Teoria de Nombres

Artur Travesa

Universitat de Barcelona

Autor
Artur **Travesa Grau**
Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Classificació AMS (2010): Primària: 11-01, 11R, 11S.
Secundària: 11D, 11E, 11H, 11M, 11N, 13A, 13B, 14G.

Universitat de Barcelona
Facultat de Matemàtiques i Informàtica
Barcelona, 2016, 2020

Contingut

Introducció **1**

1 Llei de reciprocitat quadràtica **3**

1.1 Teoria de Galois 3
1.2 Cossos ciclotòmics 4
1.3 Períodes de Gauss 5
1.4 Caràcters de Dirichlet 6
1.5 Símbol de Legendre 8
1.6 Sumes de Gauss 9
1.7 Cossos quadràtics 11
1.8 Congruències quadràtiques 12
1.9 Llei de reciprocitat quadràtica 14
1.10 Símbol de Jacobi 16
1.11 Símbol de Kronecker 18

2 Enters dels cossos de nombres **23**

2.1 Elements enters sobre un anell 23
2.2 Enters dels cossos de nombres 25
2.3 Anells de Dedekind 26
2.4 El grup d'ideals 27
2.5 Factorialitat i principalitat 30

3 Ramificació **33**

3.1 Normes i traces 33
3.2 Extensions d'anells de Dedekind 35
3.3 Índex de ramificació i grau residual 36
3.4 La fórmula $\sum e_i f_i = n$ 38
3.5 El cas galoisià 40
3.6 Discriminant 42

3.7 Discriminant i ramificació 46
3.8 El cas quadràtic 48
3.9 El cas ciclotòmic 50

4 Geometria dels nombres **57**
4.1 Dominis fonamentals 57
4.2 Xarxes de $\mathbb{R}^n$ 58
4.3 La immersió canònica d'un cos de nombres 60
4.4 Finitud del grup de classes d'ideals 62
4.5 Teoremes de finitud 64
4.6 El teorema de Dirichlet de les unitats 67
4.7 Unitats dels cossos quadràtics 70
4.8 Exemples 71

5 Ramificació superior **75**
5.1 El diferent 75
5.2 Relació entre el diferent i el discriminant 78
5.3 Grups de descomposició i d'inèrcia 81
5.4 Cossos de descomposició i d'inèrcia 83
5.5 Automorfisme de Frobenius 85
5.6 Grups de ramificació superior 87
5.7 El grup d'inèrcia moderada 90
5.8 Grups de ramificació i diferent 91

6 El teorema de Kronecker-Weber **95**
6.1 El cas moderadament ramificat 95
6.2 El cas cíclic de grau potència d'un primer senar 97
6.3 El cas cíclic de grau potència de 2 99
6.4 Conductor d'una extensió abeliana de $\mathbb{Q}$ 100

7 Ramificació en el cas infinit **103**
7.1 Teoria de Galois 103
7.2 Grups de descomposició i d'inèrcia 105
7.3 Extensions abelianes no finites de $\mathbb{Q}$ 107

8 Equacions diofantines **109**
8.1 Còniques racionals 109
8.2 El teorema de Legendre 111

8.3 L'equació de Fermat per a exponent 3 . . . 114
8.4 L'equació de Fermat per a exponent 4 . . . 115
8.5 Primer cas de l'equació de Fermat . . . 116

9 Anàlisi p-àdica **121**
9.1 Valoracions . . . 121
9.2 Valor absoluts . . . 123
9.3 Valors absoluts de **Q**. Fórmula del producte . . . 126
9.4 Complecions . . . 128
9.5 Cossos complets no arquimedians . . . 131
9.6 Extensions finites de cossos complets no arquimedians . . . 134
9.7 Valors absoluts arquimedians . . . 135
9.8 Extensió de valors absoluts discrets . . . 136
9.9 Ramificació i compleció . . . 139
9.10 Lema de Krasner . . . 143
9.11 El cos $\mathbb{C}_p$ . . . 146
9.12 Funcions p-àdiques . . . 147

10 Formes quadràtiques p-àdiques **153**
10.1 Espais quadràtics . . . 153
10.2 Diagonalització . . . 156
10.3 Teorema de Witt . . . 157
10.4 Formes quadràtiques sobre cossos finits . . . 159
10.5 Àlgebres de quaternions . . . 161
10.6 Símbol de Hilbert . . . 164
10.7 Invariant de Hasse-Witt . . . 167
10.8 Representació de nombres per formes . . . 169
10.9 Descripció de les classes d'equivalència . . . 173

11 Formes quadràtiques racionals **175**
11.1 Propietats globals del símbol de Hilbert . . . 175
11.2 Lema d'aproximació . . . 176
11.3 El teorema de Hasse-Minkowski . . . 178
11.4 Formes quadràtiques racionals . . . 182

12 Sèries de Dirichlet **185**
12.1 La fórmula d'inversió de Möbius . . . 185
12.2 Sèries de Dirichlet . . . 187

12.3 Producte de sèries de Dirichlet 190
12.4 Productes d'Euler 192
12.5 Convergència de les sèries de Dirichlet 194
12.6 Analiticitat de les funcions de Dirichlet 196

13 La funció zeta de Hurwitz **199**
13.1 La funció Gamma d'Euler 199
13.2 Definició de la funció zeta de Hurwitz 201
13.3 Extensió de la funció zeta de Hurwitz 204
13.4 Polinomis de Bernoulli 208
13.5 El teorema de Clausen-von Staudt 212
13.6 Interpolació p-àdica de la funció zeta 214

14 El teorema de la progressió aritmètica **217**
14.1 Funció zeta d'un conjunt de nombres primers 217
14.2 Funcions L de Dirichlet 218
14.3 Demostració del teorema 222
14.4 Valors de les funcions L en els enters negatius 224
14.5 Interpolació p-àdica les funcions L de Dirichlet 227
14.6 Congruències de Kummer 230

15 Fórmules per als nombres de classes **233**
15.1 La funció zeta de Dedekind 233
15.2 El regulador d'un cos de nombres 234
15.3 Densitat dels ideals d'una classe 236
15.4 Residu de la funció zeta de Dedekind en $s = 1$ 242
15.5 Fórmula del nombre de classes: cas quadràtic 245
15.6 Fórmula del nombre de classes: cas ciclotòmic 247
15.7 Avaluació de les funcions L de Dirichlet en $s = 1$ 249
15.8 Nombre de classes dels cossos quadràtics 251
15.9 El signe de les sumes de Gauss per als caràcters de Legendre 255

16 Aplicacions a la conjectura de Fermat **261**
16.1 Factors del nombre de classes 261
16.2 Càlcul del segon factor del nombre de classes 265
16.3 El regulador p-àdic 268
16.4 El criteri de regularitat de Kummer 270
16.5 El lema de Kummer 272

16.6 El segon cas del teorema de Fermat 273

A Taules **277**

A.1 Nombres de Bernoulli 277

A.2 Polinomis de Bernoulli 279

Referències **281**

Índex terminològic **283**

Introducció

El sintagma nominal "teoria de nombres" és una perífrasi de la paraula "aritmètica", de manera que totes dues expressions tenen el mateix significat. En efecte, des del punt de vista etimològic, la paraula aritmètica deriva de la llatina *arithmetica* que, a la vegada, prové de l'expressió grega *ἀριθμητική τέχνη* (literalment, art numèrica), derivada de l'adjectiu *ἀριθμητικός* (relatiu al nombre), i, aquest, del substantiu *ἀριθμός* (nombre, número) (cf. [Cor 80, vol. I, p. 389]). Doncs, l'aritmètica és l'estudi dels nombres.

Per a fer l'estudi dels nombres s'utilitzen diversos mètodes i tècniques que donen lloc a diferents branques de la matemàtica.

La revisió de l'any 2010 de la classificació temàtica de la Societat Matemàtica Americana (*2010 AMS Subject Classification*) conté un apartat, amb l'encapçalament *Teoria de nombres*, que inclou 300 entrades distribuïdes en 21 seccions. Aquestes 21 seccions fan referència a diferents temàtiques o mètodes d'estudi relatius a la teoria de nombres; per exemple, n'hi ha dedicades a la teoria algebraica de nombres (seccions 11R: cossos globals, 30 entrades, i 11S: cossos locals, 16 entrades), a la teoria analítica de funcions zeta i de funcions L (secció 11M, 13 entrades), a la geometria algebraica aritmètica (secció 11G, 19 entrades), a la teoria transcendent de nombres i l'aproximació diofantina (secció 11J, 25 entrades), a la teoria computacional de nombres (secció 11Y, 12 entrades), a la teoria probabilística de nombres (secció 11K, 14 entrades), a la teoria elemental de nombres (secció 11A, 11 entrades), a la teoria multiplicativa de nombres (secció 11N, 17 entrades), a la teoria additiva de nombres (secció 11P, 11 entrades), o a les equacions diofantines (secció 11D, 17 entrades), entre altres.

El curs que presentem és fonamentalment un curs de *teoria algebraica de nombres algebraics*; tot i aquesta precisió, convé notar que en el seu desenvolupament apareixeran d'una manera essencial nombres no algebraics i que en algunes parts s'utilitzaran tècniques no pròpiament o exclusivament algebraiques.

La teoria algebraica de nombres (algebraics) té dos objectius principals: d'una banda, la construcció d'una teoria general dels cossos de nombres algebraics que en permeti una classificació completa i la descripció de la seva aritmètica, i, de l'altra, l'estudi de les aplicacions d'aquesta teoria general a qüestions concretes: per exemple, equacions diofantines, multiplicació complexa de funcions abelianes i el·líptiques, integració de diferencials algebraiques, teories de codificació i criptografia, i altres. El seu estudi es basa en diverses teories i metodologies; per exemple, la teoria de Galois, la de la ramificació, l'anàlisi complexa, o l'anàlisi p-àdica. I usa eines diferents; citem les funcions analítiques, les corbes el·líptiques, les formes modulars, o les varietats abelianes. Algunes d'aquestes tècniques i eines s'utilitzaran aquest curs; concretament, aquelles que duen de manera natural a la consecució dels objectius que ens proposem: d'una banda, la demostració del Teorema de Kronecker-Weber sobre el cos dels nombres racionals i, de l'altra, la prova del

darrer "teorema" de Fermat per al cas d'exponents regulars, en la línia de Kummer, en el segle XIX. Òbviament, després de la demostració completa del teorema (cf. [Wi 1995]), cal entendre aquest darrer objectiu com una revisió d'alguns dels mètodes més profitosos de la teoria que, encara que ara han quedat obsolets per al teorema, es fan servir, amb generalitzacions adequades, en altres contextos, especialment de geometria aritmètica.

Artur Travesa

Estiu de 2020

Capítol 1

Llei de reciprocitat quadràtica

1.1 Teoria de Galois

Sigui $L|K$ una extensió finita de cossos. El grup dels automorfismes de L que deixen fixos els elements de K s'anomena el grup de Galois de l'extensió $L|K$ i es denota per $\mathrm{Gal}\,(L|K)$; és un grup finit d'ordre menor o igual que el grau de l'extensió. Es diu que l'extensió $L|K$ és de Galois quan se satisfà la igualtat; equivalentment, quan l'extensió és normal i separable. Una extensió finita $L|K$ s'anomena abeliana (respectivament cíclica, resoluble, nilpotent) quan és de Galois i, a més a més, el grup de Galois $\mathrm{Gal}\,(L|K)$ és un grup abelià (respectivament cíclic, resoluble, nilpotent).

Si $L|K$ és una extensió de Galois i K' és un subcòs de L que conté K, l'extensió $L|K'$ també és una extensió de Galois i el grup $\mathrm{Gal}\,(L|K')$ és un subgrup de $\mathrm{Gal}\,(L|K)$; una condició necessària i suficient perquè l'extensió $K'|K$ sigui de Galois és que $\mathrm{Gal}\,(L|K')$ sigui un subgrup normal de $\mathrm{Gal}\,(L|K)$; en aquest cas, el grup de Galois de l'extensió $K'|K$ s'identifica de manera natural amb el grup quocient $\mathrm{Gal}\,(L|K)\,/\mathrm{Gal}\,(L|K')$, ja que hi ha una successió exacta de grups

$$1 \longrightarrow \mathrm{Gal}\,(L|K') \xrightarrow{inc} \mathrm{Gal}\,(L|K) \xrightarrow{res} \mathrm{Gal}\,(K'|K) \longrightarrow 1.$$

D'altra banda, l'anomenat teorema fonamental de la teoria de Galois afirma que hi ha una correspondència bijectiva entre el conjunt dels subcossos K' de L que contenen K i el conjunt dels subgrups de $\mathrm{Gal}\,(L|K)$; aquesta correspondència s'obté assignant a cada cos K' el grup $\mathrm{Gal}\,(L|K')$ i inverteix l'ordre donat per inclusió. Recíprocament, a cada subgrup $H \subseteq \mathrm{Gal}\,(L|K)$ li correspon el cos L^H dels elements de L que són invariants per tots els automorfismes de H.

Siguin $L_1|K$ i $L_2|K$ dues extensions finites de Galois dins d'una mateixa clausura algebraica del cos K. L'extensió composició $L_1L_2|K$ i l'extensió intersecció $L_1 \cap L_2|K$ són aleshores extensions de Galois; el grup de Galois de la composició es pot identificar amb un subgrup del grup producte $\mathrm{Gal}\,(L_1|K) \times \mathrm{Gal}\,(L_2|K)$. Aquesta identificació es fa assignant a cada K-automorfisme σ de L_1L_2 la parella d'automorfismes que s'obté per restricció de σ a cada un dels cossos L_i. A més a més, el grup de Galois $\mathrm{Gal}\,(L_1L_2|L_1 \cap L_2)$ és isomorf de manera natural al producte $\mathrm{Gal}\,(L_1|L_1 \cap L_2) \times \mathrm{Gal}\,(L_2|L_1 \cap L_2)$. D'aquesta manera obtenim una successió exacta

$$1 \longrightarrow \mathrm{Gal}\,(L_1|L_1 \cap L_2) \times \mathrm{Gal}\,(L_2|L_1 \cap L_2) \longrightarrow \mathrm{Gal}\,(L_1L_2|K) \longrightarrow \mathrm{Gal}\,(L_1 \cap L_2|K) \longrightarrow 1.$$

Quan $L_1 \cap L_2 = K$, diem que les extensions $L_1|K$, $L_2|K$ són linealment disjuntes; en aquest cas, el grup de Galois $\mathrm{Gal}\,(L_1L_2|K)$ és isomorf al producte dels grups $\mathrm{Gal}\,(L_1|K)$ i $\mathrm{Gal}\,(L_2|K)$.

D'altra banda, si $L|K$ és una extensió de Galois i $K'|K$ és una extensió qualsevol, aleshores l'extensió $LK'|K'$ és de Galois i $\mathrm{Gal}\,(LK'|K')$ és un subgrup de $\mathrm{Gal}\,(L|K)$. En canvi, el fet que dues extensions $K'|K$ i $L|K'$ siguin de Galois no implica que l'extensió $L|K$ també ho sigui.

Per a tots els detalls i les demostracions dels resultats anteriors pot ser útil gairebé qualsevol llibre de teoria de Galois; la referència [Tra 2020] s'adapta particularment a la nostra exposició.

1.2 Cossos ciclotòmics

Considerem fixada una clausura algebraica $\overline{\mathbb{Q}}$ del cos $\mathbb{Q}$ dels nombres racionals. Sigui $\zeta \in \overline{\mathbb{Q}}$ una arrel primitiva n-èsima de la unitat. L'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ s'anomena la n-èsima extensió ciclotòmica de $\mathbb{Q}$; és una extensió de Galois i el seu grup de Galois s'identifica de manera natural amb el grup multiplicatiu dels elements invertibles de l'anell $\mathbb{Z}/n\mathbb{Z}$. En efecte, si σ és un automorfisme de $\mathbb{Q}(\zeta)$, aleshores $\sigma(\zeta)$ ha de ser també una arrel primitiva n-èsima de la unitat i, per tant, de la forma $\sigma(\zeta) = \zeta^{\chi(\sigma)}$, on $\chi(\sigma)$ és un nombre enter definit mòdul n i coprimer amb n que no depèn de l'elecció de l'arrel primitiva ζ; això fa que l'aplicació $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) \xrightarrow{\chi} (\mathbb{Z}/n\mathbb{Z})^*$ sigui un isomorfisme de grups; s'anomena el n-èsim caràcter ciclotòmic. L'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és, doncs, abeliana i, en conseqüència, si $K|\mathbb{Q}$ és una extensió qualsevol, també $K(\zeta)|K$ és una extensió abeliana.

Posem $n = p^r n'$ amb $r \geq 0$ i p un nombre primer que no divideix n'. Aleshores $\zeta^{n'}$ és una arrel primitiva p^r-èsima de la unitat i $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$ és una subextensió de $\mathbb{Q}(\zeta)|\mathbb{Q}$. L'isomorfisme χ, definit per a cada nombre enter positiu n, és compatible amb els morfismes de reducció

$$\begin{aligned} \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) &\longrightarrow \mathrm{Gal}\left(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}\right) \\ (\mathbb{Z}/n\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/p^r\mathbb{Z})^* \end{aligned}$$

de manera que hi ha un diagrama commutatiu de morfismes de grups abelians

$$\begin{array}{ccc} \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) & \xrightarrow{\chi} & (\mathbb{Z}/n\mathbb{Z})^* \\ {\scriptstyle red}\downarrow & & \downarrow{\scriptstyle red} \\ \mathrm{Gal}\left(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}\right) & \xrightarrow[\chi]{} & (\mathbb{Z}/p^r\mathbb{Z})^*\,. \end{array}$$

En particular, l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és la composició de les extensions linealment disjuntes $\mathbb{Q}(\zeta^{p^r})|\mathbb{Q}$ i $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$ i $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta^{p^r})|\mathbb{Q}\right) \times \mathrm{Gal}\left(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}\right)$. Això permet reduir l'estudi dels cossos ciclotòmics al cas dels generats per arrels primitives p^r-èsimes de la unitat, amb p primer i $r \geq 1$.

La importància de les extensions ciclotòmiques de $\mathbb{Q}$ rau en el següent

Teorema 1.2.1 (Kronecker-Weber)**.** *Sigui $K|\mathbb{Q}$ una extensió abeliana finita. Aleshores, existeix una arrel de la unitat ζ tal que K és un subcòs del cos ciclotòmic $\mathbb{Q}(\zeta)$.*

Un dels objectius d'aquest curs és fer una demostració d'aquest teorema.

1.3 Períodes de Gauss

Siguin p un nombre primer senar i ζ una arrel primitiva p-èsima de la unitat. El grup de Galois $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$ és cíclic d'ordre $p-1$, de manera que hi ha una correspondència bijectiva entre el conjunt de les subextensions de l'extensió ciclotòmica $\mathbb{Q}(\zeta)|\mathbb{Q}$ i el conjunt dels divisors positius d de $p-1$. L'objectiu immediat és donar un element primitiu per a cada un dels subcossos de $\mathbb{Q}(\zeta)$; és a dir, donar-ne un generador sobre $\mathbb{Q}$.

Sigui g un generador del grup multiplicatiu $(\mathbb{Z}/p\mathbb{Z})^*$. Aleshores, l'automorfisme σ de $\mathbb{Q}(\zeta)$ definit per la fórmula $\sigma(\zeta) := \zeta^g$ és un generador del grup $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$.

En aquesta secció, i per comoditat d'escriptura, per a tot nombre enter i posarem $\zeta_i := \zeta^{g^i}$. La demostració del resultat següent no presenta cap dificultat.

Lema 1.3.1. *Siguin i, j nombres enters qualssevol. Aleshores,*

$$\zeta_i = \zeta_j \iff i \equiv j \pmod{p-1}; \qquad \sigma^j(\zeta_i) = \zeta_{i+j}. \square$$

Definició 1.3.2. Sigui n un divisor qualsevol de $p-1$, i posem $d := \dfrac{p-1}{n}$. Per a tot nombre enter i, $0 \le i \le n-1$, anomenarem i-èsim n-període de ζ relatiu a g l'element de $\mathbb{Q}(\zeta)$

$$\eta_i := \sum_{j=0}^{d-1} \sigma^{jn}(\zeta_i) = \sum_{j=0}^{d-1} \zeta_{i+jn}.$$

Els n-períodes depenen de l'elecció de ζ i de g. Ara bé, el resultat següent ens ensenya de quina forma és aquesta dependència.

Proposició 1.3.3. *Amb les notacions anteriors, el conjunt $\{\eta_0, \eta_1, \ldots, \eta_{n-1}\}$ no depèn ni de l'elecció del generador g de $(\mathbb{Z}/p\mathbb{Z})^*$ ni de l'elecció de l'arrel primitiva p-èsima de la unitat ζ. A més a més, el període η_0 no depèn de l'elecció de g, i els diferents η_i són els n-períodes η'_0 associats a les diferents arrels primitives p-èsimes de la unitat ζ'.*

Demostració: Com que n divideix l'ordre de $G := (\mathbb{Z}/p\mathbb{Z})^*$, els exponents g^{i+jn} de ζ en el n-període η_i formen una classe lateral de G mòdul el subgrup $\langle g^n \rangle$; i com que G és cíclic, aquest subgrup no depèn del generador g elegit en G. Per tant, les classes laterals tampoc no depenen de g. Això demostra que el període η_0 i el conjunt $\{\eta_0, \eta_1, \ldots, \eta_{n-1}\}$ no depenen de quin sigui el generador g de G.

D'altra banda, si canviem ζ per una altra arrel primitiva p-èsima de la unitat ζ', podem escriure $\zeta' = \zeta^{g^\alpha}$ per a un cert nombre enter α; aleshores, per a tot nombre enter i, $0 \le i \le n-1$, és

$$\eta'_i = \sum_{j=0}^{d-1} \zeta'_{i+jn} = \sum_{j=0}^{d-1} \zeta_{\alpha+i+jn} = \eta_{\alpha+i}.$$

Per tant, els períodes η_i es poden obtenir com els períodes η_0 associats a les diferents arrels primitives p-èsimes de la unitat. $\square$

Sigui, ara, $K|\mathbb{Q}$ una subextensió de $\mathbb{Q}(\zeta)|\mathbb{Q}$. El grau $n := [K : \mathbb{Q}]$ és un divisor de $p-1$ i K és el cos fix per l'únic subgrup $H \subseteq \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$ d'índex n. Per tant, el cos K és generat sobre $\mathbb{Q}$ pels coeficients del polinomi irreductible de ζ sobre el cos K (cf. [Tra 2020, Proposició 4.5.2]).

Ara bé, H és el grup $\langle\sigma^n\rangle$, de manera que

$$\mathrm{Irr}(\zeta, K) = \prod_{\tau\in H} (X - \tau(\zeta)) = \prod_{j=0}^{d-1} \left(X - \sigma^{jn}(\zeta)\right),$$

on $d := \dfrac{p-1}{n}$; els coeficients d'aquest polinomi són els polinomis simètrics elementals $s_k := s_k(x_0, x_1, \ldots, x_{d-1})$, $1 \leq k \leq d$, dels elements $x_j := \sigma^{jn}(\zeta) = \zeta_{jn}$, $0 \leq j \leq d-1$. El cos generat sobre $\mathbb{Q}$ pels polinomis simètrics elementals $s_k(x_0, x_1, \ldots, x_{d-1})$ és el mateix que el cos generat pels polinomis de Newton $t_k := t_k(x_0, x_1, \ldots, x_{d-1}) := \displaystyle\sum_{j=0}^{d-1} x_j^k$ (cf. [B-M-T 90, ex.50]). Aquests darrers són exactament els n-períodes de ζ relatius a un cert generador g' de $(\mathbb{Z}/p\mathbb{Z})^*$: en efecte, com que $1 \leq k < p$, el nombre enter k és una unitat de $(\mathbb{Z}/p\mathbb{Z})^*$ i es pot escriure en la forma $k = g^i$ per a un cert nombre enter i; aleshores, $t_k = \eta_i$. Per tant, $K \subseteq \mathbb{Q}(\eta_0, \eta_1, \ldots, \eta_{n-1})$. D'altra banda, de la definició dels períodes és clar que $\sigma^n(\eta_i) = \eta_i$, de manera que $\eta_i \in K$, ja que K és el cos fix per $\langle\sigma^n\rangle$. Això demostra la igualtat $K = \mathbb{Q}(\eta_0, \eta_1, \ldots, \eta_{n-1})$.

Finalment, se satisfà la igualtat $\sigma^j(\eta_i) = \eta_{i+j}$, per a tota parella de nombres enters i, j; per tant, els períodes η_i són tots conjugats; com que $\mathbb{Q}(\eta_i) \subseteq \mathbb{Q}(\zeta)$, l'extensió $\mathbb{Q}(\eta_i)|\mathbb{Q}$ és de Galois (i abeliana), de manera que $K = \mathbb{Q}(\eta_i)$. Hem demostrat, doncs, el següent

Teorema 1.3.4. *Siguin p un nombre primer senar, ζ una arrel primitiva p-èsima de la unitat, $K \subseteq \mathbb{Q}(\zeta)$ un subcòs qualsevol i $n := [K : \mathbb{Q}]$ el grau. Aleshores, per a tot nombre enter i, $0 \leq i \leq n-1$, podem escriure $K = \mathbb{Q}(\eta_i)$, on η_i denota el i-èsim n-període de ζ relatiu a qualsevol generador del grup $(\mathbb{Z}/p\mathbb{Z})^*$.*

Observació 1.3.5. La part final d'aquesta demostració es pot fer de manera més senzilla (cf. [vdW 70, chap.VIII,§ 4]; però hem fet aquesta a fi d'obtenir-ne posteriorment una generalització.

En particular, i com que p és senar, podem pensar en l'única subextensió quadràtica $K|\mathbb{Q}$ de $\mathbb{Q}(\zeta_p)|\mathbb{Q}$. Podem descriure aquest cos fàcilment? La resposta a aquesta pregunta és l'objectiu de les seccions següents.

1.4 Caràcters de Dirichlet

Sigui G un grup abelià finit. El grup $\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$ s'anomena el grup dual o dels caràcters (complexos) de G. Si $\chi : G \longrightarrow \mathbb{C}^*$ és un caràcter, la imatge està formada per arrels de la unitat, ja que G és d'ordre finit. Encara més, si n denota l'exponent del grup abelià G (si es vol, el generador positiu de l'ideal anul·lador del $\mathbb{Z}$-mòdul G), aleshores la imatge de χ està formada per arrels n-èsimes de la unitat.

Proposició 1.4.1. *Sigui G un grup abelià finit. Llavors G és isomorf (no canònicament) a $\widehat{G}$ i és naturalment isomorf a $\widehat{\widehat{G}}$.*

Demostració: Cf. [B-M-T 90, ex.265]. □

Proposició 1.4.2 (Relacions d'ortogonalitat dels caràcters)**.** *Siguin G un grup abelià finit i g el seu ordre. Aleshores:*

$$\sum_{\sigma\in G}\chi(\sigma)=\begin{cases}g & si\ \chi=1,\\ 0 & si\ \chi\neq 1,\end{cases}\qquad \chi\in\widehat{G},$$

$$\sum_{\chi\in\widehat{G}}\chi(\sigma)=\begin{cases}g & si\ \sigma=1,\\ 0 & si\ \sigma\neq 1,\end{cases}\qquad \sigma\in G.$$

Demostració: Cf. [B-M-T 90, ex.266] □

Proposició 1.4.3. *Sigui $0\longrightarrow G'\longrightarrow G\longrightarrow G''\longrightarrow 0$ una successió exacta de grups abelians finits. Aleshores, la successió $1\longrightarrow\widehat{G''}\longrightarrow\widehat{G}\longrightarrow\widehat{G'}\longrightarrow 1$ que s'obté en aplicar el functor $\mathrm{Hom}(*,\mathbb{C}^*)$ és exacta.*

Demostració: Exercici. □

Observació 1.4.4. En comptes d'utilitzar $\mathbb{C}^*$ podríem haver utilitzat qualsevol cos algebraicament tancat de característica zero; en particular, $\overline{\mathbb{Q}}$. Encara més, com que la imatge està formada per arrels de la unitat, és suficient que el cos que es pren contingui les arrels de la unitat necessàries. Per exemple, si p és un nombre primer que no divideix l'ordre del grup G, els resultats per al cos $\overline{\mathbb{F}}_p$ en lloc de $\mathbb{C}$ són els mateixos, perquè G també és isomorf a $\mathrm{Hom}(G,\overline{\mathbb{F}}_p^*)$.

Per comoditat d'escriptura, convé escriure $G(n)$ per a designar el grup multiplicatiu $(\mathbb{Z}/n\mathbb{Z})^*$ dels elements invertibles de l'anell $\mathbb{Z}/n\mathbb{Z}$.

Definició 1.4.5. S'anomenen caràcters de Dirichlet mòdul n els caràcters (complexos) de $G(n)$.

Sigui χ un caràcter de Dirichlet mòdul n. Per a tot múltiple m de n disposem d'un morfisme exhaustiu de grups $G(m)\xrightarrow{red}G(n)$ donat per reducció i, per tant, podem pensar χ com un caràcter de Dirichlet mòdul m en la forma $G(m)\xrightarrow{red}G(n)\longrightarrow\mathbb{C}^*$.

