sigui K un cos CM i K^+ el seu subcòs real. Aleshores*

$$\frac{R_K}{R_{K^+}} = \frac{2^r}{Q},$$

on $r = \frac{1}{2}[K : \mathbb{Q}] - 1$.

Demostració. Necessitem el següent lema.

Lema 4.16. *Siguin $\epsilon_1, \ldots, \epsilon_r$ unitats independents d'un cos de nombres K tal que generen un subgrup A d'unitats de K mòdul arrels de la unitat. Siguin $\eta_1, \ldots, \eta_r$ generadors d'un subgrup B. Si $A \subseteq B$ i l'extensió B/A té grau finit, aleshores*

$$[B : A] = \frac{R_K(\epsilon_1, \ldots, \epsilon_r)}{R_K(\eta_1, \ldots, \eta_r)}.$$

Demostració. Com $\epsilon_1, \ldots, \epsilon_r$ generen A, $\eta_1, \ldots, \eta_r$ generen B i $A \subseteq B$, podem escriure les unitats ϵ_i en funció dels generadors de B de la següent forma.

$$\epsilon_i = \left(\prod_k \eta_k^{a_{i,k}} \right) \cdot \zeta,$$

on ζ és una arrel de la unitat i $a_{i,k} \in \mathbb{Z}$. Volem ara arribar a l'expressió del regulador, per tant modifiquem la igualtat aplicant logaritmes, aplicant una immersió σ_j i multiplicant pel seu δ_j associat. En conclusió, acabem obtenint

$$\delta_j \log |\epsilon_i^{\sigma_j}| = \sum_k a_{i,k} \delta_j \log |\eta_k^{\sigma_j}|.$$

D'aquesta igualtat, en deduïm que

$$\frac{R_K(\epsilon_1, \ldots, \epsilon_r)}{R_K(\eta_1, \ldots, \eta_r)} = |\det(a_{i,k})|.$$

Per una banda, sabem que existeixen dues matrius ortogonals M i N tal que $M(a_{i,k})N = D$, amb D una matriu diagonal tal que $D = \mathrm{diag}(d_1, \ldots, d_r)$. Per tant deduïm que $\det(a_{i,k}) = \pm \prod_i d_i$. D'altra banda, podem interpretar les matrius M i N com a canvi de base de A i de B respectivament, per tant tenim dues bases $x_1, \ldots, x_r$ i $y_1, \ldots, y_r$ de A i B respectivament tal que $x_i = d_i y_i$. Aleshores $B/A = \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}$ i finalment $[B : A] = |\prod_i d_i|$. □

Pel lema, obtenim que $R_K(\epsilon_1, \ldots, \epsilon_r) = \mathcal{Q}R_K$, seguint amb la notació del lema. Unint-ho amb el resultat de 4.14 queda demostrat el teorema. □

Teorema 4.17 (Fórmula del nombre de classes)**.** *Sigui K un cos CM i X el grup de caràcters de Dirichlet associat a K. Sigui w el nombre de arrels de la unitat en K. Aleshores el nombre relatiu de classes compleix la següent fórmula:*

$$h^-(K) = \mathcal{Q}w \prod_{\chi senar} (-\frac{1}{2}B_{1,\chi}). \tag{4.1}$$

Demostració. Per aquesta demostració, donarem per conegut que la funció ζ_K té un pol simple a $s = 1$ amb residu

$$\frac{2^{r_1}(2\pi)^{r_2}h(K)R_K}{w\sqrt{|d(K)|}}.$$

Així doncs, per 2.18 i usant que $\zeta(s)$ té un pol simple a $s = 1$ de residu 1, obtindrem

$$\frac{\prod_{\chi\in X} L(1,\chi)}{\zeta(s)} = \prod_{\substack{\chi\in X \\ \chi \text{ no principal}}} L(1,\chi) = \frac{2^{r_1}(2\pi)^{r_2}h(K)R_K}{w\sqrt{|d(K)|}}.$$

Aleshores com K és CM, si $[K : Q] = n$, sabem que $r_1 = 0$ i $n_2 = n/2$. Ens queda aleshores que

$$\prod_{\substack{\chi\in X \\ \chi \text{ no principal}}} L(1,\chi) = \frac{(2\pi)^{n/2}h(K)R_K}{w\sqrt{|d(K)|}}.$$

Raonant anàlogament per K^+, obtenim la següent equació funcional:

$$\prod_{\substack{\chi\in X \\ \chi \text{ parell} \\ \chi \text{ no principal}}} L(1,\chi) = \frac{2^{n/2}h(K^+)R_{K^+}}{2\sqrt{|d(K^+)|}}.$$

Dividint, aplicant 4.15 i simplificant termes:

$$\begin{aligned}\prod_{\substack{\chi\in X \\ \chi \text{ senar}}} L(1,\chi) &= \frac{2\pi^{n/2}h(K)R_K}{wh(K^+)R_{K^+}\sqrt{|d(K)|/|d(K^+)|}}, \\ &= \frac{\pi^{n/2}h^-(K)2^{r+1}}{w\mathcal{Q}\sqrt{|d(K)|/|d(K^+)|}}, \\ &= \frac{\pi^{n/2}h^-(K)2^{n/2}}{w\mathcal{Q}\sqrt{|d(K)|/|d(K^+)|}}.\end{aligned}$$

Ja que $r = \frac{1}{2}[K : \mathbb{Q}] - 1 = n/2 - 1$. Ara llistem els resultats principals que usem per la demostració:

(1) Com tots els caràcters són senars, per 3.12 obtenim que $L(1,\chi) = \pi i \frac{\tau(\chi)}{f_\chi} B_{1,\overline{\chi}}$.

(2) Per la fórmula del Conductor-Discriminant 2.19, $\sqrt{|d(K)/d(K^+)|} = \left(\prod_{\chi \text{ senar}} f_\chi \right)^{1/2}$.

(3) Per 2.22, $\prod_{\chi \text{ senar}} \tau(\chi) = i^{n/2} \sqrt{|d(K)/d(K^+)|}$.

(4) Si χ és un caràcter de Dirichlet senar, aleshores $\overline{\chi}$ també ho és. Per veure-ho és suficient suposar que $\overline{\chi}$ és parell i aleshores

$$1 = \chi(1)\overline{\chi(1)} = -\chi(-1)\overline{\chi(-1)} = -1.$$

Per tant $\overline{\chi}$ també és senar.