Proposició 1.4.6. *Sigui $\chi:G(n)\longrightarrow\mathbb{C}^*$ un caràcter de Dirichlet mòdul n. Suposem que existeixen dos divisors de n, d_1 i d_2, tals que χ és la composició de cada un dels morfismes de reducció $G(n)\xrightarrow{red}G(d_i)$ amb un caràcter de Dirichlet $\chi_i:G(d_i)\longrightarrow\mathbb{C}^*$. Sigui d el màxim comú divisor de d_1 i d_2. Aleshores, existeix un caràcter de Dirichlet mòdul d, χ', tal que χ és la composició de χ' amb el morfisme de reducció $G(n)\xrightarrow{red}G(d)$.*

Demostració: És senzill veure que podem suposar que n divideix el producte d_1d_2 (o, si es vol, que n és el mínim comú múltiple de d_1 i d_2). Amb aquesta hipòtesi, com que χ_i està definit mòdul d_i, per a tot nombre enter a primer amb n i tal que $a\equiv 1\pmod{d_i}$ és $\chi(a)=\chi_i(a)=1$. Cal veure que si $a\equiv 1\pmod{d}$ i a és primer amb n, aleshores $\chi(a)=1$. Però el subgrup de $G(n)$ generat per la reunió dels subgrups $\{a\in G(n):\ a\equiv 1\pmod{d_i}\}$, $i=1,2$, és el subgrup $\{a\in G(n):\ a\equiv 1\pmod{d}\}$. En efecte, si escrivim $d=\lambda_1d_1+\lambda_2d_2$, i si $a=1+\alpha d$, obtenim que $a=1+\alpha\lambda_1d_1+\alpha\lambda_2d_2=(1+\alpha\lambda_1d_1)(1+\alpha\lambda_2d_2)-\alpha^2\lambda_1\lambda_2d_1d_2\equiv(1+\alpha\lambda_1d_1)(1+\alpha\lambda_2d_2)\pmod{n}$; i si a és primer amb n, també $1+\alpha\lambda_id_i$ ha de ser primer amb n. Com que χ és trivial sobre cada un dels subgrups $\{a\in G(n):\ a\equiv 1\pmod{d_i}\}$, χ ha de ser trivial sobre el subgrup $\{a\in G(n):\ a\equiv 1\pmod{d}\}$. Això acaba la demostració. □

Corol·lari 1.4.7. *Sigui χ un caràcter de Dirichlet mòdul n. Existeix el menor nombre enter f divisor de n tal que χ és la composició d'un caràcter de Dirichlet mòdul f amb el morfisme de reducció $G(n) \xrightarrow{red} G(f)$.* □

Definició 1.4.8. Aquest menor nombre enter f s'anomena el conductor del caràcter χ. Els caràcters de Dirichlet mòdul n de conductor exactament n s'anomenen caràcters de Dirichlet primitius mòdul n.

Sovint convé pensar els caràcters de Dirichlet mòdul n com a aplicacions de $\mathbb{Z}/n\mathbb{Z}$ i, fins i tot, com a aplicacions de $\mathbb{Z}$. Això es pot fer estenent a $\mathbb{Z}/n\mathbb{Z}$ l'aplicació $\chi : G(n) \longrightarrow \mathbb{C}^*$ per la fórmula $\chi(a) := 0$ si $a \in \mathbb{Z}/n\mathbb{Z}$ no és invertible; i s'estén a $\mathbb{Z}$ simplement component amb l'aplicació de reducció $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, de manera que $\chi(a) = 0$ per a tot nombre enter a tal que $\mathrm{mcd}(a, n) > 1$. Si es considera el cas en què χ és primitiu, aleshores la igualtat $\chi(a) = 0$ es produeix "tan poc sovint" com és possible; només quan a té factors primers comuns amb el conductor. Quan parlem d'un caràcter de Dirichlet sense especificar el seu conductor ni el seu mòdul de definició el considerarem sempre primitiu.

Així, només hi ha un caràcter de Dirichlet que sigui trivial, χ_1, que val 1 sobre tots els nombres enters; és el caràcter de conductor 1.

Podem multiplicar caràcters de Dirichlet. En efecte, si χ_1, χ_2 són caràcters de Dirichlet de conductors f_1, f_2, podem definir el caràcter producte $\chi_1\chi_2$ de la manera següent: considerem, en primer lloc, el morfisme de grups $\omega : G(\mathrm{mcm}(f_1, f_2)) \longrightarrow \mathbb{C}^*$ definit per $\omega(a) := \chi_1(a)\chi_2(a)$. Aleshores, ω és un caràcter de Dirichlet i definim $\chi_1\chi_2$ com el caràcter primitiu associat a ω. Això permet parlar del grup dels caràcters de Dirichlet, grup que té com a element neutre el caràcter trivial. A més a més, l'invers d'un caràcter χ és el que s'obté en compondre χ amb la conjugació complexa $\mathbb{C}^* \longrightarrow \mathbb{C}^*$; en efecte, per a tota arrel de la unitat, $\zeta \in \mathbb{C}$, se satisfà que $\overline{\zeta} = \zeta^{-1}$, on la barra indica el nombre complex conjugat. En particular, un caràcter i el seu invers tenen el mateix conductor.

Exercici 1.4.9. Siguin χ_1, χ_2 caràcters primitius de Dirichlet de conductors respectius f_1 i f_2. Suposem que $\mathrm{mcd}(f_1, f_2) = 1$. Aleshores, el producte $\chi_1\chi_2$ és un caràcter de Dirichlet de conductor $f_1 f_2$.

1.5 Símbol de Legendre

Un dels exemples més importants de caràcter de Dirichlet el proporciona l'estudi dels quadrats dels cossos finits $\mathbb{F}_p$, p primer senar.

L'aplicació $\left(\frac{*}{p}\right) : {\mathbb{F}_p}^* \longrightarrow \{\pm 1\} \subset \mathbb{C}^*$ definida per $\left(\frac{a}{p}\right) := 1$ si a és el quadrat d'un element de ${\mathbb{F}_p}^*$, $\left(\frac{a}{p}\right) = -1$ si a no és un quadrat en ${\mathbb{F}_p}^*$, és un morfisme de grups. S'anomena el símbol de Legendre i és un caràcter quadràtic de Dirichlet de conductor p (cf. per exemple, [Tra 1998]).

En efecte, el nucli d'aquest morfisme és el subgrup dels quadrats de ${\mathbb{F}_p}^*$; per tant, un subgrup d'índex 2 (el morfisme $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^{*2}$ d'elevar al quadrat té nucli $\{\pm 1\}$, de cardinal 2, si $p \neq 2$). En conseqüència, el símbol de Legendre $\left(\frac{*}{p}\right)$ no és el caràcter trivial i està

definit mòdul un primer p; això implica que el seu conductor és p. I, clarament, el quadrat d'aquest caràcter és el caràcter trivial.

Això es tradueix en les propietats següents per al símbol de Legendre:

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

$\left(\frac{a^2}{p}\right) = 1$, si a és un nombre enter no divisible per p; i

$\left(\frac{a}{p}\right) = 0$, si a és divisible per p.

Proposició 1.5.1 (Criteri d'Euler)**.** *Sigui p un nombre primer senar. Per a tot nombre enter a se satisfà la congruència* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Demostració: Sigui $b \in \overline{\mathbb{F}}_p$ un element tal que $b^2 = a$ (en $\overline{\mathbb{F}}_p$). Com que els elements de $\mathbb{F}_p{}^*$ són les arrels del polinomi $X^{p-1} - 1$ en $\overline{\mathbb{F}}_p$, tenim que $a^{p-1} = 1$ i que $a^{\frac{p-1}{2}} = \pm 1$. Per tant, dir que a és un quadrat de $\mathbb{F}_p$ és equivalent a dir que $b^{p-1} = 1$; però $b^{p-1} = 1$ equival a $a^{\frac{p-1}{2}} = 1$. Per tant, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. □

Corol·lari 1.5.2. *Sigui p un natural primer senar. Aleshores:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Demostració: La qüestió relativa al símbol $\left(\frac{-1}{p}\right)$ és immediata. D'altra banda, podem considerar $\zeta \in \overline{\mathbb{F}}_p$ una arrel primitiva d'ordre 8 de la unitat i posar $b := \zeta + \zeta^{-1}$. Com que $\zeta^4 = -1$, tenim que $\zeta^2 + \zeta^{-2} = 0$ i $b^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2$. Per tant, $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = b^{p-1}$. A més a més, com que estem treballant en un cos de característica p i ζ és d'ordre 8, disposem de la igualtat $b^p = \zeta^p + \zeta^{-p} = \zeta^r + \zeta^{-r}$, on r és un nombre enter tal que $r \equiv p \pmod 8$. Si $r = \pm 1$, aleshores $b^p = \zeta + \zeta^{-1} = b$, d'on $b^{p-1} = 1$. I si $r = \pm 5$, aleshores $b^p = \zeta^5 + \zeta^{-5} = -(\zeta + \zeta^{-1}) = -b$, d'on $b^{p-1} = -1$. Això acaba la demostració. □

1.6 Sumes de Gauss

Considerem un caràcter de Dirichlet que sigui primitiu mòdul n, χ, una arrel primitiva n-èsima de la unitat, ζ, i un nombre enter arbitrari, N.

Definició 1.6.1. Anomenarem N-èsima suma de Gauss per a χ relativa a ζ l'element de $\mathbb{Q}(\zeta)$ donat per l'expressió

$$G(\chi, N) := \sum_{a \mod n} \chi(a)\zeta^{aN}.$$

Quan l'arrel de la unitat considerada sigui $\zeta := \exp(\frac{2\pi i}{n})$ parlarem de la suma de Gauss normalitzada i la denotarem $g(\chi, N)$.

El càlcul de la N-èsima suma de Gauss es pot reduir al de la primera.

Proposició 1.6.2. *Siguin χ un caràcter de Dirichlet, primitiu mòdul n, i ζ una arrel primitiva n-èsima de la unitat. Aleshores, per a tot nombre enter N se satisfà la igualtat*

$$G(\chi, N) = \overline{\chi(N)} G(\chi, 1),$$

on $\overline{\chi(N)}$ indica el nombre complex conjugat de $\chi(N)$.

Demostració: Suposem, en primer lloc, que $\mathrm{mcd}(N, n) = 1$. En aquest cas, N és invertible mòdul n i podem escriure la igualtat

$$G(\chi, N) = \sum_{a \mod n} \chi(aNN^{-1})\zeta^{aN};$$

com que χ és multiplicatiu i $\chi(N^{-1}) = \overline{\chi(N)}$, encara la podem escriure en la forma $G(\chi, N) = \sum_{a \mod n} \overline{\chi(N)}\chi(aN)\zeta^{aN}$; i com que la multiplicació per N en el conjunt $(\mathbb{Z}/n\mathbb{Z})^*$ és una aplicació bijectiva, obtenim la igualtat que volíem veure: $G(\chi, N) = \overline{\chi(N)} G(\chi, 1)$.

Considerem ara el cas contrari. Sigui $d := \mathrm{mcd}(N, n) > 1$ i escrivim $N = N'd$, $n = n'd$, de manera que $\mathrm{mcd}(N', n') = 1$. Com que $\chi(N) = 0$, és suficient veure que $G(\chi, N) = 0$. Podem escriure la igualtat $G(\chi, N) = \sum_{a \mod n} \chi(a)\zeta^{adN'}$. Podem suposar que $0 \leq a < n$ i fer la divisió entera de a per n' en la forma $a = n'q + r$, de manera que $0 \leq r < n'$ i $0 \leq q < d$. Això dóna la igualtat $G(\chi, N) = \sum_{r \mod n'} \zeta^{rdN'} \sum_{q \mod d} \chi(n'q + r)$, ja que $\zeta^{n'qdN'} = 1$.

Com que χ és un caràcter primitiu mòdul n, no pot ser que el nucli del morfisme de reducció $G(n) \xrightarrow{red} G(n')$ estigui inclòs en el nucli de χ; per tant, existeix un element $c \in G(n)$, $c \equiv 1 \pmod{n'}$, tal que $\chi(c) \neq 1$. Aleshores, per a cada valor fix de r el subconjunt de $G(n)$ format pels elements $cn'q + cr$ amb $0 \leq q < d$ és el mateix que el format pels elements $n'q + r$ i, per tant, s'obté la igualtat $\sum_{q \mod d} \chi(n'q + r) = \sum_{q \mod d} \chi(cn'q + cr)$, de la qual es dedueix que $G(\chi, N) = \sum_{r \mod n'} \zeta^{rdN'} \sum_{q \mod d} \chi(n'q + r) = \sum_{r \mod n'} \zeta^{rdN'} \sum_{q \mod d} \chi(cn'q + cr) = \chi(c)G(\chi, N)$; i, com que $\chi(c) \neq 1$, que $G(\chi, N) = 0$. □

El resultat següent ens dóna informació sobre el valor de les sumes de Gauss.

Proposició 1.6.3. *Sigui χ un caràcter de Dirichlet primitiu mòdul n i sigui ζ una arrel n-èsima primitiva de la unitat. Aleshores, per a tot nombre enter N primer amb n se satisfà la igualtat $|G(\chi, N)| = \sqrt{n}$.*

Demostració: Com que $\mcd(N,n)=1$, podem escriure $|G(\chi,N)|=|G(\chi,1)|$. Calculem:

$$|G(\chi,1)|^2 = G(\chi,1)\overline{G(\chi,1)} = G(\chi,1)\sum_{a \bmod n}\overline{\chi(a)}\zeta^{-a} = \sum_{a \bmod n} G(\chi,a)\zeta^{-a}$$
$$= \sum_{a \bmod n}\sum_{b \bmod n}\chi(b)\zeta^{a(b-1)} = \sum_{b \bmod n}\chi(b)\sum_{a \bmod n}\zeta^{a(b-1)}.$$

Si $b \not\equiv 1 \pmod n$, aleshores $\displaystyle\sum_{a \bmod n}\zeta^{a(b-1)} = 0$, ja que és la suma dels n primers termes d'una progressió geomètrica de raó $\zeta^{b-1} \neq 1$ i tal que el producte de l'últim terme per la raó és igual al primer terme. I si $b \equiv 1 \pmod n$, aleshores $\zeta^{a(b-1)} = 1$, de manera que obtenim la igualtat $|G(\chi,1)|^2 = \chi(1)n = n$. □

Per al cas dels caràcters quadràtics podem afinar una mica més. En efecte, el resultat següent ens serà d'utilitat a la secció següent.

Corol·lari 1.6.4. *Suposem que χ és un caràcter quadràtic de Dirichlet, primitiu mòdul n. Aleshores, $G(\chi,1)^2 = \chi(-1)n$.*

Demostració: De nou podem calcular

$$G(\chi,1)^2 = G(\chi,1)\sum_{a \bmod n}\chi(a)\zeta^a = \sum_{a \bmod n} G(\chi,a)\zeta^a,$$

ja que $\chi(a) = \overline{\chi(a)}$. Per tant,

$$G(\chi,1)^2 = \sum_{a \bmod n}\sum_{b \bmod n}\chi(b)\zeta^{a(b+1)} = \sum_{b \bmod n}\chi(b)\sum_{a \bmod n}\zeta^{a(b+1)}.$$

Podem repetir el raonament de la proposició anterior canviant $b-1$ per $b+1$ i obtindrem la igualtat buscada. □

1.7 Cossos quadràtics

Sigui $K|\mathbb{Q}$ una extensió quadràtica; és a dir, de grau $[K:\mathbb{Q}]=2$. Si x és un element de K i no és racional, aleshores $K=\mathbb{Q}(x)$ i x és arrel d'una equació irreductible de grau 2 de coeficients racionals. Si escrivim aquesta equació en la forma $aX^2+bX+c=0$, $a,b,c\in\mathbb{Q}$, obtenim que x és un dels dos nombres algebraics $\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$. Com que a i b són nombres racionals, $\mathbb{Q}(x)=\mathbb{Q}(\sqrt{b^2-4ac})$. En treure denominadors, obtenim que K és de la forma $\mathbb{Q}(\sqrt{D})$, on D és un nombre enter lliure de quadrats; és a dir, $D=-1$ o bé $\pm D$ és un producte de nombres primers diferents.

Clarament, l'extensió $K|\mathbb{Q}$ és una extensió de Galois abeliana i, segons el teorema de Kronecker-Weber, ha d'haver-hi una arrel de la unitat, ζ, tal que $\sqrt{D}\in\mathbb{Q}(\zeta)$. L'objectiu d'aquesta secció és demostrar aquest fet.

Per a això, comencem considerant un nombre primer senar p i una arrel primitiva p-èsima de la unitat ζ. El primer pas consisteix a trobar les subextensions quadràtiques de $\mathbb{Q}(\zeta)|\mathbb{Q}$.

Proposició 1.7.1. *Sigui* $S := \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\zeta^a$ *la primera suma de Gauss per al caràcter de Legendre* $\left(\frac{*}{p}\right)$. *Aleshores,* $S^2 = \left(\frac{-1}{p}\right)p$.

DEMOSTRACIÓ: Només cal aplicar el darrer corol·lari de la secció anterior al caràcter de Legendre mòdul p. □

Definició 1.7.2. Sigui p un natural primer senar. Escriurem $p^* := \left(\frac{-1}{p}\right)p$. Observem que sempre és $p^* \equiv 1 \pmod 4$.

Corol·lari 1.7.3. *Siguin* p *un nombre primer senar i* $\zeta \in \mathbb{C}$ *una arrel primitiva* p*-èsima de la unitat. Aleshores* $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta)$. □

Així, per als cossos quadràtics $\mathbb{Q}(\sqrt{p^*})$ se satisfà el teorema de Kronecker-Weber.

D'altra banda, és clar que $i = \sqrt{-1}$ és una arrel quarta primitiva de la unitat, de manera que per a $\mathbb{Q}(i)$ se satisfà el teorema de Kronecker-Weber. A més a més, com que $\mathbb{Q}(\sqrt{-p^*})$ és un subcòs de la composició dels dos cossos $\mathbb{Q}(\sqrt{p^*})$ i $\mathbb{Q}(i)$, i com que la composició de cossos ciclotòmics és un cos ciclotòmic, per a les extensions quadràtiques $\mathbb{Q}(\sqrt{\pm p})|\mathbb{Q}$, on p és un nombre primer senar, se satisfà el teorema de Kronecker-Weber.

D'altra banda, el nombre complex $\zeta_8 := \dfrac{1+i}{\sqrt{2}}$ és una arrel primitiva 8-èsima de la unitat, de manera que, com que $i \in \mathbb{Q}(\zeta_8)$, també $\sqrt{2}$ i $\sqrt{-2}$ són elements de $\mathbb{Q}(\zeta_8)$ i per als cossos $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{-2})$ se satisfà el teorema.

Finalment, si $D = \pm p_1 p_2 \dots p_r$ és la descomposició de D en nombres primers, se satisfà que $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \sqrt{p_2^*}, \dots, \sqrt{p_r^*})$. I com que per a cadascun dels cossos $\mathbb{Q}(\sqrt{p_i^*})$ se satisfà el teorema, això mateix succeeix amb el cos $\mathbb{Q}(\sqrt{D})$.

Dit d'una altra manera, hem demostrat el següent

Teorema 1.7.4. *Sigui* D *un nombre enter lliure de quadrats. Aleshores* $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta)$ *on* ζ *és una arrel primitiva* $4|D|$*-èsima de la unitat.* □

1.8 Congruències quadràtiques

Tal com l'hem definit, el símbol de Legendre dóna informació sobre la resolubilitat de congruències quadràtiques mòdul un nombre primer senar p. En efecte, la congruència $ax^2+bx+c \equiv 0 \pmod p$, $a \not\equiv 0 \pmod p$, té solució quan el seu discriminant, $\Delta := b^2-4ac$, és un quadrat mòdul p; és a dir, quan $\left(\frac{\Delta}{p}\right) \neq -1$. Encara més, el nombre de solucions de la congruència és $1 + \left(\frac{\Delta}{p}\right)$.

Podríem preguntar-nos què succeeix quan canviem el primer p per un nombre enter qualsevol $N > 1$. En aquest cas, encara ens pot ajudar el símbol de Legendre. Considerem una congruència quadràtica

$$ax^2 + bx + c \equiv 0 \pmod N. \tag{1.8.1}$$

Sigui $N = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$ la descomposició de N en factors primers diferents p_i, i suposem que el coeficient dominant a no és divisible per cap dels primers p_i. Si la congruència (1.8.1) té solució, aleshores

$$ax^2 + bx + c \equiv 0 \pmod{p_i^{n_i}} \tag{1.8.2}$$

té solució per a cada valor de i; recíprocament, el teorema xinès del residu ens permet assegurar que si la congruència (1.8.2) té exactament k_i solucions diferents mòdul $p_i^{n_i}$, aleshores la congruència (1.8.1) té exactament $k_1 k_2 \dots k_r$ solucions diferents mòdul N. De manera que el problema consisteix a determinar el nombre de solucions de cada una de les congruències (1.8.2). Per tant, reduïm la dificultat del problema a la resolució de congruències de la forma

$$ax^2 + bx + c \equiv 0 \pmod{p^n} \tag{1.8.3}$$

on p és un nombre primer, a no és divisible per p i n és un natural qualsevol.

Proposició 1.8.1. *Siguin p un nombre primer (que pot ser 2), $f(X) := aX^2 + bX + c$ un polinomi de coeficients enters a, b, c, tal que a no és divisible per p, i suposem que un nombre enter $x = x_1$, $0 \leq x < p$, és una solució simple, mòdul p, de la congruència $f(X) \equiv 0 \pmod{p}$. Aleshores, per a tot nombre enter $n \geq 2$ existeix un nombre enter x_n, $0 \leq x_n < p^n$, i només un tal que $x_n \equiv x_{n-1} \pmod{p^{n-1}}$ i $f(x_n) \equiv 0 \pmod{p^n}$.*

Demostració: Farem la demostració per inducció sobre n. El cas $n = 1$ és la hipòtesi. Suposem que x_n és un nombre enter per al qual se satisfan les condicions de l'enunciat. Escrivim $f(x_n) = p^n z_n$; com que volem que $x_{n+1} \equiv x_n \pmod{p^n}$, cal determinar tots els valors de α_n, definits mòdul p, de manera que per a $x_{n+1} := x_n + \alpha_n p^n$ se satisfaci que $f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Ara bé, per a tot x_{n+1} de la forma $x_n + \alpha_n p^n$ se satisfà la congruència $f(x_{n+1}) \equiv z_n p^n + f'(x_n)\alpha_n p^n \pmod{p^{n+1}}$, de manera que demostrar que $f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}$ equival a demostrar que $z_n + f'(x_n)\alpha_n \equiv 0 \pmod{p}$. D'altra banda, l'arrel x de $f(X) \equiv 0 \pmod{p}$ és simple si, i només si, $f'(x) \not\equiv 0 \pmod{p}$; així, per hipòtesi d'inducció, $f'(x_n) \equiv f'(x) \not\equiv 0 \pmod{p}$. Això ens permet assegurar que la congruència lineal $z_n + f'(x_n)\alpha_n \equiv 0 \pmod{p}$ té exactament una solució α_n, com volíem demostrar. □

Corol·lari 1.8.2. *Siguin p un nombre primer senar i a, b, c nombres enters tals que a no és divisible per p. Si $\left(\dfrac{b^2 - 4ac}{p}\right) = 1$, aleshores, per a cada nombre natural $n \geq 1$, la congruència quadràtica $aX^2 + bX + c \equiv 0 \pmod{p^n}$ té exactament dues solucions $\pmod{p^n}$.* □

Observació 1.8.3. L'única congruència quadràtica mòdul 2 que té arrels simples mòdul 2 és la congruència $X^2 + X \equiv 0 \pmod{2}$. Per tant, si una congruència quadràtica mòdul 2^n redueix a la congruència $X^2 + X \equiv 0 \pmod{2}$, aleshores té exactament dues solucions $\pmod{2^n}$ per a tot nombre enter n.

D'aquesta manera, obtenim un criteri senzill per a saber el nombre de solucions de totes les congruències $f(X) := aX^2 + bX + c \equiv 0 \pmod{N}$ tals que $\mathrm{mcd}(a, N) = 1$ i $f(X)$ és separable $\pmod{p}$ per a tot nombre primer p que divideix N.

1.9 Llei de reciprocitat quadràtica

Un dels resultats de teoria de nombres del qual s'han publicat més demostracions diferents i que encara avui és objecte d'estudi és la llei de reciprocitat quadràtica. L'objeciu d'aquesta secció és donar-ne una demostració. Per a això, convindrà considerar certes sumes de Gauss en característica senar ℓ.

Hem vist més amunt que si p és un nombre primer senar, considerem una arrel primitiva p-èsima de la unitat $\zeta \in \mathbb{C}$ i posem $S := \sum_{a \mod p} \left(\frac{a}{p}\right)\zeta^a$, aleshores és $S^2 = \left(\frac{-1}{p}\right)p$. Aquest resultat també és vàlid si canviem $\mathbb{C}$ per $\overline{\mathbb{F}}_\ell$, per a qualsevol nombre primer senar $\ell \neq p$.

En efecte, repetim el càlcul:

$$\begin{aligned} S^2 &= \sum_{a \mod p} \sum_{b \mod p} \left(\frac{ab}{p}\right)\zeta^{a+b} = \sum_{a\neq 0 \mod p} \sum_{b \mod p} \left(\frac{ab}{p}\right)\zeta^{a+b} = \\ &= \sum_{a\neq 0 \mod p} \sum_{c \mod p} \left(\frac{a^2c}{p}\right)\zeta^{a(1+c)} = \sum_{a\neq 0 \mod p} \sum_{c \mod p} \left(\frac{c}{p}\right)\zeta^{a(1+c)} = \\ &= \sum_{c \mod p} \left(\frac{c}{p}\right) \sum_{a\neq 0 \mod p} \zeta^{a(1+c)}. \end{aligned}$$

Si $1 + c \not\equiv 0 \pmod p$, aleshores ζ^{1+c} és encara una arrel primitiva p-èsima de la unitat en $\overline{\mathbb{F}}_\ell$ i $\sum_{a\neq 0 \mod p} \zeta^{a(1+c)} = -1$; i si $1 + c \equiv 0 \pmod p$, aleshores $\sum_{a\neq 0 \mod p} \zeta^{a(1+c)} = p - 1$. Això fa que

$$S^2 = -\sum_{1+c\neq 0 \mod p} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1) = \left(\frac{-1}{p}\right)p.$$

Lema 1.9.1. *Amb les notacions anteriors se satisfà la fórmula* $S^{\ell-1} = \left(\frac{\ell}{p}\right)$.

Demostració: Com que treballem en característica senar ℓ, podem escriure que

$$S^\ell = \sum_{a \mod p} \left(\frac{a}{p}\right)\zeta^{a\ell} = \sum_{a \mod p} \left(\frac{a\ell^{-1}}{p}\right)\zeta^a = \left(\frac{\ell^{-1}}{p}\right) \sum_{a \mod p} \left(\frac{a}{p}\right)\zeta^a = \left(\frac{\ell}{p}\right)S.$$

I com que $S^2 \neq 0$, podem simplificar S i obtenim la igualtat cercada. □

Teorema 1.9.2. (Llei de reciprocitat quadràtica) *Siguin p, ℓ nombres primers senars. Aleshores,* $\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$.

Demostració: Si $\ell = p$ el resultat és trivial. D'altra banda, recordem que si tenim un nombre enter a, i si $z \in \overline{\mathbb{F}}_\ell$ és tal que $z^2 = a$, aleshores $\left(\frac{a}{\ell}\right) = z^{\ell-1}$. Podem aplicar aquest

fet per a calcular el símbol de Legendre $\left(\dfrac{\left(\dfrac{-1}{p}\right)p}{\ell}\right)$ en el cas que $\ell \neq p$ en la forma

$$\left(\frac{\left(\frac{-1}{p}\right)p}{\ell}\right) = S^{\ell-1} = \left(\frac{\ell}{p}\right).$$

Però sabem que $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, de manera que obtenim la igualtat

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right)$$

que volíem demostrar. □

Més endavant veurem una altra demostració d'aquest teorema.

Una aplicació immediata de la llei de reciprocitat quadràtica és el càlcul efectiu del símbol de Legendre. En efecte, la millor manera de veure-ho és en un exemple. Suposem que volem calcular el símbol

$$\left(\frac{34569284994927}{1602961}\right).$$

El primer que cal fer és calcular el residu de 34569284994927 mòdul el nombre, primer, 1602961; això dóna sense cap dificultat que

$$\begin{aligned}\left(\frac{34569284994927}{1602961}\right) &= \left(\frac{1188715}{1602961}\right) = \left(\frac{5\cdot 11\cdot 21613}{1602961}\right) = \\ &= \left(\frac{5}{1602961}\right)\left(\frac{11}{1602961}\right)\left(\frac{21613}{1602961}\right).\end{aligned}$$

Apliquem la llei de reciprocitat quadràtica. Com que $1602961 \equiv 1 \pmod 4$, els factors $(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$ són trivials i podem escriure que

$$\begin{aligned}\left(\frac{34569284994927}{1602961}\right) &= \left(\frac{1602961}{5}\right)\left(\frac{1602961}{11}\right)\left(\frac{1602961}{21613}\right) = \\ &= \left(\frac{1}{5}\right)\left(\frac{8}{11}\right)\left(\frac{3599}{21613}\right).\end{aligned}$$

Ara, $\left(\dfrac{1}{5}\right) = 1$ i $\left(\dfrac{8}{11}\right) = \left(\dfrac{2}{11}\right) = -1$, ja que $8 = 2\cdot 2^2$ i $11 \equiv 3 \pmod 8$; com que $3599 = 59\cdot 61$, obtenim que

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{59}{21613}\right)\left(\frac{61}{21613}\right) = -\left(\frac{21613}{59}\right)\left(\frac{21613}{61}\right),$$

ja que $21613 \equiv 1 \pmod 4$. Finalment, $21613 \equiv 19 \pmod{59}$ i $21613 \equiv 19 \pmod{61}$; per tant:

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{19}{59}\right)\left(\frac{19}{61}\right) = \left(\frac{59}{19}\right)\left(\frac{61}{19}\right),$$

ja que $59 \equiv 19 \equiv 3 \pmod 4$; i, com que $19 \equiv 3 \pmod 8$, és

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{2}{19}\right)\left(\frac{4}{19}\right) = \left(\frac{2}{19}\right) = -1.$$

1.10 Símbol de Jacobi

El símbol de Legendre està associat a un primer senar p. A fi d'evitar la descomposició en factors primers en el càlcul d'aquest símbol, introduirem el símbol de Jacobi.

Sigui P un nombre enter positiu senar. Per a tot nombre enter a, definim el símbol de Jacobi $\left(\frac{a}{P}\right)$ de la manera següent:

sigui $P := p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$ la descomposició de P en factors primers. Cada un dels nombres p_i és un primer senar i podem definir

$$\left(\frac{a}{P}\right) := \left(\frac{a}{p_1}\right)^{n_1}\left(\frac{a}{p_2}\right)^{n_2} \dots \left(\frac{a}{p_r}\right)^{n_r}.$$

El símbol definit d'aquesta manera s'anomena el símbol de Jacobi i se satisfan les propietats següents:

(1) si $\mathrm{mcd}(a, P) > 1$, aleshores $\left(\frac{a}{P}\right) = 0$;

(2) si $\mathrm{mcd}(a, P) = 1$, aleshores $\left(\frac{a}{P}\right) = \pm 1$;

(3) si P_1, P_2, P són nombres enters positius senars i a_1, a_2, a són nombres enters qualssevol, aleshores $\left(\frac{a}{P_1 P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$ i $\left(\frac{a_1 a_2}{P}\right) = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)$; i

(4) si $a \equiv a' \pmod P$, aleshores $\left(\frac{a}{P}\right) = \left(\frac{a'}{P}\right)$.

La demostració d'aquestes propietats és immediata a partir de la definició i de les propietats del símbol de Legendre. A més a més, se satisfà també la llei de reciprocitat quadràtica.

Proposició 1.10.1. *Siguin P_1, P_2 nombres enters positius senars. Aleshores,* $\left(\frac{P_1}{P_2}\right) = (-1)^{\frac{P_1-1}{2}\frac{P_2-1}{2}}\left(\frac{P_2}{P_1}\right)$.

Demostració: Per a fer la demostració només cal factoritzar P_1 i P_2 i aplicar la llei de reciprocitat quadràtica per al símbol de Legendre. El resultat final es dedueix del següent.

Lema 1.10.2. *Sigui $P := p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$ la descomposició com a producte de nombres primers d'un nombre enter senar P. Posem $\varepsilon(P) := \frac{P-1}{2}$. Aleshores,*

$$(-1)^{\varepsilon(P)} = \prod_i (-1)^{\varepsilon(p_i) n_i}.$$

DEMOSTRACIÓ: Si P_1, P_2 són nombres enters senars, aleshores se satisfà la igualtat $(P_1-1)(P_2-1) = P_1P_2 - P_1 - P_2 + 1 = (P_1P_2-1) - (P_1-1) - (P_2-1)$, i com que $(P_1-1)(P_2-1) \equiv 0 \pmod 4$, s'obté que $P_1P_2 - 1 \equiv (P_1-1) + (P_2-1) \pmod 4$; per tant, $(-1)^{\varepsilon(P_1P_2)} = (-1)^{\varepsilon(P_1)}(-1)^{\varepsilon(P_2)}$. □

Aquest mateix lema ens permet escriure el valor del símbol $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

De manera anàloga, tenim que $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$, ja que si $\omega(P) := \frac{P^2-1}{8}$, aleshores $(-1)^{\omega(P_1P_2)} = (-1)^{\omega(P_1)}(-1)^{\omega(P_2)}$.

En efecte. Com que P_i és senar, és $P_i^2 \equiv 1 \pmod 8$; i com que $(P_1^2-1)(P_2^2-1) = (P_1P_2)^2 - 1 - (P_1^2-1) - (P_2^2-1)$, tenim que $(P_1P_2)^2 - 1 \equiv (P_1^2-1) + (P_2^2-1) \pmod{8^2}$; per tant, $(-1)^{\omega(P_1P_2)} = (-1)^{\omega(P_1)}(-1)^{\omega(P_2)}$.

El símbol de Jacobi permet simplificar el càlcul dels símbols de Legendre. Clarament, si P és un nombre primer senar, per a tot nombre enter a el símbol de Jacobi i el de Legendre $\left(\frac{a}{P}\right)$ coincideixen. Per tant, podem evitar la descomposició en primers en el càlcul del símbol de Legendre: només cal separar els factors 2 del numerador abans d'invertir el símbol.

Veiem-ho, com a la secció anterior, en el càlcul de

$$\left(\frac{34569284994927}{1602961}\right).$$

Igual que abans, obtenim que

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1188715}{1602961}\right).$$

Aplicant la llei de reciprocitat quadràtica,

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1602961}{1188715}\right),$$

i, reduint el numerador mòdul el denominador,

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{414246}{1188715}\right).$$

Ara tenim dues possibilitats. O bé separar els factors 2 del numerador i calcular el símbol de Jacobi $\left(\frac{2}{1188715}\right)$ si el nombre de factors 2 que hem pogut treure és senar, o bé restar el denominador del numerador i calcular el símbol $\left(\frac{-1}{1188715}\right)$ a fi d'obtenir un símbol amb numerador i denominador senars positius. Ho farem de la primera forma, ja que això produirà un numerador més petit i, per tant, els càlculs posteriors es faran amb nombres de menys xifres. Això dóna

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{207123}{1188715}\right),$$

ja que $1188715 \equiv 3 \pmod 8$. Com que $1188715 \equiv 207123 \equiv 3 \pmod 4$, la llei de reciprocitat dóna

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1188715}{207123}\right) = \left(\frac{153100}{207123}\right).$$

Ara és clar un factor 10^2 en el numerador, i 5 no divideix el denominador; per tant, podem eliminar aquest factor i obtenim que

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1531}{207123}\right) = -\left(\frac{207123}{1531}\right),$$

ja que $207123 \equiv 1531 \equiv 3 \pmod 8$. En reduir de nou:

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{438}{1531}\right) = -\left(\frac{2}{1531}\right)\left(\frac{219}{1531}\right) = \left(\frac{219}{1531}\right).$$

I en reiterar el procés:

$$\begin{aligned}\left(\frac{34569284994927}{1602961}\right) &= -\left(\frac{1531}{219}\right) = -\left(\frac{217}{219}\right) = \\ &= -\left(\frac{219}{217}\right) = -\left(\frac{2}{217}\right) = -1.\end{aligned}$$

1.11 Símbol de Kronecker

Un altre exemple molt important de caràcter de Dirichlet és el donat pel símbol de Kronecker. Aquesta secció es dedica a la seva introducció i estudi; més endavant servirà per descriure còmodament les lleis de descomposició dels nombres primers en els cossos quadràtics.

Observem que $(\mathbb{Z}/4\mathbb{Z})^*$ és un grup d'ordre 2; per tant, només hi ha dos caràcters de Dirichlet mòdul 4; un d'ells és el caràcter trivial i l'altre és el caràcter quadràtic $(-1)^{\varepsilon(*)}$, primitiu mòdul 4, definit a la secció anterior en parlar del símbol de Jacobi.

Anàlogament, només hi ha quatre caràcters de Dirichlet mòdul 8. Dos d'ells, no primitius, són els induïts pels caràcters de Dirichlet mòdul 4: el caràcter trivial i el caràcter $(-1)^{\varepsilon(*)}$. Els altres dos també són quadràtics, ja que el grup $(\mathbb{Z}/8\mathbb{Z})^*$ és d'exponent 2; un d'ells és el caràcter $(-1)^{\omega(*)}$, que també ha aparegut en parlar del símbol de Jacobi; l'altre, en conseqüència, és el producte dels altres dos caràcters no trivials: $(-1)^{\varepsilon(*)+\omega(*)}$.

Hem vist, també, que si p és un nombre primer senar, aleshores el caràcter de Legendre $\left(\frac{*}{p}\right)$ és l'únic caràcter quadràtic de conductor p.

Sigui $D' := \ell_1\ell_2\ldots\ell_r$ un producte de nombres naturals primers senars diferents, que pot ser $D' = 1$. El producte dels caràcters de Legendre $\left(\frac{*}{\ell_i}\right)$, és a dir, el caràcter de Jacobi $\left(\frac{*}{D'}\right)$, és un caràcter quadràtic de Dirichlet definit mòdul D', el trivial si $D' = 1$. Si el multipliquem per la potència $\varepsilon(D')$-èsima de l'únic caràcter primitiu mòdul 4, $(-1)^{\varepsilon(*)}$, obtenim un caràcter quadràtic de Dirichlet definit mòdul $4D'$. És el caràcter quadràtic de Dirichlet $\chi_{D'} := (-1)^{\varepsilon(D')\varepsilon(*)}\left(\frac{*}{D'}\right)$ i s'anomena el D'-èsim caràcter de Kronecker.

A partir d'aquest caràcter podem definir tres caràcters més:

$$\chi_{-D'} := (-1)^{\varepsilon(*)}\chi_{D'},$$

$$\chi_{2D'} := (-1)^{\omega(*)}\chi_{D'},$$

$$\chi_{-2D'} := (-1)^{\varepsilon(*)}(-1)^{\omega(*)}\chi_{D'}.$$

Són caràcters quadràtics de Dirichlet definits mòdul $4D'$, $8D'$ i $8D'$, respectivament. S'anomenen els caràcters de Kronecker.

Proposició 1.11.1. *Sigui D un nombre enter lliure de quadrats. Aleshores, χ_D és l'únic caràcter quadràtic de Dirichlet mòdul $4|D|$ tal que per a tot natural primer senar p que no divideix D és $\chi_D(p) = \left(\dfrac{D}{p}\right)$.*

Demostració: Sigui $D' := \ell_1\ell_2\dots\ell_r$ la descomposició en nombres primers de la part positiva senar de D. La llei de reciprocitat quadràtica per al símbol de Jacobi $\left(\dfrac{*}{D'}\right)$ permet demostrar de seguida que per al caràcter de Kronecker χ_D se satisfà la propietat enunciada. En efecte,

$$\chi_{D'}(p) = (-1)^{\varepsilon(D')\varepsilon(p)}\left(\frac{p}{D'}\right) = \left(\frac{D'}{p}\right);$$

per tant, també

$$\chi_{-D'}(p) = (-1)^{\varepsilon(p)}\chi_{D'}(p) = (-1)^{\varepsilon(p)}\left(\frac{D'}{p}\right) = \left(\frac{-D'}{p}\right),$$

$$\chi_{2D'}(p) = (-1)^{\omega(p)}\chi_{D'}(p) = (-1)^{\omega(p)}\left(\frac{D'}{p}\right) = \left(\frac{2D'}{p}\right),$$

i

$$\chi_{-2D'}(p) = (-1)^{\varepsilon(p)}(-1)^{\omega(p)}\chi_{D'}(p) = (-1)^{\varepsilon(p)}(-1)^{\omega(p)}\left(\frac{D'}{p}\right) = \left(\frac{-2D'}{p}\right).$$

Resta demostrar la unicitat.

Per a això, suposem que χ és un caràcter quadràtic de Dirichlet definit mòdul $4|D|$ per al qual se satisfà la propietat i considerem $\psi := \chi\chi_D^{-1}$. Aleshores, ψ és un caràcter de Dirichlet definit mòdul $4|D|$ tal que per a tot natural primer senar p que no divideix D se satisfà que $\psi(p) = 1$. Com que ψ és multiplicatiu, també se satisfà que $\psi(a) = 1$ per a tot nombre natural senar a primer amb D; és a dir, per a tot nombre natural a primer amb $4D$. Això demostra que $\chi = \chi_D$. □

Proposició 1.11.2. *Sigui D un nombre enter lliure de quadrats i sigui D' la part senar positiva de la seva descomposició en producte de nombres primers. El conductor del caràcter de Kronecker χ_D és exactament $4|D|$, excepte en el cas $D \equiv 1 \pmod 4$ en què el conductor és D'.*

Demostració: Com que els caràcters de Legendre $\left(\dfrac{*}{\ell_i}\right)$ són primitius de conductor ℓ_i, el caràcter $\psi := \left(\dfrac{*}{\ell_1}\right)\left(\dfrac{*}{\ell_2}\right)\cdots\left(\dfrac{*}{\ell_r}\right)$ és primitiu de conductor $\ell_1\ell_2\dots\ell_r$. Com que

el caràcter de Kronecker és el producte de ψ per caràcters de conductor potència de 2, només cal estudiar el conductor dels altres factors.

Si $D = D' \equiv 1 \pmod 4$, per a obtenir χ_D es multiplica ψ pel caràcter trivial, ja que $(-1)^{\varepsilon(D)\varepsilon(*)} = 1$. I si $D = -D' \equiv 1 \pmod 4$, també es multiplica ψ pel caràcter trivial, ja que $(-1)^{\varepsilon(D)\varepsilon(*)}(-1)^{\varepsilon(*)} = 1$. En els altres casos, o bé ψ es multiplica pel caràcter primitiu de conductor 4, en el cas $D \equiv 3 \pmod 4$ o bé es multiplica per un dels dos caràcters primitius de conductor 8, en el cas en què D és parell. □

La proposició següent generalitza el fet que els únics caràcters quadràtics de Dirichlet de conductor primer senar són els caràcters de Legendre.

Proposició 1.11.3. *Sigui χ un caràcter quadràtic de Dirichlet, primitiu. Aleshores, existeix un nombre enter D lliure de quadrats tal que χ és el caràcter de Kronecker χ_D, considerat definit mòdul el seu conductor.*

Per a la demostració usarem un seguit de resultats previs.

Lema 1.11.4. *Sigui f el conductor d'un caràcter quadràtic de Dirichlet i suposem que f és senar. Aleshores, f és lliure de quadrats.*

Demostració: Sigui χ un caràcter quadràtic de Dirichlet definit mòdul un nombre senar n i sigui n' el producte dels nombres primers senars diferents que divideixen n. Si demostrem que tots els elements $a \in G(n)$ que satisfan la congruència $a \equiv 1 \pmod{n'}$ són quadrats en $G(n)$, aleshores haurem acabat ja que, per ser χ quadràtic, és $\chi(b) = \pm 1$ per a tot $b \in G(n)$ i, per tant, $\chi(b^2) = 1$; això ens permet assegurar que χ es pot definir mòdul n', de manera que el seu conductor, que és un divisor de n', és lliure de quadrats.

Ara bé, si $a \in G(n)$ és un quadrat mòdul n', ho és mòdul ℓ per a tot nombre primer ℓ que divideix n i, com que el polinomi $X^2 - a$ és separable mòdul ℓ, les congruències $X^2 - a \equiv 0 \pmod{\ell^k}$ tenen solució per a cada valor de k. Per tant, la congruència $X^2 - a \equiv 0 \pmod n$ té solució i a és un quadrat en $G(n)$. □

Lema 1.11.5. *Sigui f el conductor d'un caràcter quadràtic de Dirichlet. Aleshores, f és lliure del factor 2^4.*

Demostració: La demostració és semblant a la del lema anterior. Si $r \geq 3$, aleshores $G(2^r)/G(2^r)^2 \cong G(8) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; per tant, el subgrup dels quadrats de $G(2^r)$ és un subgrup d'índex 4. A més a més, si a és un quadrat de $G(2^r)$, aleshores $a \equiv 1 \pmod 8$. D'altra banda, el subgrup format pels elements $a \in G(2^r)$ tals que $a \equiv 1 \pmod 8$ també és d'índex 4; per tant, els dos subgrups són iguals. Això implica que, en el cas $r \geq 3$, podem abaixar els factors 2^r de n fins a 2^3. □

Lema 1.11.6. *El conductor d'un caràcter de Dirichlet (quadràtic o no) no és mai de la forma $2f$ amb f senar.*

Demostració: Ja que si f és senar, aleshores $G(2f) \cong G(f)$. □

Anem a demostrar, ara, la proposició. Sigui f el conductor del caràcter χ i suposem que f és senar. El grup dels caràcters quadràtics de Dirichlet definits mòdul f és isomorf al grup $G(f)/G(f)^2 \cong (\mathbb{Z}/2\mathbb{Z})^r$, on r és el nombre de factors primers diferents que divideixen f. D'altra banda, els caràcters quadràtics de $G(f)$ que redueixen als caràcters de Legendre

$\left(\frac{*}{\ell}\right)$, per a ℓ primer que divideix f, formen un sistema de generadors lliures del grup dels caràcters quadràtics de $G(f)$; en conseqüència, χ és un producte d'aquests caràcters. Si algun dels caràcters de Legendre no aparegués en aquest producte, el conductor no podria ser f; per tant, χ és el producte d'aquests caràcters de Legendre. I aquest producte és el caràcter de Kronecker χ_D per a $D = \pm f$ amb el signe elegit de manera que χ_D sigui de conductor f.

En el cas que f és exactament divisible per 4, cal afegir el caràcter $(-1)^{\varepsilon(*)}$ en el raonament anterior; això dóna per a χ el caràcter de Kronecker χ_{-D}, amb D elegit igual que abans. I en el cas que f és divisible per 8 cal afegir el caràcter $(-1)^{\omega(*)}$ o el caràcter $(-1)^{\omega(*)}(-1)^{\varepsilon(*)}$. Els detalls es deixen com a exercici. □

Capítol 2

Enters dels cossos de nombres

La riquesa de l'aritmètica de $\mathbb{Z}$ resta (gairebé completament) amagada en punt considerem el seu cos de fraccions, $\mathbb{Q}$. Per tant, si volem estudiar l'aritmètica d'un cos de nombres, K, serà bo cercar algun anell que el tingui com a cos de fraccions i que, alhora, tingui bones propietats de divisibilitat.

Els anells que s'utilitzen usualment són anells que tenen algunes de les bones propietats de divisibilitat de l'anell $\mathbb{Z}$; però, en general, no són anells tan agradables com $\mathbb{Z}$. En qualsevol cas, i llevat que es digui alguna cosa que ho modifiqui, a la teoria general només considerarem anells commutatius.

2.1 Elements enters sobre un anell

L'anell $\mathbb{Z}[i]$ dels nombres enters de Gauss és un dels anells més coneguts dels cursos elementals; els seus elements són els nombres complexos de la forma $a + bi$, on a i b són nombres enters; el seu cos de fraccions és el cos ciclotòmic $\mathbb{Q}(i)$.

Observem que si $\alpha := a+bi$, $a, b \in \mathbb{Z}$, és un nombre enter de Gauss, aleshores $\alpha \in \mathbb{Q}(i)$ i és arrel del polinomi mònic de coeficients enters

$$(X - a)^2 + b^2 = X^2 - 2aX + (a^2 + b^2) \in \mathbb{Z}[X].$$

Recíprocament, si un element $\alpha := a + bi \in \mathbb{Q}(i)$, a, $b \in \mathbb{Q}$, és arrel d'un polinomi mònic de coeficients enters, aleshores és un nombre enter de Gauss; és a dir, a i b són nombres enters.

En efecte; sigui $f(X) \in \mathbb{Z}[X]$ un polinomi mònic i sigui $\alpha := a+bi \in \mathbb{Q}(i)$, $a, b \in \mathbb{Q}$, una arrel de $f(X)$. Com que $f(X)$, en particular, és de coeficients reals, el nombre complex conjugat de α, $\overline{\alpha} := a - bi$, també és una arrel de $f(X)$. Per tant, el polinomi $f(X)$ és divisible per $(X-\alpha)(X-\overline{\alpha}) = (X-a)^2+b^2 \in \mathbb{Q}[X]$. Pel lema de Gauss, aquest polinomi mònic és de coeficients enters; és a dir, $2a \in \mathbb{Z}$ i $a^2 + b^2 \in \mathbb{Z}$. En conseqüència, $(2b)^2 \in \mathbb{Z}$, de manera que $2b \in \mathbb{Z}$. Escrivim $a = A/2$, $b = B/2$, amb A, $B \in \mathbb{Z}$; de $a^2 + b^2 \in \mathbb{Z}$ resulta que $A^2 + B^2 \equiv 0 \pmod 4$; com que en $\mathbb{Z}/4\mathbb{Z}$ la suma de dos quadrats només és nul·la quan els dos quadrats són nuls, ha de ser $A^2 \equiv B^2 \equiv 0 \pmod 4$, de manera que A, $B \in 2\mathbb{Z}$. Això ens assegura que a, $b \in \mathbb{Z}$, com volíem demostrar.

Aquest fet es pot resumir dient que els nombres enters de Gauss són exactament els nombres de $\mathbb{Q}(i)$ que són arrels de polinomis mònics de coeficients enters.

Definició 2.1.1. Sigui B un anell i sigui $A \subseteq B$ un subanell. Un element $b \in B$ s'anomena enter sobre A quan b és arrel d'un polinomi mònic de coeficients en A. L'extensió d'anells $B|A$ s'anomena entera quan tot element de B és enter sobre A.

Una demostració detallada dels resultats següents es pot trobar, per exemple, en [At-McD 73].

Proposició 2.1.2. *Sigui $B|A$ una extensió d'anells i sigui $b \in B$. Les propietats següents són equivalents:*

(a) *b és enter sobre A;*

(b) *l'anell $A[b]$ és un A-mòdul finitament generat;*

(c) *existeix un subanell C de B que conté A i b i que és un A-mòdul finitament generat; i*

(d) *existeix un $A[b]$-mòdul fidel i finitament generat com a A-mòdul.* □

Corol·lari 2.1.3. *Siguin A un anell i $\{a_1, a_2, \ldots, a_n\}$ elements d'un anell extensió $B|A$ tals que per a $0 \leq i < n$ l'element a_{i+1} és enter sobre l'anell $A[a_1, a_2, \ldots, a_i]$. Aleshores, l'anell $A[a_1, a_2, \ldots, a_n]$ és un A-mòdul finitament generat.* □

Corol·lari 2.1.4. *Sigui B un anell i sigui $A \subseteq B$ un subanell. El conjunt dels elements $b \in B$ que són enters sobre A és un subanell de B que conté A.* □

Corol·lari 2.1.5. *Siguin $C|B$ i $B|A$ extensions enteres d'anells. Aleshores, l'extensió $C|A$ és una extensió entera.* □

Definició 2.1.6. Sigui $B|A$ una extensió d'anells. El subanell de B format pels elements que són enters sobre A s'anomena la clausura entera de A en B. Es diu que A és íntegrament tancat en B quan A és la seva pròpia clausura entera en B. Un domini d'integritat A s'anomena íntegrament tancat quan és la seva pròpia clausura entera dins el cos de fraccions.

Ens interessa, sobretot, el cas de dominis d'integritat. Els exemples més senzills d'anells íntegrament tancats els donen els resultats següents.

Proposició 2.1.7. *Sigui $B|A$ una extensió d'anells i sigui C la clausura entera de A en B. Aleshores, C és íntegrament tancat en B.* □

Proposició 2.1.8. *Sigui A un domini factorial. Aleshores, A és íntegrament tancat.* □

Corol·lari 2.1.9. *Sigui A un domini principal. Aleshores, A és íntegrament tancat.* □

Proposició 2.1.10. *Sigui A un domini íntegrament tancat i sigui $S \subseteq A$ un subconjunt multiplicativament tancat de A. Aleshores, l'anell localitzat de A en S, $S^{-1}A$, és íntegrament tancat.* □

És evident que, en el cas d'un cos, una extensió entera és una extensió algebraica. D'altra banda, és un exercici senzill demostrar que si $A \subseteq B$ són dominis i l'extensió $B|A$ és entera, condició necessària i suficient perquè A sigui un cos és que B ho sigui. La propietat següent és útil per a determinar quan un element és enter.

Proposició 2.1.11. *Siguin A un domini d'integritat, K el cos de fraccions de A, $L|K$ una extensió algebraica, $b \in L$ un element qualsevol, i $f(X) := \mathrm{Irr}(b, K)(X)$ el polinomi mònic irreductible de $K[X]$ que té b per arrel. Suposem que A és íntegrament tancat. Aleshores, condició necessària i suficient perquè b sigui enter sobre A és que $f(X) \in A[X]$.*

Demostració: Podem suposar que l'extensió $L|K$ és normal. Sigui $g(X) \in A[X]$ una equació de dependència entera de b sobre A. Com que $f(X)$ és el polinomi irreductible de $K[X]$ de grau més petit que té b per arrel i $g(X)$ és un polinomi de $K[X]$ que té b per arrel, $f(X)$ divideix $g(X)$ en $K[X]$. Això implica que les arrels de $f(X)$ també ho són de $g(X)$, de manera que totes les arrels de $f(X)$ són elements de L enters sobre A. Per tant, els polinomis simètrics elementals d'aquestes arrels són enters sobre A. Però aquests polinomis simètrics elementals són els coeficients de $f(X)$ i, per tant, els coeficients de $f(X)$ són elements de K que són enters sobre A; com que A és íntegrament tancat, el polinomi $f(X)$ és de coeficients en A. □

2.2 Enters dels cossos de nombres

S'anomena cos de nombres tot cos K de característica zero tal que l'extensió $K|\mathbb{Q}$ és finita.

Definició 2.2.1. Un nombre enter algebraic és un element de $\overline{\mathbb{Q}}$ que és enter sobre $\mathbb{Z}$. Si K és un cos de nombres, la clausura entera de $\mathbb{Z}$ en K s'anomena l'anell dels enters de K. És l'anell format per tots els elements de K que són enters algebraics.

El primer objectiu d'aquesta secció és calcular els anells d'enters dels cossos quadràtics. Sigui, doncs, D un nombre enter lliure de quadrats. L'anell $\mathbb{Z}[\sqrt{D}]$ és un subanell del cos quadràtic $K := \mathbb{Q}(\sqrt{D})$ i és enter sobre $\mathbb{Z}$; per tant, si $\mathcal{O}_K$ designa l'anell dels enters del cos K, es té la inclusió $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_K$. El recíproc, però, no és cert en general. En efecte, se satisfà el resultat següent.

Proposició 2.2.2. *Sigui D un nombre enter lliure de quadrats. L'anell dels enters del cos $K := \mathbb{Q}(\sqrt{D})$ és l'anelll $\mathcal{O}_K = \mathbb{Z}[\omega]$, on $\omega = \sqrt{D}$ si $D \not\equiv 1 \pmod 4$ i $\omega = \dfrac{D+\sqrt{D}}{2}$ si $D \equiv 1 \pmod 4$.*

Demostració: La demostració és una generalització directa del càlcul que hem fet per al cas de l'anell $\mathbb{Z}[i]$ dels nombres enters de Gauss. Siguin a, $b \in \mathbb{Q}$ tals que $a + b\sqrt{D} \in \mathcal{O}_K$. El conjugat galoisià $a - b\sqrt{D}$ de $a + b\sqrt{D}$ també és un enter de K, de manera que la suma i el producte d'aquests dos elements són enters de K. Però són racionals i, com que $\mathbb{Z}$ és íntegrament tancat, són enters. Això ens permet assegurar que $2a$, $a^2 - Db^2 \in \mathbb{Z}$. Per tant, $4a^2 - 4Db^2 \in 4\mathbb{Z}$ i $4Db^2 \in \mathbb{Z}$. Ara, com que D és lliure de quadrats, $2b$ ha de ser enter, ja que si tingués algun denominador, D no podria dur el seu quadrat a $\mathbb{Z}$. Per tant, $A := 2a$, $B := 2b \in \mathbb{Z}$ i $A^2 - DB^2 \in 4\mathbb{Z}$. A més a més, si $D \not\equiv 1 \pmod 4$, aleshores $A^2 - DB^2 \in 4\mathbb{Z}$ només es pot donar si A i B són parells; de manera que en aquest cas a, $b \in \mathbb{Z}$ i $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. Però en el cas $D \equiv 1 \pmod 4$ pot ser que A i B siguin senars alhora; això ens permet assegurar que $\mathcal{O}_K$ està format per elements $(A+B\sqrt{D})/2$ tals que A, B són nombres enters de la mateixa paritat. En particular, com que $\dfrac{D+\sqrt{D}}{2} \in \mathcal{O}_K$

(és arrel del polinomi $X^2 - DX + \frac{D(D-1)}{4} \in \mathbb{Z}[X]$), se satisfà que $\mathcal{O}_K = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$.
□

En particular, $\mathbb{Z}[i]$ és l'anell dels enters del cos ciclotòmic $\mathbb{Q}(i)$. És ben conegut que aquest anell és un anell principal, ja que és euclidià. Aquesta propietat no és en absolut una propietat general dels anells dels enters dels cossos de nombres. En efecte, veurem de seguida que hi ha exemples d'anells d'enters de cossos de nombres, fins i tot de cossos quadràtics, que no són principals; de fet, ni tan sols factorials.

Exemple 2.2.3. Considerem l'anell $\mathbb{Z}[\sqrt{-5}]$. És l'anell dels enters del cos quadràtic $\mathbb{Q}(\sqrt{-5})$. Veiem que no és factorial.

Observem que $21 = (4+\sqrt{-5})(4-\sqrt{-5}) = 3 \cdot 7$; aquestes són dues descomposicions del nombre 21 com a producte de factors irreductibles en l'anell $\mathbb{Z}[\sqrt{-5}]$; i són essencialment diferents. En efecte, cap dels elements $4 \pm \sqrt{-5}$, 3 i 7 no és un element unitari de l'anell $\mathbb{Z}[\sqrt{-5}]$ i cap d'aquests elements no és un element associat de cap altre. Això es pot veure, per exemple, tenint en compte que si α és un element invertible, aleshores la norma $\mathrm{N}(\alpha)$ és un element invertible de $\mathbb{Z}$, ja que és un enter algebraic de $\mathbb{Q}$ i $\mathrm{N}(\alpha)\mathrm{N}(\alpha^{-1}) = \mathrm{N}(1) = 1$. Com que $\mathrm{N}(4 \pm \sqrt{-5}) = 21$, $\mathrm{N}(3) = 9$, i $\mathrm{N}(7) = 49$, cap d'aquests elements no és una unitat de l'anell $\mathbb{Z}[\sqrt{-5}]$. D'altra banda, si algun d'aquests elements fos associat d'algun altre, ambdós haurien de tenir, llevat potser del signe, la mateixa norma; però això només succeeix amb els dos elements $4 \pm \sqrt{-5}$, que tampoc no són associats ja que, per exemple, el seu quocient no és enter sobre $\mathbb{Z}$.