Comencem substituint la funció L per (1):

$$\prod_{\substack{\chi \in X \\ \chi \text{ senar}}} L(1,\chi) = \frac{\pi^{n/2} h^-(K) 2^{n/2}}{w\mathcal{Q}\sqrt{|d(K)|/|d(K^+)|}},$$

$$\prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \pi i \frac{\tau(\chi)}{f_\chi} B_{1,\overline{\chi}} = \frac{\pi^{n/2} h^-(K) 2^{n/2}}{w\mathcal{Q} \prod_{\chi \text{ senar}} f_\chi^1/2}.$$

Ara separant en diversos productoris, aplicant (2), (3) i (4), i eliminant termes comuns:

$$i^{n/2}\pi^{n/2} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \tau(\chi) \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \frac{1}{f_\chi} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} B_{1,\overline{\chi}} = \frac{\pi^{n/2} h^-(K) 2^{n/2}}{w\mathcal{Q} \prod_{\chi \text{ senar}} f_\chi^{1/2}},$$

$$i^n \sqrt{|d(K)/d(K^+)|} \frac{1}{2^{n/2}} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \frac{1}{f_\chi} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} B_{1,\chi} = \frac{h^-(K)}{w\mathcal{Q} \prod_{\chi \text{ senar}} f_\chi^{1/2}}.$$

Finalment, aplicant (2), eliminant termes i entrant el $1/2^{n/2}$ dins el productori obtenim:

$$i^n \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} (f_\chi^{1/2}) \frac{1}{2^{n/2}} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \frac{1}{f_\chi} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} B_{1,\chi} = \frac{h^-(K)}{w\mathcal{Q} \prod_{\chi \text{ senar}} f_\chi^{1/2}},$$

$$i^n \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \frac{1}{2} B_{1,\chi} = \frac{h^-(K)}{w\mathcal{Q}},$$

$$h^-(K) = i^n w\mathcal{Q} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} \frac{1}{2} B_{1,\chi}.$$

Per acabar, podem entrar el i^n dins el productori. És clar que n és parell, ja que $n = 2r_2$. Aleshores si n és múltiple de 4, tenim que $i^n = 1$ i dins el productori també seria positiu. Altrament, si n no és múltiple de 4, queda que $i^n = -1$, i dins el productori tindrem $(-1)^{n/2} = -1$. Per tant hem demostrat que

$$h^-(K) = w\mathcal{Q} \prod_{\substack{\chi \in X \\ \chi \text{ senar}}} -\frac{1}{2} B_{1,\chi}.$$

□

5 Cossos p-àdics

A partir d'ara volem treballar en cossos p-àdics. Per tant dediquem aquest capítol a definir-los. Primer de tot necessitem la definició de valoració.

5.1 Valoracions

En aquesta secció definim què és una valoració, en donem alguna propietat bàsica i finalment definim la valoració p-àdica, que serà la que utilitzarem en la resta del treball.

Definició 5.1. *Sigui K un cos i G un grup abelià totalment ordenat per una relació d'ordre $\leq$. Anomenarem valoració a una aplicació $v : K^\times \to G$ tal que per tota parella d'elements $x, y \in K^\times$ tals que $x + y \neq 0$ compleixin*

(1) $v(xy) = v(x) + v(y)$.

(2) $v(x + y) \geq min(v(x), v(y))$.

Per a completar la definició per tots els elements de K, es diu que $v(0) = +\infty$. L'infinit compleix les regles habituals per l'infinit. A més, demanarem que la valoració sigui una funció exhaustiva, i aleshores es diu que v és una valoració de K del grup de valors G.

Anem ara a classificar dos diferents tipus de valoracions depenent de com és el grup imatge.

Definició 5.2. *Una valoració v s'anomena discreta quan el grup de valors $v(K^\times) = G$ és isomorf a $\mathbb{Z}$. Una valoració v s'anomena real quan el grup de valors és isomorf a un subgrup del grup additiu dels nombres reals.*

Proposició 5.3. *Sigui K un cos i $v : K \to G \bigcup +\infty$ una valoració de K. Aleshores el conjunt $A_v := x \in K | v(x) \geq 0$ és un subanell de K amb ideal maximal $\mathfrak{P}_v := x \in K | v(x) > 0$. A més, K és el cos de fraccions de A_v.*

Demostració. A_v és un subanell de K, doncs compleix les propietats de subanell. També és fàcil veure que $\mathfrak{P}_v$ és un ideal de A_v. Per veure que $\mathfrak{P}_v$ és el seu ideal maximal, veurem que $A_v \setminus \mathfrak{P}_v$ és el grup multiplicatiu dels elements invertibles de A_v. Sigui $x \in A_v$ un element invertible. Aleshores $v(x) + v(x^{-1}) = v(xx^{-1}) = v(1) = v(1) + v(1)$ i per tant $v(1) = 0$ i com les valoracions són positives, doncs són de A_v, tenim que $v(x) = v(x^{-1}) = 0$. Per tant $x \in A_v \setminus \mathfrak{P}_v$. Per veure l'altre inclusió, agafem $x \in A_v \setminus \mathfrak{P}_v$. Aleshores com $0 = v(1) = v(x) + v(x^{-1})$, obtenim $v(x^-1) = 0$ i per tant $x^{-1} \in A_v$ i x és invertible en A_v. Falta veure ara que efectivament K és el cos de fraccions de A_v. Per fer-ho suposem que $x \in K$ i $x \notin A_v$. Aleshores $v(x) < 0$ i per tant com $0 = v(1) = v(x) + v(x^{-1})$, obtenim que $v(x^{-1}) > 0$. En conclusió, $x^{-1} \in A_v$ i $x = 1/x^{-1} \in K$. □

Definició 5.4. *Anomenarem anell de valoració a A_v i ideal de valoració a $\mathfrak{P}_v$.*

Anem a veure ara l'exemple més important sobre valoracions. Es centra en definir la valoració p-àdica, una valoració discreta associada a un primer d'un anell de Dedekind. En els propers temes ens referirem majoritàriament a aquesta valoració, així que la descriurem amb detall.

Definició 5.5. *Sigui A un anell de Dedekind, K el seu cos de fraccions i $\mathfrak{p} \subseteq A$ un ideal primer no nul. Definirem la valoració $\mathfrak{p}$-àdica $v_\mathfrak{p}(x)$ per $x \in K$ com l'exponent de $\mathfrak{p}$ en la descomposició única com a producte d'ideals primers de xA.*

És clar que $v_\mathfrak{p}$ és una valoració. També observem que la imatge de $v_\mathfrak{p}$ és $\mathbb{Z}$, per tant serà una valoració discreta.

5.2 Complecions

En aquesta secció definirem els cossos $\mathbb{Z}_p, \mathbb{Q}_p$ i $\mathbb{C}_p$. La idea serà que adjudicant el valor absolut p-àdic a $\mathbb{Q}$, i modificant el mateix cos $\mathbb{Q}$ podrem definir $\mathbb{Q}_p$. A partir de $\mathbb{Q}_p$ serà senzill definir els altres.

Comencem doncs definint valor absolut. Diferenciarem entre valor absolut arquimedià i no arquimedià. Tot i que podríem estudiar moltes propietats de cada un i observar quins cossos surten de dotar cada un a un cos, en aquest treball ens centrarem només en els no arquimedians, doncs seran els que haurem de fer servir.

Definició 5.6. *Sigui K un cos. Un valor absolut de K és una aplicació $|| : K \to \mathbb{R}$ tal que $\forall x, y \in K$ tenim que:*

(1) $|x| \geq 0$ *i* $|x| = 0 \iff x = 0$.

(2) $|xy| = |x||y|$.

(3) $|x + y| \leq |x| + |y|$.

Definició 5.7 (Valor absolut no arquimedià)**.** *Sigui $|.|$ un valor absolut d'un cos K. Diem que $|.|$ és no arquimedià si compleix la desigualtat ultramètrica, és a dir:*

$$|x + y| \leq màx(|x|, |y|).$$

Definició 5.8. *Direm que dos valors absoluts de K $|.|_1, |.|_2$ són equivalents quan per tot $x \in K$ tenim que $|x|_1 < 1 \leftrightarrow |x|_2 < 1$.*

Definició 5.9. *Sigui $K/\mathbb{Q}$ una extensió de cossos de nombres. Sigui $\mathfrak{p} \subseteq \mathcal{O}_K$ i sigui $c \in \mathbb{R}$ qualsevol. Aleshores definim el valor absolut $\mathfrak{p}$-àdic associat a la valoració $\mathfrak{p}$-àdica com:*

$$|x|_\mathfrak{p} := p^{-v_\mathfrak{p}(x)}.$$

Proposició 5.10. *Sigui $K/\mathbb{Q}$ una extensió de cossos de nombres. Siguin $|.|_1$ i $|.|_2$ dos valors absoluts de K $\mathfrak{p}$-àdics donats per $|x|_1 := c_1^{-v_\mathfrak{p}(x)}$ i $|x|_2 := c_2^{-v_\mathfrak{p}(x)}$, amb $c_1, c_2 > 1$ reals. Aleshores $|.|_1$ i $|.|_2$ són equivalents.*

Demostració. Sigui x un element de K tal que $|x|_1 < 1$. Aleshores $c_1^{-v_\mathfrak{p}(x)} < 1$. Com $c_1 > 1$, tenim que $-v_\mathfrak{p}(x) < 0$. Per tant $c_2^{-v_\mathfrak{p}(x)} < 1$. L'altre cas és anàleg. □

Gràcies a aquesta proposició li donem sentit a l'elecció de p com a base per al valor absolut p-àdic. També es pot veure que a $\mathbb{Q}$ tot valor absolut no arquimedià és equivalent a un dels valors absoluts p-àdics amb p primer. Per una demostració veure [5][Teorema 9.3.2].

Ara ja hem definit valor absolut i hem escollit el que ens interessa per la compleció de $\mathbb{Q}$. El següent pas serà definir una distància en aquest valor absolut i escollir un cos que sigui complet per aquesta. Recordem que us cos és complet si tota successió de Cauchy és convergent.

Definició 5.11. *Sigui $|.|$ un valor absolut d'un cos K. Definim doncs la distància entre dos elements x, y associada a $|.|$ com $d(x,y) = |y - x|$.*

Definició 5.12 (Compleció)**.** *Sigui $(K, |.|_1)$ una parella on K és un cos i $|.|_1$ és un valor absolut de K. Aleshores definim a la parella $(L, |.|_2)$ com a compleció de $(K, |.|_1)$ si compleix les següents condicions:*

(1) L és un cos complet amb la distància associada al valor absolut $|.|_2$.

(2) L conté K com a subcòs i $|x|_2 = |x|_1$ per tot $x \in K$.

(3) K és dens en L.

(4) Si $(L_1, |.|_1^*)$ i $(L_2, |.|_2^*)$ són dos cossos que satisfan les propietats anteriors, aleshores existeix un isomorfisme de cossos $\phi : L_1 \to L_2$ que és la identitat sobre K i que $|\phi(x)|_2^* = |x|_1^*$.

Exemple 5.13. Anem a veure una compleció de $\mathbb{Q}$. Sigui p un primer de $\mathbb{Q}$ i $|.|_p$ el valor absolut p-àdic a $\mathbb{Q}$. Considerem l'anell $\mathcal{C}(\mathbb{Q})_p$ de les successions de Cauchy de racionals amb el valor absolut p-àdic. Sigui $\mathcal{I}_\prime(\mathbb{Q})_p$ l'ideal format per les successions que tenen límit 0. $\mathcal{I}_\prime(\mathbb{Q})_p$ és un ideal maximal de l'anell $\mathcal{C}(\mathbb{Q})_p$ i podem identificar $\mathbb{Q}$ amb un subcòs de $\mathcal{C}(\mathbb{Q})_p$ enviant cada element $x \in \mathbb{Q}$ a la successió constant de valor x. L'anell quocient $L = \mathcal{C}(\mathbb{Q})_p / \mathcal{I}_\prime(\mathbb{Q})_p$ és la compleció de $\mathbb{Q}$ amb el valor absolut p-àdic $|.|_p$. Per veure-ho bé hauríem de mirar que podem estendre el valor absolut de $\mathbb{Q}$ a L. Per fer-ho el definim de la següent manera: $|\{a_n\}_n| = \lim|a_n|$. És clar doncs que es compleixen les propietats (1) i (2), i es pot veure que amb aquesta construcció també es compleixen les propietats (3) i (4).