Resta veure que aquests elements són irreductibles. Si algun d'ells no ho fos, la seva norma hauria de descompondre; però per a $\alpha \in \mathbb{Z}[\sqrt{-5}]$, no pot ser $\mathrm{N}(\alpha) = \pm 3$ ni $\mathrm{N}(\alpha) = \pm 7$, ja que les equacions $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = \pm 3, \pm 7$ no tenen solucions a, $b \in \mathbb{Z}$. En conseqüència, l'anell $\mathbb{Z}[\sqrt{-5}]$ no pot ser un anell factorial.

D'altra banda, hi ha anells d'enters de cossos quadràtics que són principals però que no són euclidians per a cap elecció de l'aplicació grau.

Exemple 2.2.4. Sigui $A := \mathbb{Z}[\theta]$, $2\theta := 1 + \sqrt{-19}$, l'anell dels enters de $\mathbb{Q}(\sqrt{-19})$. Aleshores, l'anell A és principal però no és euclidià per a cap elecció de l'aplicació grau.

Una demostració completa d'aquest fet es pot trobar indicada en el llibre [B-M-T 90, ex.24]. Més endavant, i fent servir tècniques d'aquest curs, en podrem veure una demostració més senzilla.

2.3 Anells de Dedekind

L'objectiu d'aquesta secció és donar les propietats algebraiques més elementals dels anells dels enters dels cossos de nombres.

Proposició 2.3.1. *Siguin A un domini noetherià i íntegrament tancat, K el cos de fraccions de A, $L|K$ una extensió finita i separable, i B la clausura entera de A en L. Aleshores, B és un A-mòdul finitament generat.*

Demostració: Observem, en primer lloc, que podem elegir una K-base de L formada per elements $b_1, b_2, \ldots, b_n \in B$. En efecte, sigui $b \in L$ i siguin $a_0, a_1, \ldots, a_{n-1} \in K$ tals

que $a_0 + a_1 b + a_2 b^2 + \cdots + a_{n-1} b^{n-1} + b^n = 0$; sigui $a \in A$ un denominador comú a tots els coeficients a_i; aleshores, $a_0 a^n, a_1 a^{n-1}, \ldots, a_{n-1} a \in A$ i

$$a_0 a^n + a_1 a^{n-1}(ab) + \cdots + a_{n-1} a (ab)^{n-1} + (ab)^n = 0$$

és una equació de dependència entera de ab sobre A. Per tant, podem multiplicar cada element d'una K-base de L per un element de A per a obtenir una K-base de L formada per elements de B.

D'altra banda, com que l'extensió $L|K$ és finita i separable, la forma bilineal traça, $\mathrm{T}_{L|K}$, és no degenerada i podem considerar la K-base de L dual de la base $b_1, b_2, \ldots, b_n$ respecte d'aquesta forma bilineal (cf. [B-M-T 90, ex.85]); sigui $\beta_1, \beta_2, \ldots, \beta_n \in L$ aquesta base dual i sigui $d \in A$, $d \neq 0$, un element tal que $d\beta_j \in B$ per a tot β_j. Aleshores, B és un A-submòdul del A-mòdul lliure i finitament generat $M := d^{-1}(Ab_1 + \cdots + Ab_n) \subseteq L$. En efecte; sigui $b \in B$ i escrivim-lo en la forma $b = \alpha_1 b_1 + \cdots + \alpha_n b_n$ amb els coeficients $\alpha_i \in K$; com que $\mathrm{T}_{L|K}(b_i \beta_j) = \delta_{ij}$, obtenim que $d\alpha_j = \mathrm{T}_{L|K}(db\beta_j) \in A$, ja que $db\beta_j \in B$ i la traça és la suma dels conjugats, que són enters. Per tant, $db \in Ab_1 + \cdots + Ab_n$, com volíem veure.

Ara, com que A és noetherià, $B \subseteq M$ i M és un A-mòdul finitament generat, obtenim que B és un A-mòdul finitament generat. □

Corol·lari 2.3.2. *Siguin A un domini principal, K el cos de fraccions de A, $L|K$ una extensió finita i separable, $n := [L : K]$ el grau, i B la clausura entera de A en L. Aleshores, B és un A-mòdul lliure de rang n.*

Demostració: És ben conegut que si B és un mòdul finitament generat i sense torsió sobre un domini d'ideals principals, aleshores B és un A-mòdul lliure. La proposició anterior ens assegura que B és un A-mòdul finitament generat; i la qüestió relativa a la torsió és immediata, ja que B és un domini d'integritat. Finalment, una A-base de B és també una K-base de L, ja que L és el cos de fraccions de B. Per tant, B és A-lliure de rang $[L : K]$. □

Corol·lari 2.3.3. *L'anell dels enters d'un cos de nombres és un $\mathbb{Z}$-mòdul lliure de rang finit.* □

Així, l'anell dels enters d'un cos de nombres és un domini noetherià, íntegrament tancat i de dimensió 1, ja que l'extensió $A|\mathbb{Z}$ és entera i $\mathbb{Z}$ és de dimensió 1.

Definició 2.3.4. Un anell de Dedekind és un domini d'integritat noetherià, íntegrament tancat i de dimensió 1; és a dir, un anell noetherià, íntegre, íntegrament tancat, que no és un cos i tal que tot ideal primer no nul és maximal.

Corol·lari 2.3.5. *L'anell dels enters d'un cos de nombres és un anell de Dedekind.* □

2.4 El grup d'ideals

Els anells de Dedekind i, en particular, els anells d'enters dels cossos de nombres, no són, en general, principals. De tota manera, en un anell de Dedekind tot ideal no nul descompon de manera única com a producte d'ideals primers no nuls. Això fa més senzill l'estudi de la seva aritmètica (i, en conseqüència, de l'aritmètica del seu cos de fraccions) que en el cas general d'un anell qualsevol.

Definició 2.4.1. Sigui A un domini d'integritat. Un ideal fraccionari de A és un A-submòdul $\mathfrak{a}$ del cos de fraccions K de A tal que existeix un element $a \in A$, $a \neq 0$, de manera que $a\mathfrak{a} \subseteq A$.

Per exemple, tot ideal de A és un ideal fraccionari. Els ideals de A també s'anomenen, per això, els ideals enters de A.

Definició 2.4.2. Un ideal fraccionari s'anomena principal quan és de la forma aA amb $a \in K$.

Clarament, els ideals fraccionaris principals no nuls de A formen un grup abelià respecte de la multiplicació d'ideals; l'invers d'un ideal fraccionari principal aA és l'ideal fraccionari principal $a^{-1}A$; i notem que aquest grup s'identifica de manera natural amb el grup quocient K^*/A^*. Però aquesta no és l'única propietat interessant dels ideals fraccionaris dels anells de Dedekind. De fet, el conjunt de tots els ideals fraccionaris no nuls d'un anell de Dedekind és un grup respecte de la multiplicació de A-submòduls de K i el conjunt dels ideals fraccionaris principals no nuls és un subgrup del grup de tots els ideals fraccionaris. L'objectiu d'aquesta secció és demostrar aquest fet, com també fer l'estudi dels ideals fraccionaris dels anells de Dedekind.

Proposició 2.4.3. *Sigui A un domini d'integritat. Tot A-submòdul finitament generat $\mathfrak{a}$ del cos de fraccions K de A és un ideal fraccionari.*

Demostració: Sigui $a_1, a_2, \ldots, a_r$ un sistema finit de generadors de $\mathfrak{a}$ i sigui $a \in A$ un denominador comú a tots els elements a_i. Aleshores, $a\mathfrak{a} \subseteq A$. □

Proposició 2.4.4. *Sigui A un domini noetherià. El conjunt dels ideals fraccionaris de A coincideix amb el conjunt dels A-submòduls finitament generats del cos de fraccions K. Més precisament, tot ideal fraccionari és de la forma $a\mathfrak{a}$, on $a \in K$ i $\mathfrak{a} \subseteq A$ és un ideal enter de A.*

Demostració: Ja hem vist que tot A-submòdul finitament generat de K és un ideal fraccionari. Recíprocament, suposem que $\mathfrak{b} \subseteq K$ és un ideal fraccionari i sigui $b \in A$ tal que $b\mathfrak{b} \subseteq A$. Aleshores, $\mathfrak{b} \subseteq b^{-1}A$; com que $b^{-1}A$ és finitament generat (de fet, és principal) i A és noetherià, el A-submòdul $\mathfrak{b}$ de $b^{-1}A$ ha de ser finitament generat.

D'altra banda, si escrivim $\mathfrak{b} = \langle b_1, b_2, \ldots, b_r \rangle$, amb $b_i \in K$, i si $a \in A$ és un denominador comú dels elements $b_1, b_2, \ldots, b_r$, aleshores $\mathfrak{b} = a^{-1}\mathfrak{a}$, on $\mathfrak{a} := \langle ab_1, ab_2, \ldots, ab_r \rangle$ és un ideal enter de A. □

Teorema 2.4.5. *Sigui A un anell de Dedekind. Aleshores, el conjunt dels ideals fraccionaris no nuls de A és un grup abelià lliure respecte de la multiplicació de A-submòduls del cos de fraccions K de A. Els ideals primers no nuls de A formen un sistema de generadors lliures d'aquest grup. A més a més, condició necessària i suficient perquè un ideal $\mathfrak{a}$ de A sigui divisible per un ideal $\mathfrak{b}$ de A és que $\mathfrak{a} \subseteq \mathfrak{b}$.*

Demostració: Farem la demostració d'aquest teorema en diverses etapes.

Lema 2.4.6. *Sigui A un anell noetherià i sigui $\mathfrak{a} \subseteq A$ un ideal no nul de A. Aleshores, existeixen ideals primers no nuls $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r \subseteq A$ tals que $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.*

DEMOSTRACIÓ: Si no és així, el conjunt $\mathcal{C}$ format pels ideals no nuls de A que no contenen cap producte d'ideals primers no nuls és un conjunt no buit. Per ser A noetherià, aquest conjunt ha de tenir elements maximals per a la inclusió d'ideals. Sigui $\mathfrak{a}$ un element maximal de $\mathcal{C}$. L'ideal $\mathfrak{a}$ no pot ser un ideal primer de A, ja que pertany a $\mathcal{C}$; per tant, existeixen elements $a_1, a_2 \in A$ $a_1, a_2 \notin \mathfrak{a}$, tals que $a_1 a_2 \in \mathfrak{a}$. Aleshores, cadascun dels ideals $\mathfrak{b}_i := \mathfrak{a} + a_i A$, $i = 1, 2$, conté un producte d'ideals primers de A i $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$. Però aleshores, $\mathfrak{a}$ conté un producte d'ideals primers: l'ideal producte dels productes d'ideals primers que contenen els ideals $\mathfrak{b}_i$. Aquesta contradicció acaba la demostració. □

Lema 2.4.7. *Sigui A un anell de Dedekind i sigui $\mathfrak{p} \subseteq A$ un ideal primer no nul. Aleshores, $\mathfrak{p}$ és un ideal fraccionari invertible; és a dir, existeix un ideal fraccionari $\mathfrak{p}^{-1}$ de A tal que $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

DEMOSTRACIÓ: Sigui $\mathfrak{p}^{-1} := (A : \mathfrak{p}) = \{x \in K : x\mathfrak{p} \subseteq A\}$, on K designa el cos de fraccions de A. Es tracta de veure que $\mathfrak{p}\mathfrak{p}^{-1} = A$; comprovem, en primer lloc, que $A \subsetneq \mathfrak{p}^{-1}$. Prenem un element no nul $a \in \mathfrak{p}$; en virtut del lema anterior, podem elegir un nombre enter r minimal respecte de la propietat que l'ideal principal aA contingui un producte de r ideals primers no nuls de A, posem $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq aA$. Aleshores, com que $\mathfrak{p}$ és un ideal primer, $\mathfrak{p}$ ha de contenir algun dels ideals primers $\mathfrak{p}_i$, diem $\mathfrak{p}_1$; i com que $\mathfrak{p}_1$ és maximal, ha de ser $\mathfrak{p}_1 = \mathfrak{p}$. D'altra banda, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq aA$ ja que r és minimal; per tant, existeix un element $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $b \notin aA$. Aleshores, $ba^{-1} \in \mathfrak{p}^{-1}$ (ja que $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq aA$) però $ba^{-1} \notin A$, com volíem veure.

De la inclusió trivial $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq A$, i del fet que $\mathfrak{p}$ és un ideal maximal, deduïm que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ o bé $\mathfrak{p}\mathfrak{p}^{-1} = A$. Veiem que la primera igualtat no pot ser i haurem acabat. Si fos $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, aleshores tot element de $\mathfrak{p}^{-1}$ deixaria el A-submòdul finitament generat $\mathfrak{p}$ de K invariant; per tant, l'ideal fraccionari $\mathfrak{p}^{-1}$ hauria de d'estar format per elements enters sobre A (cf. **2.1.2**, (d)); i, com que A és íntegrament tancat, això voldria dir que $\mathfrak{p}^{-1} \subseteq A$; contradicció. □

Lema 2.4.8. *Sigui A un anell de Dedekind. Aleshores, tot ideal fraccionari no nul $\mathfrak{a}$ de A és invertible, i l'invers de $\mathfrak{a}$ és l'ideal fraccionari $\mathfrak{a}^{-1} := (A : \mathfrak{a}) = \{x \in K : x\mathfrak{a} \subseteq A\}$.*

DEMOSTRACIÓ: Com que A és un anell noetherià, la proposició **2.4.4** ens assegura que tot ideal fraccionari de A és el producte d'un element a de K per un ideal enter $\mathfrak{a}$ de A; com que els ideals fraccionaris principals són invertibles, per veure que un ideal fraccionari $\mathfrak{a}$ és invertible podem suposar que és un ideal enter. Així, és suficient demostrar que tot ideal enter no nul $\mathfrak{a} \subseteq A$ és invertible.

Si no és així, i de nou per la noetherianitat, podem elegir un ideal enter no nul $\mathfrak{a} \subseteq A$ maximal entre els no invertibles. Com que els ideals maximals de A són invertibles, $\mathfrak{a}$ no és un ideal maximal de A i existeix un ideal maximal $\mathfrak{p}$ de A tal que $\mathfrak{a} \subsetneq \mathfrak{p}$. Aleshores, $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$. Com que l'invers de $\mathfrak{p}$ conté elements no enters sobre A i com que $\mathfrak{a}$ és un A-submòdul finitament generat de K, no pot ser que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$; és a dir, $\mathfrak{a}\mathfrak{p}^{-1}$ és un ideal de A que conté $\mathfrak{a}$ estrictament. Per la maximalitat de $\mathfrak{a}$, l'ideal $\mathfrak{a}\mathfrak{p}^{-1}$ és un ideal fraccionari invertible; si multipliquem per $\mathfrak{p}$ que és invertible, obtenim que $\mathfrak{a}$ és un ideal invertible.

Resta veure que l'invers de $\mathfrak{a}$ és $(A : \mathfrak{a})$. Però això és clar; si $a \in \mathfrak{a}^{-1}$, és clar que $a \in (A : \mathfrak{a})$; recíprocament, si $a \in (A : \mathfrak{a})$, aleshores $a\mathfrak{a} \subseteq A$, de manera que $a\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ i, com que $1 \in A = \mathfrak{a}\mathfrak{a}^{-1}$, ha de ser $a \in \mathfrak{a}^{-1}$. Això acaba la demostració. □

Acabem de provar que el conjunt format pels ideals fraccionaris no nuls de A és un grup respecte de la multiplicació d'ideals fraccionaris. Si demostrem que tot ideal enter no nul descompon de manera única com a producte d'ideals primers de A ja haurem acabat, ja que tot ideal fraccionari és de la forma $a^{-1}\mathfrak{a}$ per a un cert element $a \in A$ i un cert ideal enter $\mathfrak{a} \subseteq A$.

El conjunt dels ideals no nuls de A que no admeten una descomposició com a producte d'ideals primers no nuls és el conjunt buit; en efecte, en cas contrari tindria un element maximal $\mathfrak{a} \subseteq A$; si $\mathfrak{p}$ és un ideal maximal de A que conté $\mathfrak{a}$, com que $\mathfrak{p}$ és invertible, ha de ser $\mathfrak{a} \subsetneq \mathfrak{p}$; aleshores, $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$, de manera que podem repetir el raonament d'abans: $\mathfrak{a}\mathfrak{p}^{-1}$ és un ideal enter de A que no pot coincidir amb $\mathfrak{a}$ ja que $\mathfrak{p}^{-1}$ conté elements no enters sobre A i $\mathfrak{a}$ és un A-submòdul finitament generat de K; per tant, $\mathfrak{a}\mathfrak{p}^{-1}$ admet descomposició com a producte d'ideals primers; si multipliquem per $\mathfrak{p}$, obtenim una descomposició de $\mathfrak{a}$ com a producte d'ideals primers de A.

Resta veure la unicitat. Però aquesta és fàcil, ja que disposem de la multiplicació pels inversos dels ideals primers no nuls de A. Si $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s$, l'ideal $\mathfrak{q}_1$ és un ideal primer que conté un producte d'ideals primers; per tant, conté algun $\mathfrak{p}_i$, diem $\mathfrak{p}_i = \mathfrak{p}_1$. La maximalitat ens permet assegurar que $\mathfrak{q}_1 = \mathfrak{p}_1$; si multipliquem per l'invers de $\mathfrak{p}_1$, obtenim la igualtat $\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_2\cdots\mathfrak{q}_s$, amb menys factors, i la prova s'acaba fàcilment per un argument recursiu. □

Definició 2.4.9. El grup dels ideals fraccionaris no nuls de l'anell de Dedekind A s'anomena el grup d'ideals de A (o el grup d'ideals de K quan l'anell A és clar). El grup quocient d'aquest grup d'ideals pel subgrup dels ideals fraccionaris principals s'anomena el grup de classes d'ideals de A (o de K). S'acostuma a designar per $\mathrm{Cl}(A)$.

De fet, es disposa de la successió exacta de grups abelians

$$1 \longrightarrow A^* \longrightarrow K^* \longrightarrow \mathbf{I}(A) \longrightarrow \mathrm{Cl}(A) \longrightarrow 1,$$

on $\mathbf{I}(A)$ designa el grup dels ideals fraccionaris no nuls de A i A^* el grup dels elements invertibles de l'anell A.

2.5 Factorialitat i principalitat

Una conseqüència immediata de la definició del grup de classes d'ideals d'un anell de Dedekind és el resultat següent.

Corol·lari 2.5.1. *Sigui A un anell de Dedekind. Condició necessària i suficient perquè l'anell A sigui un anell principal és que el grup de classes d'ideals de A sigui trivial.* □

Aquesta condició caracteritza quan un anell de Dedekind és principal. Podem dir que el grup $\mathrm{Cl}(A)$ és una mesura de quant s'aparta l'anell A de ser un anell principal. De totes maneres, encara no sabem gairebé res del grup de classes d'ideals d'un anell de Dedekind. Però podem donar alguna condició suficient perquè un anell de Dedekind sigui principal.

El fet que els ideals primers d'un anell de Dedekind formin un sistema de generadors del grup d'ideals i el fet que el producte d'ideals principals és un ideal principal ens permeten escriure immediatament que si tots els ideals primers d'un anell de Dedekind A són principals, aleshores A és un anell principal. Encara més, podem demostrar el resultat següent.

Proposició 2.5.2. *Sigui A un anell de Dedekind. Suposem que A té només un nombre finit d'ideals primers. Aleshores, A és un anell principal.*

DEMOSTRACIÓ: Siguin $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ tots els ideals primers no nuls de A. Fixat un d'ells, diem $\mathfrak{p} = \mathfrak{p}_1$, podem elegir $a \in \mathfrak{p}$ de manera que $a \notin \mathfrak{p}^2$; el sistema de congruències

$$\begin{cases} x \equiv a \pmod{\mathfrak{p}} \\ x \equiv 1 \pmod{\mathfrak{p}_i}, \quad i > 1, \end{cases}$$

té solució en A en virtut del teorema xinès del residu. I una solució x d'aquest sistema és un generador de l'ideal $\mathfrak{p}$, ja que a la descomposició en producte d'ideals primers de l'ideal principal xA no pot aparèixer cap primer $\mathfrak{p}_i \neq \mathfrak{p}$ ni tampoc $\mathfrak{p}^2$; i l'ideal xA no és tot l'anell A ja que $x \in \mathfrak{p}$ perquè per a x se safisfà la primera equació.

En conseqüència, tot ideal primer de A és un ideal principal i, per tant, A mateix és un anell principal. □

Proposició 2.5.3. *Sigui A un anell de Dedekind i suposem que el grup de classes d'ideals de A és finitament generat. Aleshores, existeix un element $a \in A$, $a \neq 0$, tal que l'anell $A[a^{-1}]$ és un anell de Dedekind principal.*

DEMOSTRACIÓ: Notem, en primer lloc, que qualsevol localitzat d'un anell de Dedekind és un anell de Dedekind. En efecte, si S és un conjunt multiplicativament tancat d'un anell de Dedekind A, aleshores l'anell $S^{-1}A$ és un domini noetherià, és íntegrament tancat i és de dimensió 1; per tant, és un anell de Dedekind.

Per a demostrar la proposició, siguin $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r \subseteq A$ ideals primers tals que les seves classes generen $\mathrm{Cl}(A)$ i sigui $a \neq 0$ un element $a \in \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r$. Aleshores, l'anell $A[a^{-1}]$ és el localitzat de A en les potències de a i, per tant, els ideals $\mathfrak{p}_i$ esdevenen, quan els estenem, tot l'anell $A[a^{-1}]$. D'altra banda, l'assignació $\mathfrak{a} \mapsto \mathfrak{a}A[a^{-1}]$ defineix un morfisme exhaustiu de grups entre els grups d'ideals fraccionaris no nuls dels anells A i $A[a^{-1}]$; el seu nucli està format pels ideals fraccionaris de A que contenen alguna potència de a. A més a més, els ideals fraccionaris principals de A van a parar a ideals fraccionaris principals de $A[a^{-1}]$, de manera que el grup $\mathrm{Cl}(A)$ s'aplica exhaustivament en el grup $\mathrm{Cl}(A[a^{-1}])$. Com que les imatges d'un sistema de generadors són un sistema de generadors, i com que els ideals $\mathfrak{p}_i$ s'apliquen en l'ideal unitat, el grup $\mathrm{Cl}(A[a^{-1}])$ és el grup trivial. □

Seguidament es tracta de caracteritzar quan un anell de Dedekind és factorial. En concret, es tracta de demostrar el resultat següent.

Proposició 2.5.4. *Sigui A un anell de Dedekind. Condició necessària i suficient perquè A sigui factorial és que sigui principal.*

DEMOSTRACIÓ: Suposem que A és un anell de Dedekind factorial i que $\mathfrak{p} \subseteq A$ és un ideal primer no nul; hem de veure que $\mathfrak{p}$ és un ideal principal. Sigui $a \neq 0$ un element de $\mathfrak{p}$; com que A és factorial, aquest element a admet una factorització $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $\alpha_i \geq 1$, com a producte d'elements irreductibles diferents p_i de A. Com que $\mathfrak{p}$ és primer, algun dels elements irreductibles p_i ha de ser un element de $\mathfrak{p}$. Aleshores, l'ideal principal generat per p_i és un ideal primer, ja que A és un anell factorial, i està inclòs en $\mathfrak{p}$; com que en A tot ideal primer no nul és maximal, ha de ser $\mathfrak{p} = p_i A$. □

Capítol 3

Ramificació

Destinem aquest capítol a fer l'estudi d'extensions d'anells de Dedekind i del comportament dels ideals primers en aquestes extensions. Comencem per repassar els conceptes i les propietats de la traça i de la norma.

3.1 Normes i traces

Sigui $L|K$ una extensió finita de cossos. Per a tot element $\theta \in L$ podem definir l'aplicació de multiplicació per θ, $\mathfrak{m}_\theta : L \longrightarrow L$ per la fórmula $\mathfrak{m}_\theta(\theta') := \theta\theta'$, per a tot $\theta' \in L$. L'aplicació $\mathfrak{m}_\theta$ és K-lineal i si elegim una K-base de L, $\{\theta_1, \theta_2, \ldots, \theta_n\}$, té associada una matriu $(a_{i,j}) \in \mathbf{M}(n, K)$, on $\mathbf{M}(n, K)$ indica l'espai vectorial de les matrius quadrades de n files i n columnes i coeficients en K. El polinomi característic de la matriu $(a_{i,j})$ no depèn de la base elegida. En particular, la traça, $\mathrm{T}_{L|K}(\theta) := \mathrm{tr}(a_{i,j}) = \sum_{i=1}^{n} a_{i,i}$, i el determinant, $\mathrm{N}_{L|K}(\theta) := \det(a_{i,j})$, no en depenen.

Definició 3.1.1. Les aplicacions $\mathrm{T}_{L|K} : L \longrightarrow K$ i $\mathrm{N}_{L|K} : L \longrightarrow K$ definides per les fórmules $\mathrm{T}_{L|K}(\theta) := \mathrm{tr}(a_{i,j}) = \sum_{i=1}^{n} a_{i,i}$, i $\mathrm{N}_{L|K}(\theta) := \det(a_{i,j})$, s'anomenen, respectivament, la traça i la norma de l'extensió $L|K$.

Llistem a continuació les propietats més elementals d'aquestes aplicacions $\mathrm{T}_{L|K}$ i $\mathrm{N}_{L|K}$.

Proposició 3.1.2. *Siguin $\theta, \theta_1, \theta_2 \in L$ i $\alpha \in K$. Aleshores:*

(a) $\mathrm{T}_{L|K}(\theta_1 + \theta_2) = \mathrm{T}_{L|K}(\theta_1) + \mathrm{T}_{L|K}(\theta_2)$;

(b) $\mathrm{T}_{L|K}(\alpha\theta) = \alpha\mathrm{T}_{L|K}(\theta)$;

(c) $\mathrm{N}_{L|K}(\theta_1\theta_2) = \mathrm{N}_{L|K}(\theta_1)\mathrm{N}_{L|K}(\theta_2)$; *i*

(d) $\mathrm{N}_{L|K}(\alpha\theta) = \alpha^n \mathrm{N}_{L|K}(\theta)$,

on $n := [L : K]$ és el grau de l'extensió $L|K$. $\square$

Els resultats següents ens proporcionen una manera còmoda per a calcular la traça i la norma.

Proposició 3.1.3. *Siguin $L|K$ una extensió finita de cossos, $\theta \in L$ un element qualsevol, s el grau de separabilitat de l'extensió $L|K$, $\sigma_1, \sigma_2, \ldots, \sigma_s$ les K-immersions diferents de L en una clausura algebraica de K, i p^i el grau d'inseparabilitat de l'extensió $L|K$. Aleshores,*

$$\mathrm{T}_{L|K}(\theta) = p^i \left(\sigma_1(\theta) + \cdots + \sigma_s(\theta)\right)$$
$$\mathrm{N}_{L|K}(\theta) = \left(\sigma_1(\theta) \cdots \sigma_s(\theta)\right)^{p^i}.$$

En particular, si l'extensió $L|K$ no és separable, aleshores $\mathrm{T}_{L|K} = 0$.

Demostració: Suposem, en primer lloc, que θ és un element primitiu de l'extensió $L|K$. Siguin $f(X) := \mathrm{Irr}(\theta, K)(X)$ el polinomi mònic irreductible de $K[X]$ que té θ per arrel i $g(X)$ el polinomi característic de la multiplicació $\mathfrak{m}_\theta$. Com que $g(\mathfrak{m}_\theta) = 0$, també $g(\theta) = 0$ i el polinomi $f(X)$ divideix el polinomi $g(X)$. A més a més, els dos polinomis $f(X)$ i $g(X)$ són del mateix grau, $n := sp^i$, i tots dos són mònics; per tant, coincideixen. Això ens permet assegurar que $\mathrm{T}_{L|K}(\theta)$ és la suma dels n conjugats de θ i que $\mathrm{N}_{L|K}(\theta)$ és el producte dels n conjugats de θ, ja que les arrels del polinomi irreductible de θ sobre K són els s conjugats diferents, $\sigma_j(\theta)$, comptats p^i vegades cadascun.

En el cas general, si θ no és un element primitiu, encara podem considerar el subcòs $K' := K(\theta)$ de L. Si elegim una K-base de K' i una K'-base de L qualssevol, els productes formen una K-base de L i la matriu de la multiplicació per θ en L en aquesta base es pot escriure en forma de matriu diagonal de caixes idèntiques a la matriu de la multiplicació per θ en K'. Per tant, el polinomi característic de la multiplicació per θ en l'extensió $L|K$ és la potència $[L : K']$-èsima del polinomi característic de la multiplicació per θ en l'extensió $K'|K$; això proporciona, en particular, les igualtats

$$\mathrm{T}_{L|K}(\theta) = [L : K']\mathrm{T}_{K'|K}(\theta), \qquad \mathrm{N}_{L|K}(\theta) = \mathrm{N}_{K'|K}(\theta)^{[L:K']},$$

per a la traça i la norma de θ en l'extensió $L|K$. Per acabar la demostració, només cal tenir en compte que les s K-immersions diferents de L es distribueixen, segons els valors que prenen sobre θ, en tantes classes d'equivalència com el grau de separabilitat de l'extensió $K'|K$, i que totes les classes tenen cardinal el grau de separabilitat de l'extensió $L|K'$. □

Proposició 3.1.4. *Siguin $L|K'$ i $K'|K$ extensions finites de cossos. Aleshores, per a tot $\theta \in L$ se satisfan les fórmules de transitivitat*

$$\mathrm{T}_{L|K}(\theta) = \mathrm{T}_{K'|K}\left(\mathrm{T}_{L|K'}(\theta)\right), \qquad \mathrm{N}_{L|K}(\theta) = \mathrm{N}_{K'|K}\left(\mathrm{N}_{L|K'}(\theta)\right).$$

És a dir, com a aplicacions, $\mathrm{T}_{L|K} = \mathrm{T}_{K'|K} \circ \mathrm{T}_{L|K'}$ i $\mathrm{N}_{L|K} = \mathrm{N}_{K'|K} \circ \mathrm{N}_{L|K'}$.