Denotem L = $\mathbb{Q}_p$. Denotem el seu aneu d'enters per $\mathbb{Z}_p$, és a dir, l'anell de la valoració p-àdica de $\mathbb{Q}_p$. Finalment, sigui $\overline{\mathbb{Q}}_p$ la clausura alegraica de $\mathbb{Q}_p$. Per dotar a $\overline{\mathbb{Q}}_p$ de valor absolut és suficient estendre el valor absolut de $\mathbb{Q}_p$ a $\overline{\mathbb{Q}}_p$. Es pot veure que ni $\mathbb{Q}_p$ ni $\overline{\mathbb{Q}}_p$ no són algebraicament tancats, i a més, $\overline{\mathbb{Q}}_p$ no és complet. Per tant podem definir la compleció de $\overline{\mathbb{Q}}_p$, i aquesta serà $\mathbb{C}_p$.

6 Funcions p-àdiques

6.1 Funcions p-àdiques per definició

Les funcions p-àdiques són funcions que estan definides d'un cos p-àdic fins a un altre cos p-àdic. Per exemple podem definir la funció exponencial p-àdica i la funció logarítmica p-àdica de la següent manera. En principi no demostrarem cap de les propietats que anunciem. Per veure demostracions veure [1][Secció §5.1]. Si no es diu el contrari, en aquesta secció estarem treballant en $\mathbb{C}_p$.

Definició 6.1 (Exponencial p-àdica)**.** *Definim la funció* $\exp_p : \mathbb{C}_p \to \mathbb{C}_p$ *tal que*

$$\exp_p(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

L'anomenarem exponencial p-àdica.

Proposició 6.2. *La funció exponencial p-àdica té radi de convergència* $p^{-\frac{1}{p-1}} < 1$.

Demostració. Per a la demostració necessitarem el següent lema:

Lema 6.3. *Sigui n tal que* $p^a \leq n < p^{a+1}$. *Aleshores*

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} < v_p(n!) < \frac{n}{p-1}.$$

Demostració. Veurem primer la primera desigualtat. Com n compleix que $p^a \leq n < p^{a+1}$, tenim que

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots,$$

ja que cada terme i conta els múltiples de p^i. Ara, aplicant que $[n/p] > n/p - 1$, obtenim

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots > \left(\frac{n}{p} - 1\right) + \left(\frac{n}{p^2} - 1\right) + \ldots = n\frac{1-p^{-a}}{p-1} - a.$$

Finalment per la restricció inicial de n, agafant logaritmes obtenim que $a < \log n / \log p$ i d'altre banda $np^{-a} < p$. Per tant

$$n\frac{1-p^{-a}}{p-1} - a > \frac{n-p}{p-1} - \frac{\log n}{\log p}.$$

Per l'altre desigualtat comencem de manera similar i observem que

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots \leq \frac{n}{p} + \frac{n}{p^2} + \ldots.$$

Ho tornem una sèrie harmònica sumant el terme inicial $i = 0$, que seria n i per tant ens queda

$$\frac{n}{p} + \frac{n}{p^2} + \ldots < n + \frac{n}{p} + \frac{n}{p^2} + \ldots = n\frac{1}{p-1}.$$

□

Anem a veure que la sèrie $\sum_n = 0^\infty \frac{X^n}{n!}$ té radi de convergència $p^{-\frac{1}{p-1}}$. La sèrie convergeix si el valor absolut del terme n-èssim tendeix a 0 quan n tendeix a infinit. Ara, el valor absolut del terme n-èssim és

$$\left|\frac{X^n}{n!}\right| = p^{-(nv_p(x) - v_p(n!))}.$$

Per tant tenim les següents equivalències

$$\left|\tfrac{X^n}{n!}\right| \xrightarrow[n\to+\infty]{} 0 \qquad \Longleftrightarrow \qquad nv_p(x) - v_p(n!) \xrightarrow[n\to+\infty]{} +\infty.$$

$$\left|\tfrac{X^n}{n!}\right| \xrightarrow[n\to+\infty]{} \infty \qquad \Longleftrightarrow \qquad -nv_p(x) + v_p(n!) \xrightarrow[n\to+\infty]{} +\infty.$$

Sigui $|x| < p^{-\frac{1}{p-1}}$. Aleshores tenim que $-v_p(x) < -\frac{1}{p-1}$ i per tant $v_p(x) > \frac{1}{p-1}$. Volem que es compleixi la primera equivalència, doncs volem veure que convergeix. Substituint per les desigualtats del lema obtenim que

$$nv_p(x) - v_p(n!) > nv_p(x) - \frac{n}{p-1} = (v_p(x) - \frac{1}{p-1})n \longrightarrow +\infty.$$

Ja que $(v_p(x) - \frac{1}{p-1}) > 0$.

D'altra banda, suposem que $|x| > p^{-\frac{1}{p-1}}$. Aleshores pel mateix raonament $v_p(x) < \frac{1}{p-1}$. Anàlogament al primer cas, obtenim

$$-nv_p(x)+v_p(n!) > -nv_p(x)+\frac{n}{p-1}-\frac{p}{p-1}-\frac{\log n}{\log p} = n\left(v_p(x)+\frac{1}{p-1}\right)-\frac{p}{p-1}-\frac{\log n}{\log p}.$$

Com $(v_p(x) + 1/(p-1)) > 0$, tenim que el resultat tendeix també a $+\infty$. □

A més, per a $|x|, |y| < p^{-\frac{1}{p-1}}$ compleix les següents propietats:

$$\exp(x+y) = \exp(x)\exp(y), \qquad \exp(-x) = \exp(x)^{-1}.$$

Definició 6.4 (Logaritme p-àdic)**.** *Definim la funció* $\log_p : \mathbb{C}_p \to \mathbb{C}_p$ *tal que*

$$\log_p(X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}X^n}{n}.$$

L'anomenarem logaritme p-àdic o funció logarítmica p-àdica.

La funció logaritme p-àdic té radi de convergència 1. A més per $|x|, |y| < 1$ compleix que:

$$\log_p(xy) = \log_p(x) + \log_p(y).$$

Es pot veure que existeix una extensió de $\log_p$ a $\mathbb{C}_p^\times$ tal que $\log_p(p) = 0$ i que $\log_p(xy) = \log_p(x) + \log_p(y)$ per tot $x, y \in \mathbb{C}_p^\times$.

Per a definir l'última funció p-àdica d'aquesta secció, necessitem introduir els símbols $<>$ com a operadors. Ho definim de la següent manera:

Definició 6.5. *Sigui* $\mathbb{Q}_p$ *amb p primer. Aleshores definim*

$$q = \begin{cases} p & \text{si } p \neq 2 \\ 4 & \text{si } p = 2 \end{cases}.$$

Sigui ara $a \in \mathbb{Z}_p$ *tal que* $p \nmid a$*. Aleshores existeix una única* $\phi(q)(= 2 \text{ o } p-1)$*-èssima arrel de la unitat* $\omega(a) \in \mathbb{Z}_p$ *tal que*

$$a \equiv \omega(a) \pmod{q}.$$

Finalment, definim l'operador $<>$ *de la següent manera*

$$<a>= \omega(a)^{-1}a.$$

Aleshores tenim que $<a> \equiv 1 \pmod{q}$, i per tant que $\log_p(<a>) = \log_p(a)$. També podem veure que com $a^{p-1} \equiv 1 \pmod{p}$, aleshores $\log_p(a) = \log_p(a^{p-1})/(p-1)$. Finalment, veiem una sèrie de propietats del logaritme p-àdic que sí que demostrem per donar-li sentit a la propera definició.

Proposició 6.6. *Si* $|x| < p^{-\frac{1}{p-1}}$*, aleshores* $|\log_p(1+x)| = |x|$*. Altrament, si* $|x| \leq p^{-\frac{1}{p-1}}$*, aleshores només podem assegurar que* $|\log_p(1+x)| \leq |x|$*.*

Demostració. Sigui $|x| < p^{-\frac{1}{p-1}}$. Primer de tot, usarem la desigualtat $|n| \geq 1/n$ per $n \geq 1$. És certa ja que $n|n| = np^{-v_p(n)} \geq 1$. Dit això, tenim els dos següents casos

$$\left|\frac{x^n}{n}\right| = |x|^{n-1} \cdot |x| < |x| \quad \text{si } 2 \leq n < p,$$
$$\left|\frac{x^n}{n}\right| < np^{\frac{1-n}{p-1}}|x| \leq |x| \quad \text{si } n \geq p.$$

On l'última desigualtat és certa ja que $np^{\frac{1-n}{p-1}}$ és decreixent per $n \geq p$ i val 1 per a $n = p$. Per tant el valor absolut del terme general de la sèrie de potències següent

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

És més petit o igual a $|x|$, el primer terme. Per tant el valor absolut de les sumes parcials és igual a $|x|$, doncs recordem que $||$ és un valor absolut no arquimedià i per tant compleix la desigualtat ultramètrica. Aleshores és una successió de Cauchy i com $\mathbb{C}_p$ és un espai complet és una sèrie convergent i per tant ha de convergir al valor del límit de les sumes parcials, que és $|x|$. Per tant $|\log_p(1+x)| = |x|$.

El segon cas es anàleg al primer intercanviant les desigualtats $<$ per $\leq$. □

Corołari 6.7. *Sigui* $|x| < p^{-\frac{1}{p-1}}$*. Aleshores es compleixen les següents igualtats.*

(1) $\log_p(\exp_p(x)) = x$*,*

(2) $\exp_p(\log_p(1+x)) = 1+x$*.*

Demostració. Per veure les dues hem de comprovar únicament que les sèries convergeixen. Per veure (1), només ens cal demostrar que $|\exp_p(x)| < 1$. Podem acotar el terme general de la seva sèrie per 1, doncs

$$v_p(n!) < \frac{n}{p-1} \to \left|\frac{x^n}{n!}\right| < 1, \text{ per } n \geq 1.$$

Per tant, també està ben definit el logaritme p-àdic i per tant $\log_p(\exp_p)(x)$ convergeix i clarament dona x. Per veure (2), usant la proposició anterior, obtenim que $|\log_p(1+x)| = |x| < p^{-\frac{1}{p-1}}$, per tant l'exponencial p-àdica està ben definida i $\exp_p(\log_p(1+x))$ convergeix i dona $1+x$. □

Definició 6.8. *Sigui* $a \in \mathbb{Z}_p$ *tal que* $p \not| a$*. Definim doncs la funció* $<a>^{\{.\}}: \mathbb{C}_p \to \mathbb{C}_p$ *de la següent manera.*

$$<a>^s = \exp(s \log_p <a>).$$

Té radi de convergència $qp^{\frac{-1}{p-1}}$, doncs $|\log_p(<a>)| \leq |q| = 1/q$. Igual que les funcions p-àdiques anteriors podem expressar $<a>^s$ en funció d'una sèrie de potències. Enunciem un resultat més general per a una funció p-àdica arbitrària i ho aplicarem posteriorment a la funció $<a>^s$.

Proposició 6.9. *Siguin* $r < p^{-\frac{1}{p-1}} < 1$ *i*

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n},$$

tal que $|a_n| \leq Mr^n$ *per algun* $M > 0$ *i* $\binom{X}{n}$ *segueix la definició natural*

$$\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}.$$

Aleshores $f(X)$ *pot ser expressada com una sèrie de potències amb radi de convergència* $R \geq (rp^{-1\frac{1}{p-1}})^{-1} > 1$.

Per veure quina sèrie de potències estaria adjudicada a la funció $< a >^s$, l'expandim de la següent manera:

$$< a >^s = (1 + < a > -1)^s = \sum_{n=0}^{\infty} \binom{s}{n} (< a > -1)^n.$$

Com $| < a > -1 \leq 1/q$, per la notació de la proposició $r = q$ i aleshores tenim que $< a >^s$ és una funció analítica amb radi de convergència més gran o igual que $qp^{-\frac{1}{p-1}}$. Tenim doncs que

$$< a >^s = \exp_p(s \log_p(< a >)),$$

per $s \in \mathbb{C}_p$ tal que $|s| < qp^{-\frac{1}{p-1}} > 1$.

6.2 Funcions p-àdiques mitjançant interpolació

En aquesta secció definirem dues funcions p-àdiques mitjançant interpolació. Definirem una funció p-àdica relacionada amb la funció zeta de Hurwitz i l'altre serà la funció L p-àdica. Les definirem per valors enters i després veurem que es poden estendre a funcions meromorfes a $\mathbb{C}_p$ amb un cert radi de convergència més gran que 1.

Primer fem una petita modificació a la funció zeta de Hurwitz de la següent manera.