Demostració: Només cal tenir en compte que les K-immersions de L són les extensions diferents a L de les K-immersions de K' i de quina manera s'obtenen a partir de les K'-immersions de L. □

La forma lineal traça ens permet definir de manera natural, ja que L és una K-àlgebra, una aplicació bilineal $\mathrm{T}_{L|K} : L \times L \longrightarrow K$ per la fórmula $(a, b) \mapsto \mathrm{T}_{L|K}(ab)$. Com que L és commutatiu, la forma bilineal és simètrica. El resultat que segueix ja ha estat usat en un parell d'ocasions.

Proposició 3.1.5. *Siguin $L|K$ una extensió finita de cossos i $T_{L|K} : L \times L \longrightarrow K$ la forma bilineal simètrica definida per $(x, y) \mapsto \mathrm{T}_{L|K}(xy)$. A fi que l'extensió $L|K$ sigui separable és condició necessària i suficient que la forma $\mathrm{T}_{L|K}$ sigui no degenerada; és a dir que de la igualtat $\mathrm{T}_{L|K}(xy) = 0$ per a tot $y \in L$ es dedueixi $x = 0$.*

Demostració: Suposem, en primer lloc, que l'extensió $L|K$ és separable i sigui θ un element primitiu de l'extensió. El conjunt $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, on $n := [L : K]$ designa el grau de l'extensió $L|K$, és una K-base de L. Sigui $D := (d_{i,j})$ la matriu de la forma bilineal $\mathrm{T}_{L|K}$ en aquesta base; és a dir, $d_{i,j} := \mathrm{T}_{L|K}(\theta^{i-1}\theta^{j-1})$. Cal veure que la matriu D és no singular; és a dir, que $\det D \neq 0$.

Per a això, considerem la matriu de Vandermonde

$$V = V(\theta_1, \theta_2, \ldots, \theta_n) := \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \theta_1^2 & \theta_2^2 & \ldots & \theta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots & \theta_n^{n-1} \end{bmatrix},$$

on els elements θ_i són els diferents conjugats de $\theta_1 := \theta$. La traça de θ és la suma dels conjugats, $\theta_1 + \cdots + \theta_n$; anàlogament, per a tot nombre enter k, la traça de θ^k és la suma dels seus conjugats, $\theta_1^k + \cdots + \theta_n^k$. Això implica que la matriu D és el producte $D = VV^t$ de V per la seva matriu transposada; per tant, el determinant de D és el quadrat del determinant de la matriu V, que és no nul ja que els elements $\theta_i - \theta_j$ són diferents quan $i \neq j$.

Recíprocament, ja hem vist que si l'extensió $L|K$ no és separable, aleshores $\mathrm{T}_{L|K} = 0$. □

3.2 Extensions d'anells de Dedekind

En moltes aplicacions, els anells de Dedekind són extensions d'altres anells de Dedekind. Concretament, en el cas dels cossos de nombres, l'anell dels enters d'un cos de nombres L, extensió de K, és la clausura entera en L de l'anell dels enters de K. Aquest resultat és més general.

Proposició 3.2.1. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i B la clausura entera de A en L. Aleshores, B és un anell de Dedekind.*

Demostració: L'anell B és íntegrament tancat, ja que és una clausura entera, i és de dimensió 1, ja que A ho és i l'extensió $B|A$ és entera. Resta veure la noetherianitat.

Sigui $K' \subseteq L$ la clausura separable de K en L. Això vol dir que l'extensió $K'|K$ és separable i l'extensió $L|K'$ és purament inseparable. Sigui A' la clausura entera de A en K'; aleshores, B també és la clausura entera de A' en L. Això fa que puguem fer la prova de la proposició en dues etapes i amb una hipòtesi suplementària per a cada una d'elles: en primer lloc, podem suposar que l'extensió $L|K$ és separable; i després, que l'extensió $L|K$ és purament inseparable. I, en el cas separable, la noetherianitat queda assegurada per la proposició (**2.3.1**).

Suposem, doncs, que l'extensió $L|K$ és purament inseparable. Com que és finita, existeix un nombre enter q, potència de la característica, de manera que $L^q \subseteq K$. Considerem el cos M, extensió de L, definit per la condició $M^q = K$; és a dir, $x \in M \iff x^q \in K$. La clausura entera, C, de A en M és l'anell definit per la condició $x \in C \iff x^q \in A$. El morfisme de cossos $M \longrightarrow K$ definit per $x \mapsto x^q$ és un isomorfisme i, en conseqüència, la seva restricció $C \longrightarrow A$ també és un isomorfisme; per tant, l'anell C és un anell de Dedekind. D'aquí deduirem la noetherianitat de B.

Sigui $\mathfrak{a}$ un ideal no nul de B i sigui $\mathfrak{A}$ la seva extensió a l'anell C; com que C és un anell de Dedekind, l'ideal $\mathfrak{A}$ és invertible i el seu invers és l'ideal fraccionari $(C : \mathfrak{A})$. Això ens permet assegurar que existeixen elements $a_i \in \mathfrak{a}$ i elements $c_i \in (C : \mathfrak{A})$ tals que $\sum_i a_i c_i = 1$. En elevar a q, obtenim la igualtat $\sum_i a_i a_i^{q-1} c_i^q = 1$, que té coeficients $b_i := a_i^{q-1} c_i^q \in L$, ja que $a_i \in \mathfrak{a}$ i $c_i \in M$. Encara més, $b_i \mathfrak{a} \subseteq c_i^q \mathfrak{a}^q \subseteq C$, ja que $c_i \in (C : \mathfrak{A})$ i $\mathfrak{a} \subseteq \mathfrak{A}$. Per tant, $b_i \mathfrak{a} \subseteq C \cap L = B$, de manera que $b_i \in (B : \mathfrak{a})$; ara, la igualtat $\sum_i a_i c_i = 1$ implica que $\mathfrak{a}(B : \mathfrak{a}) = B$ i, en conseqüència, l'ideal $\mathfrak{a}$ és un ideal invertible de B.

Dit d'una altra manera, hem provat que tot ideal no nul de B és invertible. Però això ja implica que B és un anell noetherià; en efecte, sigui $\mathfrak{a} \subseteq B$ un ideal no nul; podem elegir elements $a_1, a_2, \ldots, a_r \in \mathfrak{a}$ i elements $b_1, b_2, \ldots, b_r \in (B : \mathfrak{a})$ tals que $\sum_{i=1}^r a_i b_i = 1$; en aquest cas, $\{a_1, a_2, \ldots, a_r\}$ és un sistema de generadors de $\mathfrak{a}$, ja que si $a \in \mathfrak{a}$, aleshores $ab_i \in B$ i $\sum_{i=1}^r a_i a b_i = a$. Així, tot ideal de B és finitament generat. □

3.3 Índex de ramificació i grau residual

Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i B la clausura entera de A en L. A la secció anterior hem vist que B també és un anell de Dedekind. En particular, si $\mathfrak{p} \subseteq A$ és un ideal primer no nul de A, la seva extensió a B, $\mathfrak{p}B$, és un ideal no nul que no és tot l'anell B perquè l'extensió $B|A$ és entera. Per tant, l'ideal $\mathfrak{p}B$ descompon com a producte d'ideals primers de B de manera única.

Sigui $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$ aquesta descomposició en factors primers; això vol dir que els ideals $\mathfrak{P}_i$, $1 \leq i \leq g$, són ideals primers diferents i no nuls de B i que $e_i \geq 1$ són nombres enters.

Definició 3.3.1. S'anomena índex de ramificació de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ el nombre enter e_i. S'acostuma a designar per $e(\mathfrak{P}_i|\mathfrak{p})$ o per $e_{\mathfrak{P}_i|\mathfrak{p}}$.

Observem que podem partir d'un ideal primer $\mathfrak{P} \subseteq B$, considerar la seva contracció $\mathfrak{p} := \mathfrak{P} \cap A$ en A i després mirar quin és l'exponent de $\mathfrak{P}$ en la descomposició de $\mathfrak{p}B$ com a producte d'ideals primers de B; això sempre dóna un exponent $e(\mathfrak{P}|\mathfrak{p}) \geq 1$ ja que $\mathfrak{P} \supseteq \mathfrak{p}B$ i, per tant, $\mathfrak{P}$ és un ideal primer que divideix l'ideal $\mathfrak{p}B$.

Definició 3.3.2. Sigui $\mathfrak{p}$ un ideal primer no nul de l'anell de Dedekind A. L'anell quocient, $A/\mathfrak{p}$, és un cos, ja que $\mathfrak{p}$ és un ideal maximal de A. S'anomena el cos residual de A en $\mathfrak{p}$.

Considerem, ara, els cossos residuals de A en $\mathfrak{p}$ i de B en $\mathfrak{P}$. El morfisme d'anells $A \xrightarrow{inc} B$ donat per la inclusió de A en B dóna lloc per pas al quocient a un morfisme dels cossos residuals $A/\mathfrak{p} \longrightarrow B/\mathfrak{P}$, ja que $\mathfrak{P} \cap A = \mathfrak{p}$. Això ens permet assegurar que el cos residual de B en $\mathfrak{P}$ és un cos extensió del cos residual de A en $\mathfrak{p}$.

Proposició 3.3.3. *Siguin A un anell de Dedekind, K el cos de fraccions de A, $L|K$ una extensió finita, B la clausura entera de A en L, $\mathfrak{P}$ un ideal primer no nul de B, i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Aleshores, l'extensió dels cossos residuals $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ és una extensió finita i per al seu grau se satisfà la desigualtat $[B/\mathfrak{P} : A/\mathfrak{p}] \leq [L : K]$.*

Demostració: Comencem per fer un procés de localització amb la finalitat de fer que l'anell A sigui principal. Per a això, sigui $S := A - \mathfrak{p}$ el complementari de l'ideal primer $\mathfrak{p}$ de A i considerem els anells localitzats $S^{-1}A$ i $S^{-1}B$. Els localitzats d'anells de Dedekind són anells de Dedekind, de manera que $S^{-1}A$ és encara un anell de Dedekind; a més a més, $S^{-1}A$ només té un ideal maximal: l'ideal $\mathfrak{p}S^{-1}A$; per tant, en virtut de la proposició (**2.5.2**), l'anell $S^{-1}A$ és un anell de Dedekind principal. D'altra banda, l'anell $S^{-1}B$ és la clausura entera de $S^{-1}A$ en L i, com que la localització i el pas al quocient commuten, encara tenim isomorfismes $A/\mathfrak{p} \cong S^{-1}A/\mathfrak{p}S^{-1}A$ i $B/\mathfrak{P} \cong S^{-1}B/\mathfrak{P}S^{-1}B$. A més a més, se satisfà la igualtat $\mathfrak{P}S^{-1}B \cap S^{-1}A = \mathfrak{p}S^{-1}A$. Aquestes consideracions fan que puguem suposar, a l'hora de fer la demostració, que l'ideal $\mathfrak{p}$ és un ideal principal.

Sigui, doncs, $\pi \in \mathfrak{p}$ un generador de $\mathfrak{p}$. Suposem que en $B/\mathfrak{P}$ tenim un conjunt $\{b_i+\mathfrak{P}\}_i$ format per elements $A/\mathfrak{p}$-linealment independents, on $b_i \in B$; aleshores, el conjunt $\{b_i\}_i$ és un conjunt linealment independent d'elements de B. En efecte, si tinguéssim una relació no trivial de dependència lineal $\sum_i a_i b_i = 0$ amb $a_i \in K$, podríem treure denominadors dels a_i i suposar que $a_i \in A$ per a tot i; i després de dividir per una potència adequada de π, podríem suposar que algun dels elements a_i no pertany a l'ideal primer $\mathfrak{p}$; en reduir aquesta equació mòdul $\mathfrak{P}$, obtindríem una relació de dependència lineal dels elements $b_i + \mathfrak{P}$, de coeficients en $A/\mathfrak{p}$ i amb algun d'ells no nul.

Dit d'una altra manera, elements $A/\mathfrak{p}$-linealment independents de $B/\mathfrak{P}$ provenen d'elements K-linealment independents de L, de manera que el grau de l'extensió residual en $\mathfrak{P}$ és menor o igual que el grau de l'extensió $L|K$. □

Definició 3.3.4. El grau $[B/\mathfrak{P} : A/\mathfrak{p}]$ s'anomena el grau residual en $\mathfrak{P}$ de l'extensió d'anells $B|A$. Quan no hi ha confusió possible sobre quin és l'anell A (i, en conseqüència, B) també es parla del grau residual de $L|K$ en $\mathfrak{P}$. S'acostuma a designar per $f(\mathfrak{P}|\mathfrak{p})$ o per $f_{\mathfrak{P}|\mathfrak{p}}$.

Una propietat molt important i, alhora, de demostració immediata, és la multiplicativitat dels índexs de ramificació i dels graus residuals en cadenes d'extensions finites. Concretament, se satisfà el resultat següent.

Proposició 3.3.5. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $K'|K$ i $L|K'$ extensions finites, A' la clausura entera de A el K', B la clausura entera de A' en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, $\mathfrak{P}' := \mathfrak{P} \cap A'$ la seva contracció a A' i $\mathfrak{p} := \mathfrak{P} \cap A = \mathfrak{P}' \cap A$ la contracció a A de $\mathfrak{P}$ i de $\mathfrak{P}'$. Aleshores se satisfan les fórmules:*

$$e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}')e(\mathfrak{P}'|\mathfrak{p}),$$
$$f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}'|\mathfrak{p}),$$
$$g(\mathfrak{p}) = \sum_{\mathfrak{P}' \cap A = \mathfrak{p}} g(\mathfrak{P}'). \square$$

Definició 3.3.6. Siguin $B|A$ una extensió finita i entera d'anells de Dedekind, $\mathfrak{P} \subseteq B$ un ideal primer de B i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Es diu que l'extensió $B|A$ és ramificada en $\mathfrak{P}$ si l'extensió residual en $\mathfrak{P}$ no és separable o bé si $e(\mathfrak{P}|\mathfrak{p}) > 1$; es diu que l'extensió $B|A$ és ramificada en $\mathfrak{p}$ quan hi ha algun ideal primer $\mathfrak{P}$ en B tal que $\mathfrak{P}^2$ divideix $\mathfrak{p}B$ o bé l'extensió residual en $\mathfrak{P}$ no és separable. Es diu que l'extensió $B|A$ és no ramificada en $\mathfrak{P} \subseteq B$ quan l'extensió residual $B/\mathfrak{P}$ de $A/\mathfrak{p}$ és separable i $e(\mathfrak{P}|\mathfrak{p}) = 1$. Es diu que l'extensió $B|A$ és no ramificada en el primer $\mathfrak{p} \subseteq A$ quan és no ramificada en tot ideal primer $\mathfrak{P} \subseteq B$ que divideix $\mathfrak{p}$.

3.4 La fórmula $\sum e_i f_i = n$

Acabem de veure que a cada extensió finita i entera, $B|A$, d'anells de Dedekind li podem associar tres famílies importants d'invariants: les famílies $\{e(\mathfrak{P}|\mathfrak{p})\}_{\mathfrak{P}}$, dels índexs de ramificació dels ideals primers no nuls $\mathfrak{P} \subseteq B$; $\{f(\mathfrak{P}|\mathfrak{p})\}_{\mathfrak{P}}$, dels graus residuals; i $\{g(\mathfrak{p})\}_{\mathfrak{p}}$, dels nombres d'ideals primers de B que divideixen els ideals primers no nuls $\mathfrak{p} \subseteq A$. Es tracta, seguidament, de demostrar una relació, potser la més important, entre aquests invariants.

Proposició 3.4.1. *Siguin A un anell de Dedekind, K el cos de fraccions de A, $L|K$ una extensió finita, $n := [L : K]$ el grau, B la clausura entera de A en L i $\mathfrak{p}$ un ideal primer no nul de A. Sigui $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ la descomposició de $\mathfrak{p}B$ en factors primers en B. Aleshores, se satisfà la desigualtat*

$$\sum_{i=1}^{g} e_i f_i \leq n.$$

La suma $\displaystyle\sum_{i=1}^{g} e_i f_i$ és la dimensió de $B/\mathfrak{p}B$ com a $A/\mathfrak{p}$-espai vectorial.

Demostració: Sigui $S := A - \mathfrak{p}$. Aleshores, l'anell $S^{-1}A$ és un anell de Dedekind principal i local amb ideal maximal $\mathfrak{p}S^{-1}A$. L'anell $S^{-1}B$ és la clausura entera de $S^{-1}A$ en L, els ideals $\mathfrak{P}_i S^{-1}B$ són els ideals primers de $S^{-1}B$, se satisfà la descomposició $\mathfrak{p}S^{-1}B = \mathfrak{P}_1^{e_1}S^{-1}B\cdots\mathfrak{P}_g^{e_g}S^{-1}B$ i es tenen isomorfismes $A/\mathfrak{p} \cong S^{-1}A/\mathfrak{p}S^{-1}A$ i $B/\mathfrak{P}_i \cong S^{-1}B/\mathfrak{P}_i S^{-1}B$. Per tant, i igual que en la demostració de la proposició **3.3.3**, podem suposar que A és un anell de Dedekind local (i, per tant, principal). Amb aquesta hipòtesi suplementària, l'anell de Dedekind B només té un nombre finit d'ideals primers i, en conseqüència, és principal. Per tant, podem raonar de la manera següent. En primer lloc, el teorema xinès del residu ens permet escriure l'isomorfisme d'anells

$$B/\mathfrak{p}B \cong \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}.$$

Per tant, si demostrem que $B/\mathfrak{P}_i^{e_i}$ és de dimensió $e_i f_i$ sobre $A/\mathfrak{p}$, obtindrem el valor de la suma $\displaystyle\sum_{i=1}^{g} e_i f_i$ com la dimensió de $B/\mathfrak{p}B$. Tot i que l'anell $B/\mathfrak{P}_i^{e_i}$ no és, en general, un $B/\mathfrak{P}_i$-espai vectorial, els seus ideals $\mathfrak{P}_i^a/\mathfrak{P}_i^{e_i}$, $0 \leq a \leq e_i - 1$, formen una cadena amb quocients $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ que són $B/\mathfrak{P}_i$-espais vectorials de dimensió 1 (la multiplicació per la potència a-èsima d'un generador de $\mathfrak{P}_i$ defineix un isomorfisme de $B/\mathfrak{P}_i$ en $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$).

Per a acabar la demostració de la segona propietat només cal tenir en compte que el $A/\mathfrak{p}$-espai vectorial $B/\mathfrak{P}_i$ és de dimensió f_i.

Resta demostrar que la dimensió de $B/\mathfrak{p}B$ com a $A/\mathfrak{p}$-espai vectorial és menor o igual que el grau $[L : K]$. L'anell $B/\mathfrak{p}B$ és un $A/\mathfrak{p}A$-espai vectorial, i $\mathfrak{p}B \cap A = \mathfrak{p}$; sigui $\{b_i\}_i$ un conjunt d'elements de B tals que les seves classes $b_i + \mathfrak{p}B$ siguin $A/\mathfrak{p}$-linealment independents. Si tinguéssim una relació no trivial de dependència lineal $\sum_i a_i b_i = 0$ en L amb els coeficients $a_i \in K$, en multiplicar (o dividir) per una potència adequada d'un generador π de l'ideal $\mathfrak{p}$ podríem suposar que tots els coeficients a_i són de A i que algun d'ells no és de l'ideal $\mathfrak{p}$; la reducció d'aquesta igualtat mòdul l'ideal $\mathfrak{p}B$ donaria una relació no trivial de dependència lineal dels elements $b_i + \mathfrak{p}B$. Això ens permet assegurar que la dimensió de $B/\mathfrak{p}B$ com a $A/\mathfrak{p}$-espai vectorial no pot superar la dimensió de L com a K-espai vectorial. Això acaba la demostració. □

Observació 3.4.2. Si, en aquesta demostració, l'anell $S^{-1}B$ és un $S^{-1}A$-mòdul finitament generat (per exemple, si B és un A-mòdul finitament generat), aleshores la dimensió de $B/\mathfrak{p}B$ com a $A/\mathfrak{p}$-espai vectorial i el grau $[L : K]$ coincideixen.

En efecte, el lema de Nakayama (cf., per exemple, [At-McD 73, prop. 2.6]) ens permet assegurar que un sistema minimal de generadors de $S^{-1}B$ com a $S^{-1}A$-mòdul dóna lloc, per reducció, a una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$ (recordem que $A/\mathfrak{p} \cong S^{-1}A/\mathfrak{p}S^{-1}A$ i que, anàlogament, $B/\mathfrak{p}B \cong S^{-1}B/\mathfrak{p}S^{-1}B$); i a la demostració de la proposició hem vist que aquests elements són K-linealment indepentents de L. Sigui $\{b_1, b_2, \ldots, b_n\}$ un sistema minimal de generadors de $S^{-1}B$ com a $S^{-1}A$-mòdul. Com que $L = S^{-1}BK$, si $b \in L$ és un element qualsevol, aleshores existeix $a \in S^{-1}A$ tal que $ab \in S^{-1}B$; per tant, ab pertany al K-subespai vectorial de L generat pels elements b_i, de manera que b ha de pertànyer a aquest subespai. Això demostra que un sistema minimal de generadors de $S^{-1}B$ com a $S^{-1}A$-mòdul és automàticament una K-base de L. Per tant, les dues dimensions coincideixen.

Dit d'una altra manera, hem demostrat una de les implicacions del resultat següent.

Proposició 3.4.3. *Mantinguem les mateixes notacions que en la proposició anterior i posem $S := A - \mathfrak{p}$. Aleshores, condició necessària i suficient perquè la dimensió de $B/\mathfrak{p}B$ com a $A/\mathfrak{p}$-espai vectorial coincideixi amb el grau $[L : K]$ és que l'anell $S^{-1}B$ sigui un $S^{-1}A$-mòdul finitament generat.*

Demostració: Només resta veure la necessitat de la condició. De nou podem suposar que A és principal; en aquest cas, ja hem vist que un conjunt $\{b_1, b_2, \ldots, b_r\}$ d'elements de B que donin una base del quocient $B/\mathfrak{p}B$ sobre $A/\mathfrak{p}$ és automàticament un conjunt d'elements de L que són K-linealment independents. Com que suposem que totes dues dimensions són iguals, això implica que $\{b_1, b_2, \ldots, b_r\}$ és una K-base de L. Veiem que és un sistema de generadors de B com a A-mòdul i haurem acabat. Si $b \in B$, podem escriure $b = \sum_{i=1}^{r} a_i b_i$ amb $a_i \in K$; si algun coeficient a_i no fos de A, en multiplicar per una potència positiva adequada d'un generador π de $\mathfrak{p}$, obtindríem una igualtat de la forma $\pi^k b = \sum_{i=1}^{r} (\pi^k a_i) b_i$, amb els coeficients $\pi^k a_i \in A$, algun d'ells invertible; aquesta igualtat donaria, per reducció mòdul $\mathfrak{p}B$ una relació no trivial de dependència lineal dels elements b_i en $B/\mathfrak{p}B$, i això contradiria el fet que els elements b_i són una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$. □

Observació 3.4.4. En particular, la condició de generació finita de la proposició se satisfà en el cas que l'extensió $L|K$ sigui separable; per exemple, en el cas dels anells d'enters dels cossos de nombres.

Corol·lari 3.4.5. *Siguin A un anell de Dedekind, K el cos de fraccions de A, $L|K$ una extensió finita, B la clausura entera de A en L, $n := [L : K]$ el grau, $\mathfrak{p}$ un ideal primer no nul de A, i $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ la descomposició de $\mathfrak{p}B$ en factors primers en B. Suposem, a més a més, que l'extensió $L|K$ és separable o bé que $S^{-1}B$ és un $S^{-1}A$-mòdul finitament generat (per a $S := A - \mathfrak{p}$). Aleshores se satisfà la igualtat*

$$\sum_{i=1}^{g} e_i f_i = [L : K]. \square$$

3.5 El cas galoisià

Un cas molt important per les seves aplicacions pràctiques és el cas en què l'extensió dels cossos de fraccions és una extensió de Galois. En aquest cas, les propietats generals admeten una forma més senzilla i són més fàcils d'utilitzar. Aquesta secció es destina a fer l'estudi en aquest cas particular.

Siguin, doncs, A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita, $n := [L : K]$ el grau, B la clausura entera de A en L, suposem que l'extensió $L|K$ és una extensió de Galois i posem $G := \mathrm{Gal}\,(L|K)$ per al seu grup de Galois.

Proposició 3.5.1. *Considerem un ideal primer no nul $\mathfrak{p} \subseteq A$. Aleshores, l'acció natural del grup de Galois G en el conjunt dels ideals primers $\mathfrak{P}$ de B que divideixen $\mathfrak{p}$ és transitiva.*

Demostració: En efecte, si $\sigma \in G$ és un K-automorfisme de L, aleshores la imatge $\sigma(b)$ d'un element $b \in B$ és un element de B, ja que $\sigma(b)$ és un conjugat de b sobre K i, per tant, és arrel del mateix polinomi mònic irreductible de coeficients en A que té b per arrel. Per tant, σ és un A-automorfisme de B. Ara, la imatge per un isomorfisme d'un ideal primer és un ideal primer; per tant, G opera en el conjunt dels ideals primers de B; i si $\mathfrak{P} \cap A = \mathfrak{p}$, aleshores, $\sigma(\mathfrak{P}) \cap A = \mathfrak{p}$, ja que A (i, per tant, $\mathfrak{p}$) és fix element a element per σ. Per tant, G opera en el conjunt dels ideals primers de B que divideixen un ideal primer donat $\mathfrak{p}$ en A. Resta veure que aquesta acció és transitiva.

Per a això, siguin $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_s$, $s \leq g$, els diferents ideals primers de B conjugats de $\mathfrak{P}_1 := \mathfrak{P}$. Suposem que $s < g$. Clarament, G permuta els ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ i també permuta els ideals $\mathfrak{P}_{s+1}, \ldots, \mathfrak{P}_g$; el producte $\mathfrak{P}_1 \cdots \mathfrak{P}_s$ no està inclòs en cap $\mathfrak{P}_i$ per a $i > s$, de manera que existeix $b \in \mathfrak{P}_1 \cdots \mathfrak{P}_s$ tal que $b \notin \mathfrak{P}_i$ per a tot i, $s < i \leq g$. Aleshores, $\mathrm{N}_{L|K}(b) = \prod_{\sigma \in G} \sigma(b)$ és un element del producte $\mathfrak{P}_1 \cdots \mathfrak{P}_s$ i també de A; per tant, de la intersecció, que està inclosa en $\mathfrak{P} \cap A = \mathfrak{p}$; és a dir, $\mathrm{N}_{L|K}(b) \in \mathfrak{p}$. En conseqüència, $\mathrm{N}_{L|K}(b) \in \mathfrak{P}_i$, de manera que per a algun $\sigma \in G$ és $\sigma(b) \in \mathfrak{P}_i$, ja que $\mathfrak{P}_i$ és un ideal primer de B i $\sigma(b) \in B$ per a tot $\sigma \in G$. Però aleshores, $b \in \sigma^{-1}(\mathfrak{P}_i)$, de manera que $\sigma^{-1}(\mathfrak{P}_i)$ és un dels ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$, que són els únics que poden contenir b. Això contradiu el fet que $s < g$. $\square$

En el cas galoisià, la fórmula $\sum_{i=1}^{g} e_i f_i = n$ del cas separable admet una expressió més senzilla.

Proposició 3.5.2. *Suposem que l'extensió $L|K$ és de Galois. Aleshores, tots els ideals primers $\mathfrak{P} \subseteq B$ que divideixen l'ideal primer $\mathfrak{p} \subseteq A$ tenen el mateix índex de ramificació i el mateix grau residual; és a dir, $e := e(\mathfrak{P}|\mathfrak{p})$ i $f := f(\mathfrak{P}|\mathfrak{p})$ no depenen de l'ideal primer $\mathfrak{P}$ de B que divideix $\mathfrak{p}$. A més a més, se satisfà la fórmula $n = efg$, on g és el nombre d'ideals primers de B que divideixen l'ideal $\mathfrak{p}$.*

Demostració: Si $g > 1$, siguin $\mathfrak{P} \neq \mathfrak{P}'$ dos ideals primers de B que divideixen l'ideal primer $\mathfrak{p}$ de A i sigui $\sigma \in G$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Aleshores, σ defineix un isomorfisme de $B/\mathfrak{P}$ en $B/\mathfrak{P}'$ que restringeix a la identitat sobre $A/\mathfrak{p}$; per tant, els graus residuals de $\mathfrak{P}$ i de $\mathfrak{P}'$ coincideixen. Anàlogament, com que $\sigma(\mathfrak{p}B) = \mathfrak{p}B$, la descomposició de $\mathfrak{p}B$ com a producte d'ideals primers de B es transforma per σ en ella mateixa; això vol dir que els exponents de $\mathfrak{P}$ i de $\mathfrak{P}'$ en aquesta descomposició han de coincidir; és a dir, que els índexs de ramificació de $\mathfrak{P}$ i de $\mathfrak{P}'$ són iguals. Si ara apliquem la fórmula $\sum_{i=1}^{g} e_i f_i = n$, tenint en compte que tots els e_i coincideixen i que tots els f_i també, obtenim la fórmula $n = efg$ de l'enunciat. □

Definició 3.5.3. Sigui $\mathfrak{P} \subseteq B$ un ideal primer no nul de B i sigui $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. El subgrup d'isotropia de $\mathfrak{P}$,

$$D(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

s'anomena el grup de descomposició del primer $\mathfrak{P}$ en l'extensió de Galois $B|A$.