Definició 6.10. *Siguin* $s \in \mathbb{C}$, $a, F \in Z$ *tals que* $0 < a < F$ *i* $\zeta(s, b)$ *la funció zeta de Hurwitz. Definim doncs*

$$H(s, a, F) = \sum_{\substack{m \equiv a(F) \\ m > 0}} m^{-s}.$$

Operant obtenim que

$$H(s, a, F) = \sum_{\substack{m \equiv a(F) \\ m > 0}} m^{-s} = \sum_{n=0}^{\infty} \frac{1}{(a + nF)^s} = F^{-s} \zeta(s, \frac{a}{F}).$$

H té un pol simple a $s = 1$ de residu $1/F$. Farem servir aquesta funció per a la interpolació, per tant ens interessa saber els seus valors a $1 - n$, que són

$$H(1-n,a,F) = -\frac{F^{n-1}B_n(\frac{a}{F})}{n} \in \mathbb{Q}, \quad n \geq 1.$$

Teorema 6.11. *Sigui $q|F$ i $p \not| a$. Aleshores existeix una funció p-àdica meromòrfica $H_p(s,a,F)$ a $D = \{s \in \mathbb{C}_p || s| < qp - \frac{1}{p-1} > 1\}$ tal que per $n \geq 1$*

$$H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F).$$

On recordem $\omega(a)$ és l'única arrel $\phi(q)$-èssima de la unitat tal que $a \equiv \omega(a) \pmod q$. A més, la funció H_p és analítica amb un pol simple a $s=1$ amb residu $1/F$.

Demostració. Definim la funció $H_p(s,a,F)$ de la següent manera.

$$H_p(s,a,F) = \frac{1}{s-1}\frac{1}{F} <a>^{1-s} \sum_{i=0}^{\infty} \binom{1-s}{i} (B_i) \left(\frac{F}{a}\right)^i,$$

on B_i és el nombre de Bernoulli i-èssim. Cal veure la convergència, que coincideix en els valors $n-1$ amb el que hem enunciat, i que a $s=1$ té un pol simple de residu $1/F$.

Per veure la convergència, usarem el teorema de von Staudt-Clausen que en particular justifica que $pB_n \in \mathbb{Z}_p$ per tot p i per tot n positiu i parell. Aleshores, comencem observant que $|((B_i)\left(\frac{F}{a}\right)^i|)$. Per tant per la proposició 6.9, tenim que $r = |q| = 1/q$, per tant

$$\sum_{i=0}^{\infty} \binom{s}{i} (B_i) \left(\frac{F}{a}\right)^i,$$

és analítica en D. Ara, observem que $D = \{s \in \mathbb{C}_p || 1-s| < qp - \frac{1}{p-1}\}$, doncs $qp^{-\frac{1}{p-1}} > 1$. Per tant

$$\sum_{i=0}^{\infty} \binom{1-s}{i} (B_i) \left(\frac{F}{a}\right)^i,$$

també és analítica en D. Ja hem comentat que $<a>^s$ és analítica en D, per tant pel mateix raonament $<a>^{1-s}$ també ho serà. Per tant H_p és una funció analítica amb un pol a $s=1$.

Anem a veure ara la igualtat pels valors $n \geq 1$. Substituint obtenim que

$$\begin{aligned} H_p(1-n,a,F) &= \frac{1}{-n}\frac{1}{F} <a>^{n} \sum_{i=0}^{\infty} \binom{n}{i} (B_i) \left(\frac{F}{a}\right)^i, \\ &= -\frac{F^{n-1}\omega^{-n}(a)}{n} B_n\left(\frac{a}{F}\right), \\ &= \omega^{-n}(a)H(1-n,a,F). \end{aligned}$$

Ara, per acabar, en $s=1$

$$H_p(1,a,F)(s-1) = \frac{1}{F} <a>^0 \sum_{i=0}^{\infty} \binom{0}{i} (B_i) \left(\frac{F}{a}\right)^i = \frac{1}{F}.$$

□

Observació 6.12. Si $n \equiv 0 \pmod{\phi(q)}$, aleshores

$$H_p(1-n,a,F) = H(1-n,a,F).$$

Ja hem definit la funció p-àdica associada a la funció zeta de Hurwitz mitjançant interpolació. De manera similar, anem a definir la funció L_p. Abans de tot, comentem que podem suposar els caràcters de Dirichlet χ en $\mathbb{C}_p$. Per tant $\omega(a)$ és un caràcter de Dirichlet en $\mathbb{C}_p$ de conductor q i ordre $\phi(q)$.

Teorema 6.13. *Sigui χ un caràcter de Dirichlet no principal de conductor f i sigui F un múltiple qualsevol de q i de f_χ. Aleshores existeix una funció p-àdica meromorfa $L_p(s,\chi)$ a $\{s \in \mathbb{C}_p || s| < qp^{-\frac{1}{p-1}}\}$ tal que:*

$$L_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \qquad n \geq 1.$$

A més, tenim la fórmula següent:

$$L_p(s,\chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a) <a>^{1-s} \sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j.$$

Demostració. Sigui

$$L_p(s,\chi) = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(s,a,F).$$

Per tant les propietats meromorfes ens venen del teorema anterior. Si $s=1$, tenim un residu

$$\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)(1/F) = \frac{1}{F}\sum_{a=1}^{F}\chi(a) - \frac{1}{F}\sum_{a|p}^{F}\chi(a) = \frac{1}{F}\sum_{b=1}^{F/p}\chi(pb).$$

Volem veure que el segon sumand també és 0. Si $p|f_\chi$, aleshores $\chi(pb)=0$ per tot b. Altrament, si $p \not| f_\chi$, aleshores $f_\chi|(F/p)$, doncs F és un múltiple de f_χ, i per tant el sumatori es 0. Per tant, $L_p(s,\chi)$ realment no té cap pol a $s=1$ si χ és no principal.

Hem comprovat que la funció és una funció p-àdica meromorfa a $L_p(s,\chi)$ a $\{s \in \mathbb{C}_p||s| < qp^{-\frac{1}{p-1}}\}$. Ara anem a veure que els seus valors en enters negatius concorden amb el que hem enunciat. Sigui $n \geq 1$. Aleshores substituint per la definció de H_p:

$$\begin{aligned} L_p(1-n,\chi) &= \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(1-n,a,F), \\ &= \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\omega^{-n}(a)H(1-n,a,F). \end{aligned}$$

Ara aplicant la definició de H i reordenant termes:

$$\begin{aligned} L_p(1-n,\chi) &= \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\omega^{-n}(a)\left(-\frac{F^{n-1}B_n\left(\frac{a}{F}\right)}{n}\right), \\ &= -\frac{F^{n-1}}{n}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right). \end{aligned}$$

Separant el sumatori en dos:

$$L_p(1-n,\chi) = -\frac{F^{n-1}}{n}\left(\sum_{a=1}^{F}\chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right) - \sum_{b=1}^{F/p}\chi\omega^{-n}(bp)B_n\left(\frac{bp}{F}\right)\right).$$

Entrant les F dins, substituint per la relació entre polinomis de Bernoulli i nombres de Bernoulli generalitzats vistes a 3.9, i reorganitzant termes obtenim:

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{1}{n}\left(F^{n-1}\sum_{a=1}^{F}\chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right) - p^{n-1}\frac{F^{n-1}}{p^{n-1}}\sum_{b=1}^{F/p}\chi\omega^{-n}(bp)B_n\left(\frac{bp}{F}\right)\right), \\ &= -\frac{1}{n}\left(B_{n,\chi\omega^{-n}} - \chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}\right), \\ &= -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}. \end{aligned}$$

□

Corołari 6.14. *Si χ és un caràcter de Dirichlet principal, aleshores $L_p(s,\chi_0)$ és una funció analítica amb un pol a $s=1$ de residu $(p-1)/p$.*

Demostració. Sigui $\chi = \chi_0$ un caràcter de Dirichlet principal. Aleshores el residu a $s=1$ de $L_p(s,\chi_0)$ és

$$\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\frac{1}{F} = 1 - \frac{1}{p}.$$

Per tant té un pol a $s=1$ de residu $1-\frac{1}{p} = \frac{p-1}{p}$ □

Observació 6.15. Si χ és un caràcter de Dirichlet senar, aleshores n i $\chi\omega^{-n}$ tenen paritats diferents, i per tant $B_{n,\chi\omega^{-n}} = 0$. Així doncs si χ és senar, obtenim que $L_p(s,\chi) = 0$.

Per tant en general treballarem amb χ parells, així no tenim que tot és igual a 0. La funció L_p es pot expressar també en forma de sèrie de potències de la següent manera:

Teorema 6.16. *Sigui χ un caràcter de Dirichlet no principal de conductor f_χ i siguin $pq \nmid f_\chi$. Aleshores*

$$L_p(s,\chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \ldots = \sum_{a=0}^{\infty}.a_i(s-1)^i,$$

tal que $|a_0| \leq 1$ i $p|a_i$ per tot $i \geq 1$.

Demostració. Per aquesta demostració es prova que per a $i \geq 6$ és cert que $p|a_i$ i després es comprova a mà que per les altres i també és cert. Per una demostració detallada veure [1][Teorema 5.12]. □

7 Teorema de Kummer

En aquest últim capítol demostrarem el dos últims teoremes del treball. El primer diu que que p divideix el nombre de classes relatiu si i només si p divideix el numerador d'un nombre de Bernoulli B_j tal que j és un nombre senar més petit o igual a $p-3$. El segon teorema ens dona la implicació $p|h_p^+ \to p|h_p^-$.

7.1 Congruències

En aquesta secció veurem tres resultats que donen equivalències entre funcions L_p, i entre nombres de Bernoulli. Seran resultats clau per les demostracions dels teoremes de la següent secció.

Proposició 7.1. *Sigui χ un caràcter de Dirichlet no principal de conductor f_χ i siguin $pq \nmid f_\chi$. Siguin $m, n \in \mathbb{Z}$. Aleshores*

$$L_p(m, \chi) \equiv L_p(n, \chi) \pmod{p}.$$

Demostració. Per 6.16 els dos costats són congruents a a_0 amb la notació del teorema, i per tant són congruents entre ells. □

Proposició 7.2 (Congruències de Kummer)**.** *Siguin $m \equiv n \not\equiv 0 \pmod{p-1}$ enters parells positius. Aleshores*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

Demostració. Com ω és una arrel $\phi(q)$-èssima de la unitat, tenim $L_p(s, \omega^n) = L_p(s, \omega^m)$. Per tant pel teorema 6.13

$$L_p(1-n, \omega^n) = -\frac{1}{n}(1 - \omega^{n-n}(p)p^{n-1})B_{n,1} = -\frac{1}{n}(1-p^{n-1})B_n.$$

Finalment obtenim doncs que

$$\begin{aligned} -\frac{1}{n}(1-p^{n-1})B_n &= L_p(1-n, \omega^n), \\ &= L_p(1-n, \omega^m), \\ &\equiv L_p(1-m, \omega^m) \pmod{p}, \\ &= -\frac{1}{m}(1-p^{m-1})B_m. \end{aligned}$$

□

Per últim, veiem una equivalència entre els nombres de Bernoulli generalitzats i els nombres de Bernoulli.

Proposició 7.3. *Sigui $n \in \mathbb{Z}$ senar tal que $n \not\equiv -1 \pmod{p-1}$. Aleshores*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod{p}.$$

Demostració. Primer de tot observem que $\omega^{-n} \neq 1$, ja que $n \not\equiv -1$. A més, com $\omega^n \neq 1$, obtenim que $\omega^n(p) = 0$. Per tant

$$B_{1,\omega^n} = (1 - \omega^n(p))B_{1,\omega^n}.$$

Ara aplicant 6.13:

$$(1 - \omega^n(p))B_{1,\omega^n} = -L_p(0, \omega^{n+1}).$$

Utilitzant 7.1 obtenim:

$$L_p(0, \omega^{n+1}) \equiv -L_p(1-(n+1), \omega^{n+1}).$$

Finalment, tornant a utilitzar 6.13 i operant:

$$-L_p(1-(n+1), \omega^{n+1}) = (1-p^n)\frac{B_{n+1}}{n+1} \equiv \frac{B_{n+1}}{n+1} \pmod{p}.$$

□

7.2 Teoremes de Kummer

En aquesta última secció veiem els últims resultats del treball. Usarem resultats importants com la fórmula del nombre de classes que van demostrar al capítol 4 i altres proposicions vistes al capítol anterior.

Teorema 7.4. *Sigui p un primer senar i sigui h_p^- el nombre de classes relatiu de $\mathbb{Q}(\zeta_p)$. Aleshores*

$$p|h_p^- \leftrightarrow p \text{ divideix el numerador de } B_j \text{ per algun } j \in \{2, 4, \ldots, p-3\}.$$

Demostració. Abans de començar, hem de trobar els caràcters senars de $\mathbb{Q}(\zeta_p)$. Està clar que els caràcters senars corresponents són $\omega, \omega^3, \ldots, \omega^{p-2}$.