Suposem, ara, que $\mathfrak{P}'$ és un altre ideal primer de B que divideix $\mathfrak{p}$. En virtut de la proposició **3.5.1**, existeix un automorfisme $\sigma \in G$ tal que $\mathfrak{P}' = \sigma(\mathfrak{P})$. En conseqüència, el grup de descomposició de $\mathfrak{P}'$ és conjugat del grup de descomposició de $\mathfrak{P}$; concretament, $D(\mathfrak{P}'|\mathfrak{p}) = \sigma D(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$. A més a més, l'índex de $D(\mathfrak{P}|\mathfrak{p})$ en G és el nombre d'ideals primers de B que divideixen $\mathfrak{p}$; és a dir, $D(\mathfrak{P}|\mathfrak{p})$ és un subgrup de G d'índex $g(\mathfrak{p})$; equivalentment, l'ordre del grup de descomposició és el producte $e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$.

Proposició 3.5.4. *Suposem que l'extensió $L|K$ és de Galois. Sigui $\mathfrak{P} \subseteq B$ un ideal primer no nul i sigui $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció. Aleshores, l'extensió residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ és una extensió normal; a més a més, hi ha un morfisme exhaustiu de grups $D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,((B/\mathfrak{P})|(A/\mathfrak{p}))$.*

Demostració: Sigui $b \in B$ un representant d'una classe qualsevol $b + \mathfrak{P} \in B/\mathfrak{P}$. Considerem el polinomi, de $L[X]$, $f(X) := \prod_{\sigma \in G}(X - \sigma(b))$; les arrels del polinomi $f(X)$ són els diferents conjugats de b comptats cadascun tantes vegades com el grau de l'extensió $L|K(b)$, de manera que el polinomi $f(X)$ és la potència $[L : K(b)]$-èsima del polinomi $\mathrm{Irr}(b, K)(X)$; per tant, $f(X)$ és un polinomi mònic de coeficients en $A[X]$. La reducció mòdul $\mathfrak{P}$ del polinomi $f(X)$ és un polinomi de coeficients en $A/\mathfrak{p}$ que té per arrels les classes $\sigma(b) + \mathfrak{P} \in B/\mathfrak{P}$; per tant, descompon en factors lineals en $B/\mathfrak{P}$; en conseqüència, el polinomi $\mathrm{Irr}(b + \mathfrak{P}, A/\mathfrak{p})$, que n'és un divisor, també descompon en factors lineals en

$B/\mathfrak{P}$. Això ens diu que tots els conjugats sobre $A/\mathfrak{p}$ de tots els elements de $B/\mathfrak{P}$ són elements de $B/\mathfrak{P}$; per tant, l'extensió $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ és una extensió normal.

D'altra banda, sigui $\sigma \in D(\mathfrak{P}|\mathfrak{p})$; és a dir, un A-automorfisme de B que deixa $\mathfrak{P}$ invariant. Per pas al quocient, σ defineix un $A/\mathfrak{p}$-automorfisme de $B/\mathfrak{P}$; és a dir, un element del grup de Galois de l'extensió $A/\mathfrak{p} \subseteq B/\mathfrak{P}$. D'aquesta manera s'obté un morfisme de grups $D(\mathfrak{P}|\mathfrak{p}) \xrightarrow{\pi} \mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p})$. Volem provar que π és exhaustiu. Per a això, comencem per recordar que un $A/\mathfrak{p}$-automorfisme de $B/\mathfrak{P}$ queda determinat de manera única per la seva acció sobre un element primitiu de la clausura separable de $A/\mathfrak{p}$ dins $B/\mathfrak{P}$; és a dir, que donar un element de $\mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p})$ equival a donar un conjugat sobre $A/\mathfrak{p}$ d'un tal element primitiu.

Sigui, doncs, $\overline{b} \in B/\mathfrak{P}$ un tal element primitiu; podem elegir $b \in B$ de manera que $b \equiv \overline{b} \pmod{\mathfrak{P}}$ i que $b \in \sigma^{-1}(\mathfrak{P})$ per a tot $\sigma \in G - D(\mathfrak{P}|\mathfrak{p})$; per exemple, un element que satisfaci simultàniament les congruències

$$\begin{aligned} b &\equiv \overline{b} \pmod{\mathfrak{P}}, \\ b &\equiv 0 \pmod{\sigma^{-1}(\mathfrak{P})}, \text{ per a tot } \sigma \in G - D(\mathfrak{P}|\mathfrak{p}). \end{aligned}$$

Si considerem el polinomi $f(X) := \prod_{\sigma \in G} (X - \sigma(b))$, les arrels no nul·les de la seva reducció mòdul $\mathfrak{P}$ són de la forma $\sigma(b) + \mathfrak{P}$ amb $\sigma \in D(\mathfrak{P}|\mathfrak{p})$; això diu que tots els conjugats de $\overline{b} + \mathfrak{P}$ sobre $A/\mathfrak{p}$ són les reduccions mòdul $\mathfrak{P}$ de conjugats $\sigma(b)$ de b sobre A. És a dir, donada una $A/\mathfrak{p}$-immersió de $B/\mathfrak{P}$, aleshores existeix un element $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ que la té per reducció mòdul $\mathfrak{P}$. Això demostra l'exhaustivitat de π. □

Definició 3.5.5. Sigui $\mathfrak{P} \subseteq B$ un ideal primer no nul de B i sigui $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. El nucli del morfisme $D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p})$, és a dir, el subgrup $I(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) : \sigma(b) - b \in \mathfrak{P} \text{ per a tot } b \in B\}$ de $D(\mathfrak{P}|\mathfrak{p})$ s'anomena el grup d'inèrcia del primer $\mathfrak{P}$ en l'extensió de Galois $B|A$.

En particular, el grup d'inèrcia és un subgrup normal del grup de descomposició i el seu quocient és el grup de Galois de l'extensió residual. Com que aquesta extensió residual és normal, l'ordre del seu grup de Galois és exactament el seu grau de separabilitat. Dit d'una altra manera, l'índex del grup d'inèrcia en el grup de descomposició és el grau de separabilitat de l'extensió residual. Tornarem més endavant a l'estudi dels grups de descomposició i d'inèrcia.

3.6 Discriminant

L'estudi dels ideals primers que ramifiquen en una extensió finita i entera d'anells de Dedekind $B|A$ es pot fer, en el cas separable, amb l'ajuda d'un invariant associat a l'extensió de manera natural i que serveix per a determinar el conjunt dels ideals primers de A que ramifiquen en l'extensió $B|A$: el discriminant. L'objectiu d'aquesta secció és definir i estudiar algunes de les seves propietats.

Siguin, doncs, A un domini íntegrament tancat, K el seu cos de fraccions, $L|K$ una extensió finita i separable, $n := [L : K]$ el grau de l'extensió, i B la clausura entera de A en L. Ja hem vist a la secció primera que el fet que l'extensió $L|K$ sigui separable és equivalent al fet que la forma bilineal $\mathrm{T}_{L|K}$ sigui no degenerada. Aquest fet és capital per a les propietats del discriminant.

Definició 3.6.1. Sigui $\{b_1, b_2, \ldots, b_n\}$ una K-base arbitrària de L. Anomenarem discriminant de $\{b_1, b_2, \ldots, b_n\}$ el determinant $\det\big(\mathrm{T}_{L|K}(b_i b_j)\big)$ de la matriu de la forma bilineal traça en aquesta base. Com que la forma bilineal $\mathrm{T}_{L|K}$ és no degenerada, el discriminant és un element de K^*. Escriurem $D(b_1, b_2, \ldots, b_n) := \det\big(\mathrm{T}_{L|K}(b_i b_j)\big)$. Si $b_1, b_2, \ldots, b_n$ són elements de B, aleshores $D(b_1, b_2, \ldots, b_n) \in A$, ja que $\mathrm{T}_{L|K}(b_i b_j) \in A$ per a tota parella d'elements $b_i, b_j \in B$.

Considerem una nova base $\{b'_1, b'_2, \ldots, b'_n\}$ donada a partir de la base $\{b_1, b_2, \ldots, b_n\}$ per multiplicació per una matriu P en la forma

$$(b'_1, b'_2, \ldots, b'_n) = P(b_1, b_2, \ldots, b_n).$$

Aleshores, se satisfà la igualtat $D(b'_1, b'_2, \ldots, b'_n) = \det P^2 D(b_1, b_2, \ldots, b_n)$, ja que fem un canvi de base a una forma bilineal. Per tant, els discriminants de bases diferents coincideixen mòdul quadrats de K^*.

Definició 3.6.2. Anomenarem discriminant de l'extensió $B|A$ l'ideal de A generat pels discriminants $D(b_1, b_2, \ldots, b_n)$, quan els conjunts $\{b_1, b_2, \ldots, b_n\}$ recorren totes les possibles K-bases de L formades per elements de B. El designarem amb el símbol $\Delta(B|A)$.

Lema 3.6.3. *Sigui $\{b_1, b_2, \ldots, b_n\}$ una K-base de L formada per elements de B. L'ideal extensió $D(b_1, b_2, \ldots, b_n)B$ està inclòs en el A-mòdul lliure $Ab_1 \oplus Ab_2 \oplus \cdots \oplus Ab_n$.*

Demostració: En efecte, donat $b \in B$ podem escriure $b = \sum_{i=1}^{n} a_i b_i$ amb els coeficients $a_i \in K$; en multiplicar per b_j obtenim les expressions $bb_j = \sum_{i=1}^{n} a_i b_i b_j$ i, en prendre traces, $\mathrm{T}_{L|K}(bb_j) = \sum_{i=1}^{n} a_i \mathrm{T}_{L|K}(b_i b_j)$. Com que bb_j, $b_i b_j \in B$, les seves traces pertanyen a A i la regla de Cramer per a la resolució de sistemes d'equacions lineals ens permet assegurar que els coeficients a_i s'obtenen com el quocient d'un determinant format per elements de A pel determinant de la matriu $(\mathrm{T}_{L|K}(b_i b_j))$; per tant, $a_i \in \dfrac{1}{D(b_1, b_2, \ldots, b_n)} A \subseteq K$. Això demostra la segona part. □

La propietat que demostrarem a continuació fa referència al cas que B sigui un A-mòdul lliure.

Proposició 3.6.4. *Suposem que B és un A-mòdul lliure i que el conjunt $\{b_1, b_2, \ldots, b_n\}$ és una A-base de B. Aleshores, $\Delta(B|A)$ és l'ideal principal generat per $D(b_1, b_2, \ldots, b_n)$.*

Demostració: Si $\{b'_1, b'_2, \ldots, b'_n\}$ és una altra K-base de L formada per elements de B, com que $\{b_1, b_2, \ldots, b_n\}$ és una A-base de B, existeix una matriu $(a_{i,j}) \in \mathbf{M}(n, A)$, no necessàriament invertible en A, i la matriu de la forma $\mathrm{T}_{L|K}$ en aquesta nova base és el producte $(a_{i,j})\big(\mathrm{T}_{L|K}(b_i b_j)\big)(a_{j,i})$. Per tant, $D(b'_1, b'_2, \ldots, b'_n) = \det(a_{i,j})^2 D(b_1, b_2, \ldots, b_n)$ pertany a l'ideal generat per $D(b_1, b_2, \ldots, b_n)$. □

En segon lloc, veurem que el discriminant es comporta bé per localització. Concretament, si $S \subseteq A$ és un conjunt multiplicativament tancat, aleshores $S^{-1}A$ és un domini íntegrament tancat amb cos de fraccions K i $S^{-1}B$ és la clausura entera de $S^{-1}A$ en L. Per tant, té sentit parlar del discriminant $\Delta(S^{-1}B|S^{-1}A)$.

Proposició 3.6.5. *Sigui S un subconjunt multiplicativament tancat de A. Aleshores, se satisfà la igualtat $\Delta(S^{-1}B|S^{-1}A) = S^{-1}\Delta(B|A)$.*

Demostració: La inclusió $S^{-1}\Delta(B|A) \subseteq \Delta(S^{-1}B|S^{-1}A)$ és clara. Efectivament, si $\{b_1, b_2, \ldots, b_n\}$ és una K-base de L formada per elements de B, també és una K-base de L formada per elements de $S^{-1}B$; per tant, $\Delta(B|A) \subseteq \Delta(S^{-1}B|S^{-1}A)$ i, en conseqüència, $S^{-1}\Delta(B|A) \subseteq \Delta(S^{-1}B|S^{-1}A)$.

D'altra banda, si $\{b_1, b_2, \ldots, b_n\}$ és una K-base de L formada per elements de $S^{-1}B$, podem multiplicar tots els elements b_i per un element convenient $s \in S$ de manera que $sb_i \in B$; aleshores, $D(sb_1, sb_2, \ldots, sb_n) \in \Delta(B|A)$ i de la igualtat $D(sb_1, sb_2, \ldots, sb_n) = s^{2n}D(b_1, b_2, \ldots, b_n)$, es dedueix immediatament que $D(b_1, b_2, \ldots, b_n) \in S^{-1}\Delta(B|A)$. Això demostra l'altra inclusió. □

Finalment, anem a veure una propietat que facilitarà el càlcul del discriminant en alguns casos particulars importants.

Proposició 3.6.6. *Siguin $\theta \in L$ un element primitiu de l'extensió $L|K$ i considerem $f(X) := \mathrm{Irr}(\theta, K)(X)$ el polinomi mònic irreductible de $K[X]$ que té θ per arrel. Aleshores,*

$$D(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{n(n-1)/2}\mathrm{N}_{L|K}(f'(\theta)),$$

on $f'(X)$ denota el polinomi derivat del polinomi $f(X)$.

Demostració: Podem escriure $f(X) = (X - \theta_1)\cdots(X - \theta_n)$ on $\theta_1, \ldots, \theta_n$ són els n conjugats diferents de $\theta =: \theta_1$. En derivar la igualtat i substituir en θ_i obtenim que

$$f'(\theta_i) = \prod_{j\neq i}(\theta_i - \theta_j); \qquad \text{i, per tant, que} \qquad \prod_{i=1}^{n} f'(\theta_i) = \prod_{i=1}^{n}\prod_{j\neq i}(\theta_i - \theta_j).$$

Com que el polinomi $f'(X)$ és de coeficients en el cos K, la norma $\mathrm{N}_{L|K}(f'(\theta))$ pot ésser calculada com el producte $\mathrm{N}_{L|K}(f'(\theta)) = \prod_{i=1}^{n} f'(\theta_i)$ dels conjugats de $f'(\theta)$. D'altra banda, el discriminant es pot calcular en la forma $D(1, \theta, \ldots, \theta^{n-1}) = \det(\theta_i^{j-1})^2$, com ja ha estat provat anteriorment (cf. la proposició **3.1.5**). Per tant, i com que el determinant de la matriu de Vandermonde

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots & \theta_n^{n-1} \end{bmatrix}$$

és el producte $\prod_{i=2}^{n}\prod_{j<i}(\theta_i - \theta_j)$, obtenim la igualtat

$$D(1, \theta, \ldots, \theta^{n-1}) = \prod_{i=2}^{n}\prod_{j<i}(\theta_i - \theta_j)^2 = (-1)^{n(n-1)/2}\prod_{i=1}^{n}\prod_{j\neq i}(\theta_i - \theta_j)$$

que, combinada amb la que dóna la norma de $f'(\theta)$, fa el resultat evident. □

Un exemple important de discriminant és el discriminant de les successives potències d'una arrel de la unitat; aquest discriminant el farem servir més endavant.

Proposició 3.6.7. *Sigui $\zeta_n \in \mathbb{C}$ una arrel primitiva n-èsima de la unitat. Aleshores,*

$$D(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\varphi(n)-1}) = (-1)^{\varphi(n)(\varphi(n)-1)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Demostració: La demostració que farem està basada en el coneixement dels polinomis ciclotòmics $\Phi_n(X)$; més concretament, en les dues fórmules següents:

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)},$$

per a tot nombre natural n, i on μ denota la funció de Möbius, i

$$\Phi_{n'}(X)\Phi_{n'p}(X) = \Phi_{n'}(X^p),$$

sempre que p sigui un nombre natural primer que no divideix n' (cf., per exemple, [Tra 2020]). Els casos $n = 1$ i $n = 2$ no tenen cap dificultat; per tant, podem suposar que $n > 2$.

En derivar la primera d'aquestes fórmules i substituir en ζ_n s'obté l'expressió

$$\Phi_n'(\zeta_n) = \zeta_n^{-1} n \prod_{d|n,\, d\neq n} (\zeta_n^d - 1)^{\mu(n/d)}.$$

La proposició **3.6.6** ja dóna el signe enunciat, de manera que només hem de calcular la norma $\mathrm{N}_n(\Phi_n'(\zeta_n))$, on posem N_n per a indicar la norma de l'extensió $\mathbb{Q}(\zeta_n)|\mathbb{Q}$. El fet que la norma sigui multiplicativa, com també la seva transitivitat per a cadenes d'extensions, ens legitimen a escriure consecutivament les igualtats

$$\begin{aligned}
\mathrm{N}_n(\Phi_n'(\zeta_n)) &= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq n} \mathrm{N}_n(\zeta_n^d - 1)^{\mu(n/d)} \\
&= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq n} \mathrm{N}_n(\zeta_{n/d} - 1)^{\mu(n/d)} \\
&= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq 1} \mathrm{N}_n(\zeta_d - 1)^{\mu(d)} \\
&= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq 1} \mathrm{N}_d(\zeta_d - 1)^{\mu(d)\varphi(n)/\varphi(d)}.
\end{aligned}$$

Observem, en primer lloc, que per a tot nombre natural $n > 2$ és $\mathrm{N}_n(\zeta_n) = 1$, ja que l'invers de cada conjugat de ζ també és un conjugat de ζ i són diferents. D'altra banda, com que $d \neq 1$, és $\zeta_d \neq 1$ i $\mathrm{N}_d(\zeta_d - 1) \neq 0$. Si d és divisible pel quadrat d'un nombre primer, aleshores $\mu(d) = 0$ i el factor $\mathrm{N}_d(\zeta_d - 1)^{\mu(d)\varphi(n)/\varphi(d)}$ val 1. Per tant, el producte s'estén als naturals $d \neq 1$ diferents de n que són lliures de quadrats.

Ara, podem observar que $\mathrm{N}_d(\zeta_d - 1) = (-1)^{\varphi(d)} \mathrm{N}_d(1 - \zeta_d)$, de manera que els factors del producte són $\mathrm{N}_d(1 - \zeta_d)^{\mu(d)\varphi(n)/\varphi(d)}$, ja que el signe és $(-1)^{\mu(d)\varphi(n)} = 1$, perquè el nombre $\varphi(n)$ és parell per a tot $n > 2$. D'aquesta manera obtenim l'expressió

$$\mathrm{N}_n(\Phi_n'(\zeta_n)) = n^{\varphi(n)} \prod_{d|n,\, d\neq 1} \mathrm{N}_d(1 - \zeta_d)^{\mu(d)\varphi(n)/\varphi(d)},$$

el producte estès a tots els nombres naturals d lliures de quadrats i diferents de 1 que divideixen n.

De la segona de les fórmules generals pels polinomis ciclotòmics que hem escrit es dedueix que $\Phi_d(1) = 1$ per a tot nombre natural d que sigui divisible per dos o més nombres primers diferents; en efecte, com que $1 \in \mathbb{Q}$, 1 no pot ser arrel de cap polinomi ciclotòmic $\Phi_d(X)$, de manera que de la igualtat $\Phi_{n'}(1)\Phi_{n'p}(1) = \Phi_{n'}(1)$ es dedueix que $\Phi_{n'p}(1) = 1$. D'altra banda, per a tot nombre natural primer p que divideix n se satisfà la igualtat $\mathrm{N}_p(1-\zeta_p) = \Phi_p(1) = p$, ja que $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$. En portar aquests càlculs a la fórmula anterior obtenim la fórmula que volíem provar. □

3.7 Discriminant i ramificació

En aquesta secció es tracta de veure quina relació té el discriminant amb la ramificació. Per a això, ens posarem en la situació en què A és un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i separable, $n := [L : K]$ el grau de l'extensió, i B la clausura entera de A en L. Aleshores, l'ideal discriminant $\Delta(B|A)$ descompon de manera única com a producte d'ideals primers no nuls de A. Es tracta de provar que el conjunt dels ideals primers de A que ramifiquen en B està format exactament pels ideals primers que divideixen el discriminant.

Comencem per estudiar una mica més de prop el comportament local del discriminant i de la ramificació. Sigui $\mathfrak{p} \subseteq A$ un ideal primer no nul i sigui $S := A - \mathfrak{p}$. Aleshores, $S^{-1}\mathfrak{p} := \mathfrak{p}S^{-1}A$ és un ideal primer de $S^{-1}A$ i, en virtut de la proposició **3.6.5**, condició necessària i suficient perquè $\Delta(B|A) \subseteq \mathfrak{p}$ és que $\Delta(S^{-1}B|S^{-1}A) \subseteq S^{-1}\mathfrak{p}$. D'altra banda, $S^{-1}A$ és un anell de Dedekind local i $S^{-1}B$ és la clausura entera de $S^{-1}A$ en L; a més a més, si $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ és la descomposició de $\mathfrak{p}B$ en B, la descomposició de $\mathfrak{p}S^{-1}B$ en $S^{-1}B$ és $\mathfrak{p}S^{-1}B = (S^{-1}\mathfrak{P}_1)^{e_1} \cdots (S^{-1}\mathfrak{P}_g)^{e_g}$ i l'extensió residual $S^{-1}A/S^{-1}\mathfrak{p} \subseteq S^{-1}B/S^{-1}\mathfrak{P}_i$ és l'extensió $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$; per tant, condició necessària i suficient perquè l'ideal $\mathfrak{p} \subseteq A$ ramifiqui en B és que l'ideal $S^{-1}\mathfrak{p} \subseteq S^{-1}A$ ramifiqui en $S^{-1}B$. Però, ara, els anells $S^{-1}A$ i $S^{-1}B$ són anells de Dedekind principals i $S^{-1}B$ és un $S^{-1}A$-mòdul lliure de rang n; de manera que l'ideal discriminant $\Delta(S^{-1}B|S^{-1}A)$ és principal i generat pel discriminant d'una $S^{-1}A$-base de $S^{-1}B$ (cf. la proposició **3.6.4**).

Aquestes consideracions fan que puguem suposar d'entrada que A és un anell de Dedekind principal i local i que $\mathfrak{p}$ és l'únic ideal primer no nul de A. Si $\{b_1, b_2, \ldots, b_n\}$ és una A-base de B, aleshores és una K-base de L i $\{b_1 + \mathfrak{p}B, b_2 + \mathfrak{p}B, \ldots, b_n + \mathfrak{p}B\}$ és una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$. Això ja ha estat provat en el transcurs de la secció quarta.

Sigui $b \in B$ un element qualsevol. La multiplicació per b en B es pot considerar com una aplicació A-lineal $\mathfrak{m}_b : B \longrightarrow B$ que, en la A-base $\{b_1, b_2, \ldots, b_n\}$ de B admet una certa matriu $(a_{i,j}) \in \mathbf{M}(n, A)$. La reducció mòdul $\mathfrak{p}B$ d'aquesta aplicació lineal dóna lloc a una aplicació $A/\mathfrak{p}A$-lineal $\overline{\mathfrak{m}}_b : B/\mathfrak{p}B \longrightarrow B/\mathfrak{p}B$ de multiplicació, en $B/\mathfrak{p}B$, per la classe $b+\mathfrak{p}B$; i aquesta aplicació admet, en la $A/\mathfrak{p}$-base $\{b_1+\mathfrak{p}B, b_2+\mathfrak{p}B, \ldots, b_n+\mathfrak{p}B\}$ de $B/\mathfrak{p}B$, la matriu reduïda $(a_{i,j}+\mathfrak{p}) \in \mathbf{M}(n, A/\mathfrak{p}A)$. En particular, se satisfà que $\mathrm{T}_{L|K}(b)+\mathfrak{p} = \mathrm{tr}(\overline{\mathfrak{m}}_b)$, de manera que la reducció mòdul $\mathfrak{p}$ del discriminant $D_{B|A}(b_1, b_2, \ldots, b_n)$ és el determinant $\overline{D}(b_1, b_2, \ldots, b_n) := \det\left[\mathrm{tr}\left((b_i + \mathfrak{p}B)(b_j + \mathfrak{p}B)\right)\right]$.

Com que $\Delta(B|A)$ és generat per $D(b_1, b_2, \ldots, b_n)$, dir que $\Delta(B|A) \subseteq \mathfrak{p}$ equival a dir que $D(b_1, b_2, \ldots, b_n) \in \mathfrak{p}$, o sigui, que $\overline{D}(b_1, b_2, \ldots, b_n) = 0$ en $A/\mathfrak{p}$. Per tant, cal provar

que condició necessària i suficient perquè $\mathfrak{p}$ ramifiqui en B és que $\overline{D}(b_1, b_2, \ldots, b_n) = 0$ en $A/\mathfrak{p}$. Per a això, sigui $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ la descomposició de $\mathfrak{p}B$ com a producte d'ideals primers de B. El teorema xinès del residu ens legitima a escriure la descomposició

$$B/\mathfrak{p}B \cong \bigoplus_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$$

de $B/\mathfrak{p}B$ com a suma directa de subespais vectorials sobre $A/\mathfrak{p}$. Podem considerar una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$ construïda reunint bases dels sumands $B/\mathfrak{P}_i^{e_i}$; si $\theta \in B/\mathfrak{p}B$ és un element qualsevol i $\theta = \theta_1 + \cdots + \theta_g$ és la descomposició de θ en sumands $\theta_i \in B/\mathfrak{P}_i^{e_i}$, la matriu de la multiplicació per θ en $B/\mathfrak{p}B$ en aquesta nova base s'expressa en forma de matriu de caixes a la diagonal, cada una d'elles corresponent a la matriu de la multiplicació per θ_i en la base que hem pres en $B/\mathfrak{P}_i^{e_i}$ per a construir per reunió la base de $B/\mathfrak{p}B$. En particular, això ens permet assegurar que la traça de l'aplicació lineal de multiplicació per θ en $B/\mathfrak{p}B$ és la suma de les traces de les aplicacions lineals de multiplicació per θ_i en cada $B/\mathfrak{P}_i^{e_i}$. En conseqüència, la matriu de les traces dels productes pren la forma d'una matriu de caixes a la diagonal on cada una és la matriu de les traces dels productes dels elements de la base de $B/\mathfrak{P}_i^{e_i}$, ja que els productes d'elements de diferents factors $B/\mathfrak{P}_i^{e_i}$ s'anul·len. Com que els determinants de les matrius d'una forma bilineal simètrica en dues bases diferents són iguals llevat de la multiplicació pel quadrat del determinant de la matriu del canvi de base, i aquest determinant sempre és invertible, obtenim la fórmula

$$\overline{D}(b_1, b_2, \ldots, b_n) = \det P^2 \prod_{i=1}^{g} \overline{D}_i,$$

on $\overline{D}_i$ és el determinant de la matriu de les traces dels productes dels elements de la base que hem triat en $B/\mathfrak{P}_i^{e_i}$.

Suposem que l'ideal primer $\mathfrak{p}$ és no ramificat en B; és a dir, que per a $1 \leq i \leq g$ l'extensió $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$ és separable i $e_i = 1$. Com que les extensions $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$ són separables, els determinants $\overline{D}_i$ són no nuls i obtenim que $\overline{D}(b_1, b_2, \ldots, b_n) \neq 0$ en $A/\mathfrak{p}$, com volíem veure. Recíprocament, cal veure que si $\mathfrak{p}$ ramifica en B, aleshores $\overline{D}(b_1, b_2, \ldots, b_n) = 0$. Suposem, primer, que $e_1 > 1$. Podem elegir la $A/\mathfrak{p}$-base de $B/\mathfrak{P}_1^{e_1}$ completant bases en la filtració de $B/\mathfrak{P}_1^{e_1}$ donada pels ideals (i $A/\mathfrak{p}$-espais vectorials) $\mathfrak{P}_1^a/\mathfrak{P}_1^{e_1}$, $e_1 - 1 \geq a \geq 0$; el fet que el primer vector d'aquesta base sigui nilpotent (la seva potència e_1-èsima s'anul·la) fa que l'aplicació lineal de multiplicació per aquest element sigui un endomorfisme nilpotent de $B/\mathfrak{P}_1^{e_1}$ i, per tant, tots els valors propis siguin nuls. Anàlogament, els productes d'aquest element per qualsevol altre també són nilpotents i el mateix succeeix amb els endomorfismes de $B/\mathfrak{P}_1^{e_1}$ de multiplicació per aquests productes; per tant, les traces dels productes són nul·les i la matriu que serveix per a calcular el determinant $\overline{D}_1$ té una columna de zeros. Per tant, $\overline{D}_1 = 0$. Resta el cas que tots els índexs de ramificació siguin trivials, però que alguna de les extensions $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$ no sigui separable. Però, en aquest cas, la forma traça en $B/\mathfrak{P}_i$ és la forma nul·la i $\overline{D}_i = 0$.

En resum, hem demostrat el resultat següent.

Proposició 3.7.1. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i separable, B la clausura entera de A en L i $\mathfrak{p}$ un ideal primer no nul de A. Condició necessària i suficient perquè l'ideal $\mathfrak{p}$ ramifiqui en l'extensió $B|A$ és que el discriminant $\Delta(B|A)$ sigui divisible per $\mathfrak{p}$.* □

3.8 El cas quadràtic

En el capítol anterior hem calculat exactament l'anell dels enters de tots els cossos quadràtics. Ara podem calcular el determinant i les lleis de descomposició de tots els ideals primers de $\mathbb{Z}$ en un cos quadràtic. Comencem pel discriminant.

Proposició 3.8.1. *Siguin D un nombre enter lliure de quadrats i $K := \mathbb{Q}(\sqrt{D})$. Aleshores, el discriminant de l'extensió $K|\mathbb{Q}$ és el nombre enter $4D$ si $D \not\equiv 1 \pmod 4$ i és D si $D \equiv 1 \pmod 4$.*

Demostració: Com que $\mathbb{Z}$ és principal, el discriminant de l'extensió quadràtica $K|\mathbb{Q}$ és l'ideal principal generat pel discriminant $D(1,\omega)$ on podem prendre per a $\{1,\omega\}$ la base de l'anell dels enters de K que hem determinat anteriorment (cf. la proposició **2.2.2**). Concretament, si $D \not\equiv 1 \pmod 4$, podem prendre $\omega = \sqrt{D}$. En aquest cas, la matriu de la forma bilineal traça és la matriu

$$\begin{bmatrix} \mathrm{T}(1) & \mathrm{T}(\sqrt{D}) \\ \mathrm{T}(\sqrt{D}) & \mathrm{T}(D) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2D \end{bmatrix},$$

ja que el polinomi irreductible de $\sqrt{D}$ i, per tant, el polinomi característic de la multiplicació per $\sqrt{D}$ en $\mathcal{O}_K$ és el polinomi $X^2 - D$. Això fa que $D(1,\sqrt{D}) = 4D$, com volíem demostrar.

En el cas $D \equiv 1 \pmod 4$, podem prendre $2\omega = 1 + \sqrt{D}$ (o bé $2\omega = D + \sqrt{D}$) i repetir el càlcul que hem fet en l'altre cas. Però, amb la finalitat de veure una altra manera de calcular el discriminant, utilitzarem la fórmula

$$D(1,\omega,\ldots,\omega^{n-1}) = \det(\sigma_i(\omega^{j-1}))^2,$$

on σ_i recorre el conjunt de les immersions diferents de K en $\overline{\mathbb{Q}}$, que hem obtingut a la demostració de la proposició **3.1.5** en la forma

$$D(1,\omega,\ldots,\omega^{n-1}) = \det V^2$$

on $V = (\sigma_i(\omega^{j-1}))$ és la matriu de Vandermonde dels conjugats de ω. Calculem:

$$D(1,\omega) = \det \begin{bmatrix} 1 & 1 \\ \dfrac{1+\sqrt{D}}{2} & \dfrac{1-\sqrt{D}}{2} \end{bmatrix}^2 = (-\sqrt{D})^2 = D. \square$$

En conseqüència, els ideals primers de $\mathbb{Z}$ que ramifiquen a l'extensió $K|\mathbb{Q}$ són els generats pels nombres primers que divideixen D, si $D \equiv 1 \pmod 4$, i, a més a més, 2, en el cas que $D \equiv 2,3 \pmod 4$. Com que l'extensió és de grau 2 i les extensions residuals són separables, això vol dir que l'extensió d'aquests primers és el quadrat d'un ideal primer de K. D'altra banda, només queden dues possibilitats per a la descomposició dels altres ideals primers de $\mathbb{Z}$ en K: o bé l'ideal primer de $\mathbb{Z}$ continua essent un ideal primer un cop estès a K, i en aquest cas es diu que el primer és inert, o bé el primer descompon com a producte de dos ideals primers diferents de K; en aquest cas es diu que el primer descompon completament.

El resultat següent explica com descomponen tots els primers de $\mathbb{Z}$ en l'extensió quadràtica $\mathbb{Q}(\sqrt{D})|\mathbb{Q}$.

Proposició 3.8.2. *Siguin D un nombre enter lliure de quadrats, $K := \mathbb{Q}(\sqrt{D})$, $\mathcal{O}_K$ l'anell dels enters de K, i p un nombre natural primer. Si p divideix el discriminant de l'extensió quadràtica $K|\mathbb{Q}$, aleshores, $p\mathcal{O}_K = \mathfrak{p}^2$, on $\mathfrak{p}$ és un ideal primer de $\mathcal{O}_K$ de grau residual 1; si $p \neq 2$ i D és un residu quadràtic mòdul p, aleshores $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, el producte de dos ideals primers diferents de $\mathcal{O}_K$ de grau residual 1; si $p \neq 2$ i D no és un residu quadràtic mòdul p, aleshores $p\mathcal{O}_K$ és un ideal primer de $\mathcal{O}_K$ de grau residual 2. Finalment, $2\mathcal{O}_K$ és el producte de dos ideals primers diferents de $\mathcal{O}_K$ de grau residual 1 si $D \equiv 1 \pmod 8$ i $2\mathcal{O}_K$ és un ideal primer de $\mathcal{O}_K$ de grau residual 2 si $D \equiv 5 \pmod 8$.*

Demostració: El cas dels ideals primers que ramifiquen és clar. Per tant, podem suposar que l'ideal primer $p\mathbb{Z}$ no ramifica en l'anell $\mathcal{O}_K$ dels enters de K. Comencem per estudiar el cas $p \neq 2$. Hem d'estudiar la descomposició de l'anell $\mathcal{O}_K/p\mathcal{O}_K$ com a producte de cossos, ja que una condició necessària i suficient perquè l'ideal $p\mathcal{O}_K$ sigui primer és que l'anell quocient $\mathcal{O}_K/p\mathcal{O}_K$ sigui un cos. De nou, el càlcul de l'anell dels enters de K dóna que l'anell $\mathcal{O}_K$, com a grup abelià, és la suma dels subgrups $\mathbb{Z}$ i $\omega\mathbb{Z}$, ω com a la proposició anterior. En el cas $D \not\equiv 1 \pmod 4$, l'anell $\mathcal{O}_K/p\mathcal{O}_K$ és l'anell $\mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}]$; i en el cas $D \equiv 1 \pmod 4$, si calculem $\mathcal{O}_K/p\mathcal{O}_K$ podem observar que aquest anell també és l'anell $\mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}]$, ja que, per a $a, b \in \mathbb{Z}$ és $a + b\,\dfrac{1+\sqrt{D}}{2} \equiv a + (b+p)\,\dfrac{1+\sqrt{D}}{2}$ $(\mathrm{mod}\ p\mathcal{O}_K)$, de manera que si b és senar, aleshores $b + p$ és parell i $(b+p)\,\dfrac{1+\sqrt{D}}{2}$ és la suma d'un nombre enter amb un múltiple enter de $\sqrt{D}$. Per tant, cal descompondre $\mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}]$ en producte de cossos. Ara bé,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[X]/(p, X^2 - D) \cong \mathbb{F}_p[X]/(X^2 - D);$$

per tant, i com que el polinomi $X^2 - D$ és separable en $\mathbb{F}_p[X]$, l'anell quocient $\mathcal{O}_K/p\mathcal{O}_K$ és un cos exactament quan el polinomi $X^2 - D$ és irreductible en $\mathbb{F}_p[X]$, i descompon en producte de dos cossos isomorfs a $\mathbb{F}_p$ quan el polinomi $X^2 - D$ té dues arrels diferents en $\mathbb{F}_p$. Això acaba el cas $p \neq 2$.

Per a $p = 2$ només cal considerar el cas $D \equiv 1 \pmod 4$, ja que en cas contrari 2 ramifica, en virtut de la proposició anterior. En aquest cas, ω admet com a polinomi irreductible el polinomi $X^2 - X + \dfrac{1-D}{4}$, de manera que si b és la classe mòdul 2 de $\dfrac{1-D}{4}$, aleshores

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[X]/(2, X^2 - X + \frac{1-D}{4}) \cong \mathbb{F}_2[X]/(X^2 - X + b).$$

Però condició necessària i suficient perquè el polinomi (separable) $X^2 - X + b$ sigui irreductible en $\mathbb{F}_2[X]$ és que $b = 1$ en $\mathbb{F}_2$; i això equival a dir que $D \equiv 5 \pmod 8$. □

Corol·lari 3.8.3. *Les lleis de descomposició dels ideals primers de $\mathbb{Z}$ en el cos quadràtic $K := \mathbb{Q}(\sqrt{D})$ són donades pel caràcter quadràtic de Kronecker, χ_D. Concretament,*

$$\chi_D(p) = \begin{cases} 0, & \text{si } p \text{ ramifica,} \\ 1, & \text{si } p \text{ descompon completament,} \\ -1, & \text{si } p \text{ és inert.} \end{cases}$$

DEMOSTRACIÓ: Per al cas dels nombres primers senars p, només cal recordar que el caràcter de Kronecker χ_D és l'únic caràcter quadràtic de Dirichlet definit mòdul $4|D|$ per al qual se satisfà la igualtat $\chi_D(p) = \left(\frac{D}{p}\right)$ per a tot nombre primer senar p. I per al cas $p = 2$ només observar que si $D \equiv 1 \pmod 4$, aleshores el valor de $\chi_D(2)$ és donat exactament per $(-1)^{\omega(D)}$. □

Una aplicació aritmètica interessant de les lleis de descomposició dels ideals primers de $\mathbb{Z}$ en l'anell dels enters de Gauss $\mathbb{Z}[i]$ és l'obtenció d'aquells nombres enters que són suma de dos quadrats. En efecte, podem demostrar molt fàcilment el teorema següent.

Teorema 3.8.4. *Sigui $n \in \mathbb{Z}$ un nombre enter positiu qualsevol. Aleshores, n és la suma dels quadrats de dos nombres enters si, i només si, tots els nombres primers senars que divideixen n amb exponent senar són de la forma $p \equiv 1 \pmod 4$.*

DEMOSTRACIÓ: En primer lloc, l'anell $\mathbb{Z}[i]$ dels enters de Gauss és l'anell dels enters de $\mathbb{Q}(i)$. Observem que per a $a, b \in \mathbb{Z}$ és $\mathrm{N}_{\mathbb{Q}(i)|\mathbb{Q}}(a + bi) = a^2 + b^2$, una suma de dos quadrats, de manera que un nombre enter n és suma dels quadrats de dos nombres enters exactament quan és norma d'un element de $\mathbb{Z}[i]$. D'altra banda, és ben conegut que $\mathbb{Z}[i]$ és un anell euclidià i, per tant, principal. A més a més, $i = \sqrt{-1}$ i $-1 \equiv 3 \pmod 4$, de manera que $\Delta(\mathbb{Z}[i]|\mathbb{Z}) = 4\mathbb{Z}$; per tant $2\mathbb{Z}$ és el quadrat d'un ideal primer de $\mathbb{Z}[i]$. Per a p un natural primer senar, condició necessària i suficient perquè $p\mathbb{Z}[i]$ sigui el producte de dos ideals primers diferents de $\mathbb{Z}[i]$ és que $p \equiv 1 \pmod 4$, ja que el valor del caràcter de Kronecker χ_{-1} en un primer senar p és exactament $(-1)^{\varepsilon(p)}$. D'aquesta manera, si $p \equiv 1 \pmod 4$, aleshores, existeixen ideals primers $\mathfrak{p}_1, \mathfrak{p}_2$ en $\mathbb{Z}[i]$ tals que $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$; si $a + bi$ és un generador d'un d'aquests ideals primers, ha de ser $\mathrm{N}(a + bi) = a^2 + b^2 = p$, ja que $\mathrm{N}(a+bi)$ ha de ser un divisor no trivial de $\mathrm{N}(p) = p^2$. En conseqüència, si $p \equiv 1 \pmod 4$, i també si $p = 2 = 1^2 + 1^2 = \mathrm{N}(1 + i) = \mathrm{N}(1 - i)$, p és suma dels quadrats de dos nombres enters. Com que la norma és multiplicativa i tot quadrat és suma de dos quadrats, la condició de l'enunciat és suficient.

Però també és necessària. Suposem que n és la suma dels quadrats de dos nombres enters; és a dir, la norma d'un element $\alpha \in \mathbb{Z}[i]$. Sigui $p \equiv 3 \pmod 4$ un natural primer que divideix n; aleshores, l'ideal $p\mathbb{Z}[i]$ és un ideal primer de $\mathbb{Z}[i]$ i l'exponent de p en la descomposició en factors primers de $n = \mathrm{N}(\alpha)$ és dues vegades l'exponent de $p\mathbb{Z}[i]$ en la descomposició en primers de l'ideal $\alpha\mathbb{Z}[i]$, ja que $\mathrm{N}(p) = p^2$. □

3.9 El cas ciclotòmic

Ja hem comentat més amunt la importància que tenen els cossos ciclotòmics. En aquesta secció es tracta de fer un estudi d'algunes de les seves propietats aritmètiques. Concretament, estudiarem quin és el seu anell d'enters, quin és el seu discriminant, i quines són les lleis de descomposició dels ideals primers en aquests anells.

Considerem, doncs, un nombre enter $n > 1$, una arrel primitiva n-èsima de la unitat $\zeta := \zeta_n \in \mathbb{C}$, el cos ciclotòmic $K := \mathbb{Q}(\zeta)$ i l'anell dels enters de K, $A := \mathcal{O}_K$. És ben conegut que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ i que el conjunt $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1}$ és una $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$, on φ designa la funció d'Euler. Ja hem calculat el discriminant $D(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})$; això ens dóna informació sobre el conjunt dels ideals primers de $\mathbb{Z}$ que ramifiquen en A.

Corol·lari 3.9.1. *Sigui p un natural primer que ramifica en $\mathbb{Q}(\zeta_n)$. Aleshores, p divideix n.*

Demostració: El discriminant de l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és l'ideal principal generat pel discriminant d'una $\mathbb{Z}$-base de l'anell dels enters de $\mathbb{Q}(\zeta)$. Com que $\zeta \in A$, el discriminant $D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$ és el producte del discriminant d'aquesta base pel quadrat del determinant de la matriu dels elements ζ^i expressats en aquesta base; aquesta matriu és de coeficients enters i, per tant, el discriminant de l'extensió divideix l'ideal generat per $D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$. Per tant, el discriminant de l'extensió divideix $n^{\varphi(n)}$. Com que els idelas primers que ramifiquen divideixen el discriminant, si p ramifica, aleshores p ha de dividir n. □

Aquest resultat té un recíproc. Si n és un natural senar, aleshores $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$, de manera que en parlar de cossos ciclotòmics podem suposar sempre que $n \not\equiv 2 \pmod 4$. En aquestes condicions, els ideals primers de $\mathbb{Z}$ que ramifiquen en $\mathbb{Q}(\zeta)$ són exactament els ideals $p\mathbb{Z}$ tals que p divideix n. Per a demostrar-ho, començarem pel cas que n sigui potència d'un nombre primer.

Proposició 3.9.2. *Suposem que p és un natural primer i que $n = p^r$, $r \geq 1$. Sigui $\alpha := 1 - \zeta \in \mathbb{Q}(\zeta)$. Aleshores:*

(a) *L'ideal principal αA és un ideal primer.*

(b) *El grau residual de αA és 1.*

(c) *L'ideal pA és la potència $\varphi(n)$-èsima de l'ideal primer αA.*

Demostració: Com que les arrels de la unitat són nombres enters algebraics, és clar que $\zeta \in A$; per tant, αA és un ideal enter de $\mathbb{Q}(\zeta)$. Sigui $f(X) := \Phi_{p^r}(X)$ el polinomi ciclotòmic; és ben conegut que

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

Per a tot nombre enter i se satisfà la fórmula $u_i := \dfrac{1 - \zeta^i}{1 - \zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{i-1}$, de manera que $u_i \in A$; i si i no és divisible per p, en intercanviar els papers de ζ i ζ^i, obtenim també que $u_i^{-1} \in A$, de manera que u_i és un element invertible de A. Això fa que a partir de la igualtat $f(X) = \displaystyle\prod_{\mathrm{mcd}(i,p)=1} (X - \zeta^i)$ puguem escriure

$$p = f(1) = \prod_{\mathrm{mcd}(i,p)=1} (1 - \zeta^i) = u(1 - \zeta)^{\varphi(n)},$$

on $u = \displaystyle\prod_{\mathrm{mcd}(i,p)=1} u_i$ és invertible en A. En particular, els elements $1 - \zeta^i$, $\mathrm{mcd}(i, p) = 1$, i α són associats (generen el mateix ideal) i l'ideal pA és la potència $\varphi(n)$-èsima de l'ideal principal αA. Com que $p\mathbb{Z}$ és un ideal primer de $\mathbb{Z}$ i l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és de Galois, la fórmula $efg = n$ ens permet assegurar que l'ideal αA és un ideal primer de A de grau residual 1. □

Corol·lari 3.9.3. *Siguin $n \not\equiv 2 \pmod 4$ un nombre natural, que escriurem en la forma $n = p^r n'$, amb $r \geq 0$ i $\mathrm{mcd}(p, n') = 1$, i $\mathfrak{P} \subseteq A$ un ideal primer de A que divideix p. Aleshores, $e(\mathfrak{P}|p\mathbb{Z}) = \varphi(p^r)$. En particular, condició necessària i suficient perquè p ramifiqui en $\mathbb{Q}(\zeta)$ és que p divideixi n.*

Demostració: Podem considerar les dues cadenes d'extensions $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{n'}) \subseteq \mathbb{Q}(\zeta_n)$ i $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{p^r}) \subseteq \mathbb{Q}(\zeta_n)$. Acabem de provar que l'extensió $\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}$ només ramifica en el primer $p\mathbb{Z}$ i que l'índex de ramificació és $\varphi(p^r)$; per tant, l'extensió $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ ramifica en $p\mathbb{Z}$ i l'índex de ramificació de $p\mathbb{Z}$ és un múltiple de $\varphi(p^r)$. D'altra banda, en virtut del corol·lari **3.9.1**, l'extensió $\mathbb{Q}(\zeta_{n'})|\mathbb{Q}$ no ramifica en cap ideal primer de $\mathbb{Q}(\zeta_{n'})$ que divideix $p\mathbb{Z}$; en conseqüència, si $\mathfrak{P}$ és un ideal primer de $\mathbb{Q}(\zeta_n)$ que contrau a $p\mathbb{Z}$, i si $\mathfrak{p}$ és la contracció de $\mathfrak{P}$ a $\mathbb{Q}(\zeta_{n'})$, aleshores, $e(\mathfrak{P}|p\mathbb{Z}) = e(\mathfrak{P}|\mathfrak{p})$ divideix el grau $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n'})] = \varphi(p^r)$. Per tant, la igualtat $e(\mathfrak{P}|p\mathbb{Z}) = \varphi(p^r)$. □

A continuació determinarem el grau residual de tots els ideals primers. Començarem per demostrar el resultat següent.

Lema 3.9.4. *Siguin ℓ un nombre natural primer que no divideix n i $\mathfrak{l} \subseteq A$ un ideal primer que divideix ℓA. Aleshores, les classes residuals de les potències $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ en el cos residual $A/\mathfrak{l}$ són totes diferents. A més a més, si $f := f(\mathfrak{l}|\ell)$ designa el grau residual en $\mathfrak{l}$, aleshores $\ell^f \equiv 1 \pmod n$.*

Demostració: El polinomi $X^n - 1 \in \mathbb{Z}[X]$ és separable sobre $\mathbb{Z}$ i sobre $\mathbb{F}_\ell$, ja que ℓ no divideix n. Per tant, la reducció mòdul $\mathfrak{l}$ de les arrels diferents de $f(X)$, $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, han de ser arrels diferents de $X^n - 1$ en $\overline{\mathbb{F}}_\ell$. Això demostra la primera afirmació. D'altra banda, el conjunt $\{\zeta^i \in A/\mathfrak{l} : 0 \leq i \leq n-1\}$ és un subgrup d'ordre n de $(A/\mathfrak{l})^*$, que és d'ordre $\ell^f - 1$. Per tant, n divideix $\ell^f - 1$. □

Lema 3.9.5. *Sigui ℓ un nombre natural primer que no divideix n. Llavors, $A = \ell A + \mathbb{Z}[\zeta]$.*

Demostració: Cal demostrar que per a tot element $b \in A$ existeix $b' \in \mathbb{Z}[\zeta]$ tal que $b - b' \in \ell A$. Posem $D := D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$; aleshores, $D \in \mathbb{Z}$ i ℓ no divideix D, ja que D divideix una potència de n. En conseqüència, D és invertible a $\mathbb{Z}/\ell\mathbb{Z}$; és a dir, existeix $D' \in \mathbb{Z}$ tal que $DD' \equiv 1 \pmod \ell$. Això ens permet assegurar que $b \equiv DD'b \pmod{\ell A}$. Però, en virtut del lema **3.6.3**, $Db \in \mathbb{Z}[\zeta]$, de manera que $DD'b \in \mathbb{Z}[\zeta]$ i podem prendre $b' = DD'b$. □

Corol·lari 3.9.6. *Siguin ℓ un nombre natural primer que no divideix n i f un nombre natural qualsevol tal que $\ell^f \equiv 1 \pmod n$. Llavors, per a tot element $b \in A$ és $b^{\ell^f} - b \in \ell A$.*

Demostració: Acabem de provar que existeixen $a_i \in \mathbb{Z}$ tals que $b - \sum_{i=1}^{\varphi(n)} a_i \zeta^i \in \ell A$. Com que $a_i \in \mathbb{Z}$, se satisfan les congruències $a_i^\ell \equiv a_i \pmod \ell$, de manera que $a_i^\ell - a_i \in \ell\mathbb{Z} \subseteq \ell A$; per tant, en elevar a ℓ i tenir en compte que els nombres combinatoris $\binom{\ell}{i}$ són múltiples de ℓ, per a $1 \leq i \leq \ell - 1$, obtenim que $b^\ell - \sum_{i=1}^{\varphi(n)} a_i \zeta^{i\ell} \in \ell A$. I, per inducció, $b^{\ell^f} - \sum_{i=1}^{\varphi(n)} a_i \zeta^{i\ell^f} \in \ell A$. Per hipòtesi, $\zeta^{\ell^f} = \zeta$, de manera que la darrera suma és b; per tant, $b^{\ell^f} - b \in \ell A$ com volíem provar. □

Proposició 3.9.7. *Siguin ℓ un nombre natural primer que no divideix n i f el nombre natural més petit tal que $\ell^f \equiv 1 \pmod{n}$. Aleshores,*

$$\ell A = \mathfrak{l}_1 \mathfrak{l}_2 \cdots \mathfrak{l}_g,$$

on $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_g$ són ideals primers diferents de A de grau residual $f(\mathfrak{l}_i|\ell\mathbb{Z}) = f$ i g és definit per la fórmula $fg = \varphi(n)$.

Demostració: Com que ℓ no divideix n, l'assignació $\zeta \mapsto \zeta^\ell$ defineix un automorfisme de $\mathbb{Q}(\zeta)$; posem F_ℓ. Aleshores, per a tot $b \in A$ és $F_\ell(b) - b^\ell \in \ell A$, ja que podem elegir $a_i \in \mathbb{Z}$ tals que $b - \sum_{i=1}^{\varphi(n)} a_i \zeta^i \in \ell A$ i, en conseqüència, $F_\ell(b) \equiv \sum_i a_i \zeta^{i\ell} \equiv \sum_i a_i^\ell \zeta^{i\ell} \equiv \left(\sum_i a_i \zeta^i\right)^\ell \equiv b^\ell \pmod{\ell A}$. Per inducció, $F_\ell^f(b) - b^{\ell^f} \in \ell A$, de manera que, en virtut del corol·lari anterior, $F_\ell^f(b) - b \in \ell A$, per a tot $b \in A$.

Per hipòtesi, l'ordre de l'automorfisme $F_\ell \in \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$ és exactament f. Siguin $\mathfrak{l}$ un ideal primer de A que divideix ℓA i f_1 el grau residual de $\mathfrak{l}$. Això ens diu que $A/\mathfrak{l}A$ és el cos finit de ℓ^{f_1} elements; per tant, f_1 és el nombre natural no nul més petit tal que per a tot element $b \in A$ se satisfà que $b^{\ell^{f_1}} - b \in \mathfrak{l}$. Com que per a f també se satisfà la propietat, ha de ser $f_1 \leq f$. Però, d'altra banda, com que $\zeta^{\ell^{f_1}} - \zeta \in \mathfrak{l}$ i les arrels de la unitat $1, \zeta, \ldots, \zeta^{n-1}$ són diferents en $A/\mathfrak{l}$, ha de ser $\ell^{f_1} \equiv 1 \pmod{n}$; això demostra l'altra desigualtat: $f \leq f_1$. Per tant, $f = f_1$, fet que acaba la demostració. □

Podem, per tant, donar les lleis de descomposició de tots els ideals primers de $\mathbb{Z}$ en els cossos ciclotòmics $\mathbb{Q}(\zeta)$, $\zeta = \zeta_n$ una arrel primitiva n-èsima de la unitat.

Teorema 3.9.8. *Siguin $n \not\equiv 2 \pmod 4$ un nombre natural, ζ una arrel primitiva n-èsima de la unitat, A l'anell dels enters del cos ciclotòmic $\mathbb{Q}(\zeta)$ i $p \in \mathbb{Z}$ un nombre natural primer. La descomposició de $p\mathbb{Z}$ en A és donada de la manera següent. Posem $n = p^r n'$ amb $r \geq 0$ i $\mathrm{mcd}(p, n') = 1$; aleshores*

$$pA = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_g)^e,$$

on $e = \varphi(p^r)$, $\mathfrak{p}_i$ són ideals primers diferents de A de grau residual el nombre enter més petit f tal que $p^f \equiv 1 \pmod{n'}$ i $fg = \varphi(n')$.

Demostració: Resta veure el cas $r \geq 1$. Ara podem considerar la cadena de cossos $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{n'}) \subseteq \mathbb{Q}(\zeta_n)$ i tenir en compte la multiplicativitat dels índexs de ramificació i la dels graus residuals. Sigui $\mathfrak{P} \subseteq A$ un ideal primer que divideix p i sigui $\mathfrak{p}$ la seva contracció a l'anell dels enters de $\mathbb{Q}(\zeta_{n'})$. Aleshores, $f(\mathfrak{P}|\mathfrak{p}) = g(\mathfrak{p}) = 1$, ja que $e(\mathfrak{P}|\mathfrak{p}) = \varphi(p^r)$ és el grau de l'extensió; per tant, $f(\mathfrak{P}|p) = f(\mathfrak{p}|p)$ i podem aplicar la proposició anterior. I com que $e(\mathfrak{p}|p) = 1$, és $e(\mathfrak{P}|p) = \varphi(p^r)$. □

Anem a fer, ara, l'estudi dels anells dels enters.

Teorema 3.9.9. *Siguin n un nombre enter, $\zeta := \zeta_n$ una arrel primitiva n-èsima de la unitat, i $K := \mathbb{Q}(\zeta)$ el n-èsim cos ciclotòmic. Aleshores, l'anell dels enters de K és l'anell $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

DEMOSTRACIÓ: Siguin $A := \mathcal{O}_K$ i $B := \mathbb{Z}[\zeta]$. Clarament, $\zeta \in A$, de manera que $B \subseteq A$ i cal provar la igualtat. Comencem pel cas $n = p^r$, on p és un nombre natural primer i $r \geq 1$. Reprenem la notació de la proposició **3.9.2**. Hem demostrat que $B + \alpha A = A$; com que $\alpha \in B$, després de multiplicar per α i substituir, obtenim la igualtat $B + \alpha^2 A = A$; i, per inducció, per a tot nombre enter $s \geq 1$ és $B + \alpha^s A = A$. Ara bé, també hem vist que $D(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})A \subseteq B$ i que $D(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})$ és una potència de p. Per tant, per a s prou gran se satisfà la inclusió $p^s A \subseteq B$; i com que pA és una potència de αA, també $\alpha^s A \subseteq B$ per a s prou gran. Això implica la igualtat $B = A$.

El cas general es pot provar per inducció sobre la quantitat de nombres primers diferents que divideixen n. Posem $n = p^r n'$ amb p primer, $\mathrm{mcd}(p, n') = 1$, i $r \geq 1$, $\zeta' := \zeta_{n'}$ una arrel primitiva n'-èsima de la unitat, $K' := \mathbb{Q}(\zeta')$ i $A' = B' = \mathbb{Z}[\zeta']$ l'anell dels enters de K' (hipòtesi d'inducció). És clar que $\zeta^{n'}$ és una arrel primitiva p^r-èsima de la unitat i que $A'[\zeta^{n'}] = \mathbb{Z}[\zeta] \subseteq A$; cal provar la igualtat. El discriminant $D(1, \zeta^{n'}, \zeta^{2n'}, \ldots, \zeta^{n'(\varphi(p^r)-1)})$ es pot calcular com el discriminant de l'extensió $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$, ja que les extensions $\mathbb{Q}(\zeta_{n'})|\mathbb{Q}$ i $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$ són linealment disjuntes; pel que hem vist en el cas que n és potència de p, el discriminant $D(1, \zeta^{n'}, \zeta^{2n'}, \ldots, \zeta^{n'(\varphi(p^r)-1)})$ és una potència de p en $\mathbb{Z}$ i, per tant, una potència p^k de p en A'. Igual que a la demostració del lema **3.6.3**, obtenim la inclusió $p^k A \subseteq A'[\zeta^{n'}]$ tenint en compte la regla de Cramer. D'altra banda, com que l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}(\zeta')$ és totalment ramificada en tots els ideals primers $\mathfrak{P}$ de A que divideixen $p\mathbb{Z}$ (és a dir, el seus índexs de ramificació coincideixen amb el grau), els cossos residuals de A en $\mathfrak{P}$ i de A' en $\mathfrak{P} \cap A'$ coincideixen per a tot ideal primer $\mathfrak{P}$ de A que divideix p. Siguin $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ tots els ideals primers de A que divideixen p i siguin $\mathfrak{P}'_i := \mathfrak{P}_i \cap A'$ les seves contraccions a A'. Es tenen igualtats $pA' = \mathfrak{P}'_1 \mathfrak{P}'_2 \cdots \mathfrak{P}'_g$ en A', ja que el nombre d'ideals primers de A i de A' que divideixen p és el mateix i $A'|\mathbb{Z}$ és no ramificada en p, i $(1 - \zeta^{n'})A = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_g$, ja que la potència $\varphi(p^r)$-èsima dels dos ideals és l'ideal pA. Aquesta darrera igualtat ens permet assegurar que $A/(1 - \zeta^{n'})A \cong A'/\mathfrak{P}'_1 \mathfrak{P}'_2 \cdots \mathfrak{P}'_g$, en virtut del teorema xinès del residu, de manera que $A = A' + (1 - \zeta^{n'})A = A'[\zeta^{n'}] + (1 - \zeta^{n'})A$. De nou per inducció tenint en compte que $1 - \zeta^{n'} \in A'[\zeta^{n'}]$, s'obté que per a tot nombre enter s suficientment gran és $A = A'[\zeta^{n'}] + (1 - \zeta^{n'})^s A$. Com que una potència de l'ideal $(1 - \zeta^{n'})A$ és l'ideal pA, si prenem s prou gran, obtenim la igualtat $A = A'[\zeta^{n'}]$, com volíem demostrar. □

Com a conseqüència d'aquest resultat, el discriminant $\Delta(\mathbb{Z}[\zeta]|\mathbb{Z})$ és el determinant $D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$ que hem calculat en la proposició **3.9.7**. Obtenim, per tant, el resultat següent.