Aleshores, pel teorema 4.17, com $\mathcal{Q} = 1$ i $w = 2p$, obtenim que

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ senar}}}^{p-2} (-\frac{1}{2}B_{1,\omega^j}).$$

Trobem primer una equivalència de l'últim terme del productori:

$$B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv \frac{p-1}{p} \pmod{\mathbb{Z}_p}.$$

Per tant

$$(2p)(-\frac{1}{2}B_{1,\omega^{p-2}}) \equiv 1 \pmod{p}.$$

Per tant podem eliminar l'últim terme i el $2p$ i el resultat serà equivalent a h_p^- mòdul p. Finalment obtenim:

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ senar}}}^{p-4} (-\frac{1}{2}B_{1,\omega^j}) \pmod{p},$$

$$h_p^- \overset{7.3}{\equiv} \prod_{\substack{j=1 \\ j \text{ senar}}}^{p-4} (-\frac{1}{2}\frac{B_{j+1}}{j+1}) \pmod{p}.$$

□

Ara tenim una fórmula per a h_p^- i també per als nombres de Bernoulli. Ens falta encara relacionar que p divideixi h_p i que p divideixi h_p^-. Primer observem que una implicació és trivial, doncs si $p|h_p^-$, per definició $p|h_p$, ja que $h_p^- = h_p/h_p^+$. Per tant, només ens queda per veure que si $p|h_p$ aleshores $p|h_p^-$. Per veure-ho serà suficient veure que $p|h_p^+ \to p|h_p^-$.

Usarem la següent fórmula, anomenada la fórmula del nombre de classes p-àdica. La seva demostració queda fora de l'abast d'aquest treball. Abans de tot, necessitem la següent definició.

Definició 7.5 (Regulador p-àdic)**.** *Sigui K un cos de nombres. Sigui $r = r_1 + r_2 - 1$, on r_1, r_2 són el nombre d'immersions reals i imaginàries respectivament. Siguin doncs les immersions de K a $\mathbb{C}_p$ $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1,r_2}$. Sigui $\delta_i = 1$ si σ_i és real i $d_i = 2$ si σ_i és imaginari. Siguin $\epsilon_1, \ldots, \epsilon_r$ unitats independents de K. Aleshores*

$$R_{K,p}(\epsilon_1, \ldots, \epsilon_r) = \det(\delta_i \log_p(\sigma_i \epsilon_j))_{1 \leq i,j \leq r}.$$

Si $\epsilon_1, \ldots, \epsilon_r$ és una base d'unitats de K mòdul arrels de la unitat, aleshores usarem la següent notació:

$$R_{K,p}(\epsilon_1, \ldots, \epsilon_r) = R_p(K).$$

Teorema 7.6 (Fórmula del nombre de classes p-àdica)**.** *Sigui X un grup de caràcters de Dirichlet tal que el seu cos de nombres associat K és totalment real, abelià i de grau n. Aleshores*

$$\frac{2^{n-1} h(K) R_p(K)}{\sqrt{d(K)}} = \prod_{\substack{\chi \in X \\ \chi \text{ no principal}}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi).$$

Proposició 7.7. *Sigui K un cos de nombres totalment real i abelià. Si p no divideix $[K : \mathbb{Q}]$, existeix només un primer de K sobre p, i l'índex de ramificació de p és com a molt $p - 1$, aleshores*

$$\left| \frac{R_p(K)}{\sqrt{d(K)}} \right| \leq 1.$$

Demostració. La demostració usa alguns resultats vistos en aquest treball, però principalment usa raonaments basats en cossos p-àdics. Com no hem profunditzat massa en aquests cossos i les seves propietats, no farem la demostració en aquest treball. Per una demostració detallada veure [1][Teorema 5.33]. □

Teorema 7.8. $p|h_p^+ \Rightarrow p|h_p^-$.

Demostració. Els caràcters corresponents a $\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ són $1, \omega^2, \ldots, \omega^{p-3}$. El grau de l'extensió $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$ és $n = \frac{1}{2}(p-3)$. Per tant, per la fórmula del nombre de classes p-àdic 7.6, tenim que

$$\frac{2^{n-1} h_p^+) R_p(\mathbb{Q}^+(\zeta_p))}{\sqrt{d(\mathbb{Q}^+(\zeta_p))}} = \prod_{\substack{j=2 \\ j \text{ parell}}}^{p-3} L_p(1, \omega^j).$$

Ara, observem que $Q^+(\zeta_p)$ satisfà les condicions de 7.7, per tant

$$\left| \frac{R_p(\mathbb{Q}^+(\zeta_p))}{\sqrt{d(\mathbb{Q}^+(\zeta_p))}} \right|.$$

Aleshores obtenim que no poden ser divisibles per p. En conclusió, si $p|h^+$, aleshores cal que $p|L_p(1,\omega^j)$ per algun $j \in \{2,4,\ldots,p-3\}$.

Sigui $i=j$ tal que $p|L_p(1,\omega^j)$. Obtenim doncs que

$$0 \equiv L_p(1,\omega^i) \overset{7.1}{\equiv} L_p(0,\omega^i) \overset{6.13}{\equiv} -(1-\omega^{i-1}(p))B_{1,\omega^{i-1}} \equiv -B_{1,\omega^{i-1}} \pmod{p}.$$

Finalment, com

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ senar}}}^{p-4} (-\frac{1}{2}B_{1,\omega^j}) \pmod{p},$$

obtenim que $p|h^-$. □

Referències

[1] Washington, L. C.; *introduction to cyclotomic fields*, Graduate text in mathematics, 1980.

[2] Lang, S.; *Algebraic Number Theory*, Addison-Wesley: Reading, MA, 1970.

[3] Whittaker, E.; Watson, G.; *A Course of Modern Analysis*, 4th edition Cambridge Univ. Press: Cambridge, 1958.

[4] Iwasawa, K.; *Lectures on P-Adic L-Functions*. (AM-74), Volume 74

[5] Travesa Grau, A; *Teoria de Nombres*, Universitat de Barcelona, 2016.

[6] Plans Calvo, P;*L'últim teorema de Fermat per a primers regulars*, Universitat de Barcelona, 2024.