Corol·lari 3.9.10. *El discriminant de l'extensió ciclotòmica $\mathbb{Z}[\zeta]|\mathbb{Z}$, on $\zeta = \zeta_n$ és una arrel primitiva n-èsima de la unitat, és donat per la fórmula*

$$\Delta(\mathbb{Z}[\zeta]|\mathbb{Z}) = (-1)^{\varphi(n)(\varphi(n)-1)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}. \square$$

Observació 3.9.11. Aquesta fórmula es pot provar d'una altra manera si fem servir les fórmules de transitivitat del discriminant que encara no hem provat. Això ho podrem fer així més endavant.

Una aplicació interessant de les lleis de descomposició dels nombres primers en els cossos ciclotòmics $\mathbb{Q}(\zeta_p)$, p un nombre primer, és una nova demostració de la llei de reciprocitat quadràtica. Recordem que si ζ és una arrel primitiva p-èsima de la unitat, p

un natural primer senar, aleshores l'únic subcòs quadràtic de $\mathbb{Q}(\zeta)$ és el cos $\mathbb{Q}(\sqrt{p^*})$, on $p^* = (-1)^{\varepsilon(p)}p$. La part principal de la demostració és el resultat següent.

Lema 3.9.12. *Siguin p, ℓ, naturals primers senars diferents. Condició necessària i suficient perquè ℓ descompongui com a producte de dos ideals primers diferents en $\mathbb{Q}(\sqrt{p^*})$ és que descompongui com a producte d'un nombre parell d'ideals primers diferents en $\mathbb{Q}(\zeta)$.*

Demostració: Siguin $K := \mathbb{Q}(\zeta)$, A el seu anell d'enters, $K' := \mathbb{Q}(\sqrt{p^*})$, A' el seu anell d'enters, $\mathfrak{L} \subseteq A$ un ideal primer que divideix ℓ i $\mathfrak{l} := \mathfrak{L} \cap A'$ la seva contracció. La successió exacta de grups de Galois

$$1 \longrightarrow \mathrm{Gal}\,(K|K') \longrightarrow \mathrm{Gal}\,(K|\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(K'|\mathbb{Q}) \longrightarrow 1$$

dóna lloc, per restricció, a la successió de grups de descomposició

$$1 \longrightarrow D(\mathfrak{L}|\mathfrak{l}) \longrightarrow D(\mathfrak{L}|\ell) \longrightarrow D(\mathfrak{l}|\ell) \longrightarrow 1.$$

Aquesta successió també és exacta. L'única part que mereix una mica de comentari és l'exhaustivitat del morfisme $D(\mathfrak{L}|\ell) \longrightarrow D(\mathfrak{l}|\ell)$. Si $\sigma' \in D(\mathfrak{l}|\ell)$, aleshores, existeix $\sigma \in \mathrm{Gal}\,(K|\mathbb{Q})$ tal que la restricció de σ a K' és σ'; els ideals $\mathfrak{L}$ i $\sigma(\mathfrak{L})$ contrauen tots dos a $\mathfrak{l}$ en A', de manera que existeix $\tau \in \mathrm{Gal}\,(K|K')$ tal que $\tau\sigma\mathfrak{L} = \mathfrak{L}$; per tant, l'automorfisme $\tau\sigma$ pertany al grup de descomposició $D(\mathfrak{L}|\mathfrak{l})$; finalment, la imatge de $\tau\sigma$ en $D(\mathfrak{L}|\ell)$ s'aplica sobre σ', ja que τ és la identitat en K'.

Siguin g, g', g'' els índexs dels grups de descomposició $D(\mathfrak{L}|\ell)$, $D(\mathfrak{l}|\ell)$, $D(\mathfrak{L}|\mathfrak{l})$, respectivament; és a dir, els nombres de primers que divideixen ℓ, ℓ, $\mathfrak{l}$, en les extensions $K|\mathbb{Q}$, $K'|\mathbb{Q}$, i $K|K'$. L'exactitud de les dues successions anteriors demostra que $g = g'g''$, de manera que si g' és parell, també ho és g. Recíprocament, suposem que g és parell. Tenint en compte que els grups de Galois i, per tant, els grups de descomposició, són grups cíclics, es dedueix immediatament que $D(\mathfrak{L}|\ell)$ està inclòs en l'únic subgrup de $\mathrm{Gal}\,(K|\mathbb{Q})$ d'índex 2, que és $\mathrm{Gal}\,(K|K')$, de manera que $D(\mathfrak{L}|\ell) = D(\mathfrak{L}|\mathfrak{l})$ i $D(\mathfrak{l}|\ell)$ és el grup trivial; això diu que $g' = 2$, com volíem veure. □

Ara podem acabar fàcilment una demostració de la llei de reciprocitat quadràtica. La descripció de les lleis de descomposició dels ideals primers en els cossos quadràtics ens permet assegurar que una condició necessària i suficient perquè ℓ descompongui en producte de dos ideals primers diferents de A' és que $\left(\dfrac{p^*}{\ell}\right) = 1$; i el resultat que acabem de provar admet la conseqüència següent.

Corol·lari 3.9.13. *Condició necessària i suficient perquè ℓ descompongui completament en A' és que $\left(\dfrac{\ell}{p}\right) = 1$.*

Demostració: Amb les mateixes notacions que a la demostració del lema anterior podem escriure que g és parell si, i només si, el grau residual f de $\mathfrak{L}|\ell$ divideix $(p-1)/2$; i això darrer equival a dir que $\ell^{(p-1)/2} \equiv 1 \pmod{p}$, via la caracterització del grau residual dels ideals primers en les extensions ciclotòmiques de $\mathbb{Q}$ que hem donat més amunt. Però en ${\mathbb{F}_p}^*$ els elements ℓ per als quals se satisfà la congruència anterior són exactament els quadrats, ja que ${\mathbb{F}_p}^*$ és un grup cíclic. Per tant, ℓ descompon completament en A' si, i només si, $\left(\dfrac{\ell}{p}\right) = 1$, per definició del símbol de Legendre. □

Per tant, obtenim l'equivalència entre les propietats $\left(\frac{p^*}{\ell}\right) = 1$ i $\left(\frac{\ell}{p}\right) = 1$; només cal tenir en compte el valor del símbol $\left(\frac{-1}{\ell}\right)$. $\square$

Capítol 4

Geometria dels nombres

Aquest capítol es destina a fer l'estudi dels grups de les unitats i dels grups de classes d'ideals dels anells dels enters dels cossos de nombres. Abans d'estudiar el concepte i algunes propietats de les xarxes de $\mathbb{R}^n$ introduirem el concepte de domini fonamental per a una acció d'un grup en un conjunt; especialment en el cas d'accions contínues en espais topològics, que tenen aplicacions importants en altres temes d'estudi de la teoria algebraica de nombres; per exemple, en l'estudi de les corbes el·líptiques i les formes modulars.

4.1 Dominis fonamentals

Siguin X un espai topològic, G un grup topològic i $G \times X \xrightarrow{h} X$ una acció contínua de G en X; això vol dir que per a tot element $\sigma \in G$ disposem d'una aplicació contínua $h_\sigma : X \longrightarrow X$ de manera que $h_{\sigma\sigma'} = h_\sigma \circ h_{\sigma'}$ i que $h_1 = \mathrm{id}_X$, on 1 denota l'element neutre de G. En particular, l'aplicació h_σ és un homeomorfisme amb invers $h_{\sigma^{-1}}$.

Definició 4.1.1. S'anomena domini fonamental de X per a l'acció h tot subespai topològic $D \subseteq X$ per al qual se satisfan les condicions següents:

(a) D conté un representant de cada una de les òrbites Gx, $x \in X$; i

(b) si dos elements diferents de D són de la mateixa òrbita, aleshores estan a la frontera de D.

Exemple 4.1.2. Considerem l'espai topològic $X := \mathbb{C}$, el grup topològic discret $G := \mathbb{Z}[i]$, i l'acció donada per translació: $(a + bi, z) \mapsto a + bi + z$. Un domini fonamental per a aquesta acció és el paral·lelogram

$$\{z \in \mathbb{C} : \ 0 \leq \Re(z) \leq 1,\ 0 \leq \Im(z) \leq 1\}.$$

També ho és el paral·lelogram no compacte

$$\{z \in \mathbb{C} : \ 0 \leq \Re(z) < 1,\ 0 \leq \Im(z) < 1\}.$$

Exemple 4.1.3. De manera més general, siguin $X = \mathbb{C}$, $G = \mathbb{Z} \times \mathbb{Z}$ considerat com a grup (topològic) discret i fixem una $\mathbb{R}$-base $\{\omega_1, \omega_2\}$ de $\mathbb{C}$. Definim l'acció per la fórmula $((a, b), z) \mapsto a\omega_1 + b\omega_2 + z$. Un domini fonamental per a aquesta acció és el paral·lelogram

$$D := \{z = a\omega_1 + b\omega_2 \in \mathbb{C} : \ a, b \in \mathbb{R},\ 0 \leq a \leq 1,\ 0 \leq b \leq 1\}.$$

Observació 4.1.4. El quocient $\mathbb{C}/\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \cong D/(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) \cap D$ és una superfície de Riemann compacta de gènere 1 (un tor); en el context de les corbes algebraiques, defineix una corba, a la qual s'anomena la corba el·líptica definida per la parella ω_1, ω_2.

Exemple 4.1.5. De manera encara més general, siguin $X := \mathbb{R}^n$, $G := \mathbb{Z}^n$ i considerem l'acció donada a partir d'una $\mathbb{R}$-base $\{e_1, \ldots, e_n\}$ de $\mathbb{R}^n$ per la fórmula de translació $((a_1, \ldots, a_n), x) \mapsto x + \sum_{i=1}^{n} a_i e_i$. Un domini fonamental d'aquesta acció és el paral·lelepípede fonamental

$$D = \{\sum_{i=1}^{n} a_i e_i : \ a_i \in \mathbb{R},\ 0 \leq a_i \leq 1\}.$$

També ho és el paral·lelepípede no compacte

$$D = \{\sum_{i=1}^{n} a_i e_i : \ a_i \in \mathbb{R},\ 0 \leq a_i < 1\}.$$

Exemple 4.1.6. Sigui $X = \mathbb{H} := \{z \in \mathbb{C} : \ \Re(z) > 0\}$ el semiplà superior de Poincaré, i sigui $G := \mathbf{GL}(2, \mathbb{R})^+$, el grup de les matrius quadrades 2×2 de coeficients reals i de determinant positiu. Podem definir una acció en $\mathbb{H}$ per la fórmula següent:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az + b}{cz + d}.$$

Un domini fonamental per a aquesta acció és qualsevol conjunt D format per un sol element; en efecte, l'acció és transitiva.

Exercici 4.1.7. El conjunt $D := \{z \in \mathbb{H} : \ -1/2 \leq \Re(z) \leq 1/2,\ |z| \geq 1\}$ és un domini fonamental per a la restricció de l'acció anterior al subgrup discret $\mathbf{SL}(2, \mathbb{Z})$ de les matrius de coeficients enters i determinant 1.

4.2 Xarxes de $\mathbb{R}^n$

Ens interessarà parlar de subgrups discrets de $\mathbb{R}^n$, i convé disposar del resultat següent.

Proposició 4.2.1. *Sigui G un subgrup discret de $\mathbb{R}^n$. Aleshores, G és un grup abelià lliure de rang $r \leq n$.*

Demostració: Podem elegir en G un conjunt d'elements $\{e_1, e_2, \ldots, e_r\}$ que siguin $\mathbb{R}$-linealment independents de manera que r sigui màxim; en particular, $r \leq n$. Considerem el subconjunt $S := \{\sum_{i=1}^{r} a_i e_i \ : \ a_i \in \mathbb{R},\ 0 \leq a_i \leq 1\}$. Com que S és un subconjunt compacte de $\mathbb{R}^n$ i G és discret, el conjunt $S \cap G$ és finit. Es tracta de demostrar que $S \cap G$ és un conjunt de generadors de G; d'aquesta manera obtindrem que G és un grup abelià lliure, ja que no té torsió per ser un subgrup de $\mathbb{R}^n$ i tot grup abelià finitament generat i sense torsió és lliure.

Sigui, doncs, $x \in G$; podem escriure x en la forma $x = \sum_{i=1}^{r} \alpha_i e_i$ amb $\alpha_i \in \mathbb{R}$, ja que en cas contrari el conjunt $\{e_1, e_2, \ldots, e_r, x\}$ estaria format per més de r elements $\mathbb{R}$-linealment independents de G i r no seria maximal. Posem $y := x - \sum_{i=1}^{r} [\alpha_i] e_i = \sum_{i=1}^{r} (\alpha_i - [\alpha_i]) e_i$; com que $y, e_1, \ldots, e_r \in S \cap G$ i $x = y + \sum_{i=1}^{r} [\alpha_i] e_i$, resulta que $S \cap G$ genera G com a grup abelià i, per tant, G és finitament generat.

Resta veure que el rang de G és menor o igual que n. Per a tot nombre enter k i tot $x \in G$ posem $x_k := kx - \sum_{i=1}^{r} [k\alpha_i] e_i = \sum_{i=1}^{r} (k\alpha_i - [k\alpha_i]) e_i$; com abans, $x_k \in S \cap G$ i, com que $S \cap G$ és finit, existeixen nombres enters diferents k, j tals que $x_k = x_j \in S \cap G$. La $\mathbb{R}$-independència lineal dels elements e_i i la darrera igualtat ens permeten assegurar que per a tot índex i els coeficients α_i són racionals, ja que $\alpha_i = (k-j)^{-1}([k\alpha_i] - [j\alpha_i])$. Això implica que x pertany al $\mathbb{Q}$-espai vectorial generat pels elements e_i. En particular, els elements (en nombre finit) de $S \cap G$ són combinacions lineals de coeficients racionals dels elements e_i i podem considerar un denominador comú $d \in \mathbb{Z}$, $d \neq 0$, de tots aquests coeficients; aleshores, el grup abelià lliure G és un subgrup del grup abelià lliure $\bigoplus_{i=1}^{r} d^{-1}\mathbb{Z} e_i$ de rang r; per tant, el rang de G és menor o igual que r i, com que G conté r elements que són $\mathbb{R}$-linealment independents, els e_i, el grup G és de rang r. □

Definició 4.2.2. Un subgrup $G \subseteq \mathbb{R}^n$ s'anomena xarxa de $\mathbb{R}^n$ si és un subgrup discret de rang n.

Sigui G una xarxa de $\mathbb{R}^n$; aleshores G és un grup (topològic) que actua en $\mathbb{R}^n$ per translació: $(\sigma, x) \mapsto x + \sigma$ (cf. l'exemple **4.1.5** més amunt). A més a més, el conjunt $D := \{\sum_{i=1}^{n} a_i e_i : 0 \leq a_i < 1\}$, on $e_1, \ldots, e_n$ és una $\mathbb{Z}$-base de G, és un domini fonamental per a l'acció de G en $\mathbb{R}^n$; s'anomena el paral·lelepípede fonamental relatiu a la base $\{e_1, \ldots, e_n\}$. Observem que D és un subconjunt mesurable Lebesgue de $\mathbb{R}^n$; la seva mesura $\mu(D)$ s'anomena la malla de la xarxa G i es representa usualment per $\mu(G)$. D'altra banda, no hi ha cap parella d'elements de D que estiguin en la mateixa òrbita per l'acció de G; aquesta propietat serà útil de seguida.

Lema 4.2.3. *La malla d'una xarxa G de $\mathbb{R}^n$ no depèn de la $\mathbb{Z}$-base elegida en G.*

Demostració: En efecte, un canvi de base en G és donat per una matriu $M \in \mathbf{GL}(n, \mathbb{Z})$; i la mesura del nou paral·lelepípede fonamental s'obté a partir de l'anterior multiplicant pel valor absolut del determinant de M. Però les matrius de $\mathbf{GL}(n, \mathbb{Z})$ són de determinant ± 1. □

Teorema 4.2.4 (Minkowski)**.** *Siguin G una xarxa de $\mathbb{R}^n$ i X un subconjunt mesurable Lebesgue de $\mathbb{R}^n$ tal que $\mu(X) > \mu(G)$. Aleshores, X conté dos elements diferents x, y tals que $x \equiv y \pmod{G}$.*

Demostració: Siguin $\{e_1, \ldots, e_n\}$ una $\mathbb{Z}$-base de G i D el paral·lelepípede fonamental per a $\mathbb{R}^n$ relatiu a aquesta base. Per definició de domini fonamental, els conjunts $g + D$,

$g \in G$, formen un recobriment de $\mathbb{R}^n$; aquest recobriment és disjunt en virtut de l'elecció de D. En conseqüència, els conjunts $X \cap (g+D)$, $g \in G$, formen un recobriment disjunt de X. D'altra banda, com que la mesura de Lebesgue és invariant per translació (és la mesura de Haar del grup topològic localment compacte $\mathbb{R}^n$), els conjunts $g+D$ són mesurables; per tant, les interseccions $X \cap (g+D)$ també són mesurables i la seva mesura coincideix amb la mesura dels seus traslladats $(-g+X) \cap D$. De la igualtat $\mu(X) = \sum_{g \in G} \mu(X \cap (g+D))$, que es dedueix del fet que X és recobert de manera disjunta pels conjunts $X \cap (g+D)$, obtenim que $\mu(X) = \sum_{g \in G} \mu((-g+X) \cap D)$, de manera que els conjunts $(-g+X) \cap D$ no poden ser disjunts dos a dos, ja que la seva reunió és un subconjunt de D i estem suposant que $\mu(G) = \mu(D) < \mu(X)$.

Per tant, existeixen elements diferents $g, g' \in G$ tals que $(-g+X) \cap (-g'+X) \cap D$ és no buit; per tant, existeixen elements $x, y \in X$ tals que $x - g = y - g'$ i, aleshores, $x - y = g - g' \in G$ i $x \neq y$ ja que $g \neq g'$. □

Corol·lari 4.2.5. *Siguin G una xarxa de $\mathbb{R}^n$ i $X \subseteq \mathbb{R}^n$ un subconjunt convex, simètric respecte de l'origen i mesurable Lebesgue. Suposem que $\mu(X) > 2^n \mu(G)$ o bé que X és compacte i $\mu(X) \geq 2^n \mu(G)$. Aleshores, existeix $x \in G \cap X$ tal que $x \neq 0$.*

Demostració: Suposem que $\mu(X) > 2^n \mu(G)$; aleshores, el conjunt $Y := \{x/2 : x \in X\}$ també és mesurable Lebesgue i $\mu(Y) = 2^{-n}\mu(X) > \mu(G)$, per hipòtesi. En virtut del teorema de Minkowski existeixen dos punts diferents $y_1, y_2 \in Y$ tals que $y_2 - y_1 \in G$; el punt $x := y_2 - y_1$ és un punt no nul de $X \cap G$, ja que X és convex i simètric respecte de l'origen, $2y_1, 2y_2 \in X$ i x és el punt mitjà de $2y_2$ i $-2y_1$.

En el cas que suposem que X és compacte i que $\mu(X) \geq 2^n \mu(G)$, per a tot $\varepsilon > 0$ podem posar $X_\varepsilon := (1+\varepsilon)X$, de manera que se satisfan les mateixes hipòtesis amb la millora $\mu(X_\varepsilon) > \mu(G)$, i podem aplicar a X_ε el que acabem de demostrar: per a cada $\varepsilon > 0$ existeix un punt no nul $x_\varepsilon \in G \cap X_\varepsilon$. Els conjunts $X'_\varepsilon := X_\varepsilon \cap G - \{0\}$ són no buits, compactes i discrets, de manera que són finits i no buits; i la finitud de tots ells implica que la intersecció $\bigcap_{\varepsilon > 0} X'_\varepsilon$ és no buida. Finalment, de la compacitat de X es dedueix que la intersecció és $X \cap G \neq \{0\}$, ja que $\bigcap_{\varepsilon > 0} (1+\varepsilon)X = X$. Això acaba la demostració. □

4.3 La immersió canònica d'un cos de nombres

Siguin K un cos de nombres i $n := [K : \mathbb{Q}]$ el seu grau. Si considerem una clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, aleshores existeixen exactament n maneres diferents de pensar K com a subcòs de $\overline{\mathbb{Q}}$; en efecte, com que $\mathbb{Q}$ és de característica zero, tota extensió de $\mathbb{Q}$ és separable, de manera que el grau de separabilitat de qualsevol extensió finita $K|\mathbb{Q}$ (és a dir, el nombre de maneres d'incloure K en $\overline{\mathbb{Q}}$) coincideix amb el grau.

D'altra banda, podem canviar $\overline{\mathbb{Q}}$ per qualsevol cos que el contingui i la propietat no varia, ja que una $\mathbb{Q}$-immersió de K ha d'estar inclosa en $\overline{K} = \overline{\mathbb{Q}}$; en particular, el nombre total de $\mathbb{Q}$-immersions de K en $\mathbb{C}$ és exactament n.

Podem pensar, encara, en les $\mathbb{Q}$-immersions de K en $\mathbb{R}$; com que $\mathbb{R} \subseteq \mathbb{C}$, és clar que el nombre de $\mathbb{Q}$-immersions de K en $\mathbb{R}$ és $r_1 \leq n$. Sigui σ una immersió de K en $\mathbb{C}$; si

componem amb la conjugació complexa, $c : \mathbb{C} \longrightarrow \mathbb{C}$, donada per $c(a + bi) := a - bi$, per a $a, b \in \mathbb{R}$, obtindrem una altra $\mathbb{Q}$-immersió $c\sigma$ de K en $\mathbb{C}$. És clar que una condició necessària i suficient perquè $\sigma = c\sigma$ és que $\sigma(K) \subseteq \mathbb{R}$. Això ens permet assegurar que el nombre n de $\mathbb{Q}$-immersions diferents de K en $\mathbb{C}$ es pot expressar en la forma $n = r_1 + 2r_2$, on r_2 és el nombre de conjunts $\{\sigma, c\sigma\}$ tals que $\sigma \neq c\sigma$.

En vista d'aquest fet, i per comoditat, numerarem les $\mathbb{Q}$-immersions de K en la forma següent: $\sigma_1, \ldots, \sigma_{r_1}$ seran les *immersions reals*; i les parelles σ_{r_1+j}, $\sigma_{r_1+r_2+j} = c\sigma_{r_1+j}$, amb $1 \leq j \leq r_2$, les parelles de $\mathbb{Q}$-immersions *complexes conjugades no reals* de K. Observem que, d'aquesta manera, el coneixement de les immersions σ_i per a $1 \leq i \leq r_1 + r_2$ ja determina unívocament les altres.

Definició 4.3.1. El morfisme d'anells $K \xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definit per l'assignació

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x))$$

s'anomena la immersió canònica de K. Sovint s'acostuma a identificar $\mathbb{C}$ amb $\mathbb{R}^2$ (com a $\mathbb{R}$-espai vectorial); en aquest cas, la immersió canònica es pensa en la forma $K \xrightarrow{\sigma} \mathbb{R}^n$.

La importància i la utilitat de la immersió canònica de K es veuen bé en el resultat següent.

Proposició 4.3.2. *Sigui G un subgrup abelià lliure de rang n de K. Aleshores, la imatge de G per la immersió canònica és una xarxa de $\mathbb{R}^n$. Si $\{e_1, \ldots, e_n\}$ és una $\mathbb{Z}$-base de G, la malla de la xarxa $\sigma(G)$ és donada per la fórmula*

$$\mu(\sigma(G)) = 2^{-r_2} \left|\det(\sigma_i(e_j))\right|.$$

Demostració: Els vectors $\sigma(e_1), \ldots, \sigma(e_n)$ generen la imatge $\sigma(G)$; si demostrem que són linealment independents, aleshores sabrem que formen una $\mathbb{Z}$-base de $\sigma(G)$, de manera que $\sigma(G)$ és una xarxa de $\mathbb{R}^n$ i $\sigma(e_1), \ldots, \sigma(e_n)$ són els vèrtexs d'un paral·lelepípede fonamental; per tant, podrem calcular la malla d'aquesta xarxa com el valor absolut del determinant dels vectors $\sigma(e_j)$ expressats en la base "canònica" de $\mathbb{R}^n$. Ara bé, els components del vector $\sigma(e_j)$ en la base canònica de $\mathbb{R}^n$ són exactament els nombres $\sigma_i(e_j)$ per als r_1 components reals, i les parelles $\Re(\sigma_i(e_j)), \Im(\sigma_i(e_j))$, per als components $\sigma_i(e_j)$ amb $r_1 < i \leq r_1 + r_2$. Tenint en compte que $\Re(\sigma_i(e_j)) = (\sigma_i(e_j) + \sigma_{i+r_2}(e_j))/2$, $\Im(\sigma_i(e_j)) = (\sigma_i(e_j) - \sigma_{i+r_2}(e_j))/2i$, i la linealitat del determinant respecte de les files, el determinant a calcular és el producte del factor $(2i)^{-r_2}$ pel determinant $\det(\sigma_i(e_j))$; en efecte, per a cada índex i, $1 \leq i \leq r_2$, podem canviar la fila formada pels components $\Re(\sigma_{r_1+i}(e_j))$ per la formada pels $\sigma_{r_1+i}(e_j)$, després la formada pels components $\Im(\sigma_{r_1+i}(e_j))$ per la que consta dels $\sigma_{r_1+r_2+i}(e_j)/(-2i)$ i, finalment, treure factor comú els r_2 factors $-1/2i = i/2$. Però el determinant $\det(\sigma_i(e_j))$ és no nul, ja que els elements e_j són una $\mathbb{Q}$-base de K i l'extensió $K|\mathbb{Q}$ és separable. Aquest càlcul demostra, per tant, que els vectors $\sigma(e_j)$ són $\mathbb{R}$-linealment independents i que la malla de la xarxa és donada per la fórmula enunciada. □

Corol·lari 4.3.3. *Sigui $\{e_1, \ldots, e_n\}$ una $\mathbb{Z}$-base de l'anell del enters del cos de nombres K. Condició necessària i suficient perquè el discriminant absolut de K, $D(e_1, \ldots, e_n)$, sigui positiu és que el nombre r_2 de parelles d'immersions complexes conjugades no reals de K sigui parell.*

DEMOSTRACIÓ: En efecte, el discriminant que cal calcular és el quadrat del determinant $\det(\sigma_i(e_j))$, on $\sigma_i(e_j)$ són els diferents conjugats de e_j; i a la demostració de la proposició anterior hem vist que aquest determinant és el producte d'un determinant d'entrades reals pel producte dels factors $(-2i)^{r_2}$. Per tant, el discriminant dels vectors e_j és un nombre real positiu multiplicat per $(-2i)^{2r_2}$; i aquest nombre és positiu si, i només si, r_2 és parell. □

Observació 4.3.4. En particular, aquest resultat proporciona una manera senzilla de comprovar el signe del discriminant dels cossos ciclotòmics.

El corol·lari següent dóna compte de les xarxes més útils; concretament, ja hem vist que l'anell $\mathcal{O}_K$ dels enters de K és un $\mathbb{Z}$-submòdul lliure de rang n de K. El mateix succeeix a tot ideal $\mathfrak{a} \subseteq \mathcal{O}_K$; és clar que és un $\mathbb{Z}$-submòdul sense torsió de $\mathcal{O}_K$ i que és finitament generat, ja que $\mathbb{Z}$ és noetherià i $\mathcal{O}_K$ és finitament generat; per tant, és un grup abelià lliure de rang $\leq n$; com que per a tot $a \in \mathfrak{a}$ no nul se satisfà la inclusió $a\mathcal{O}_K \subseteq \mathfrak{a}$ i $a\mathcal{O}_K \cong \mathcal{O}_K$ com a grups abelians, $\mathfrak{a}$ conté un grup abelià lliure de rang n i, en conseqüència, $\mathfrak{a}$ és un grup abelià lliure de rang n.

Corol·lari 4.3.5. *Siguin $\mathcal{O}_K$ l'anell dels enters d'un cos de nombres K, $n := [K : \mathbb{Q}]$, el grau, $\mathfrak{a} \subseteq \mathcal{O}_K$ un ideal no nul de $\mathcal{O}_K$ i Δ el discriminant d'una $\mathbb{Z}$-base de $\mathcal{O}_K$. Aleshores, $\sigma(\mathcal{O}_K)$ i $\sigma(\mathfrak{a})$ són xarxes de $\mathbb{R}^n$ i les seves malles són donades per les fórmules:*

$$\mu(\sigma(\mathcal{O}_K)) = 2^{-r_2}|\Delta|^{1/2}, \ i$$
$$\mu(\sigma(\mathfrak{a})) = 2^{-r_2}|\Delta|^{1/2}\mathcal{N}(\mathfrak{a}),$$

on $\mathcal{N}(\mathfrak{a})$, la norma absoluta de $\mathfrak{a}$, és el cardinal de l'anell finit $\mathcal{O}_K/\mathfrak{a}$.

DEMOSTRACIÓ: La qüestió relativa a l'anell $\mathcal{O}_K$ és immediata a partir de la proposició anterior. En efecte, si $\{e_1, \ldots, e_n\}$ és una $\mathbb{Z}$-base de $\mathcal{O}_K$, el discriminant $\Delta(\mathcal{O}_K|\mathbb{Z})$ és l'ideal generat pel quadrat del determinant de la matriu $(\sigma_i(e_j))$, de manera que la malla de la xarxa només té en compte el valor absolut de l'arrel quadrada del discriminant.

D'altra banda, la diferència en considerar un ideal no nul $\mathfrak{a}$ de $\mathcal{O}_K$ està en el fet que $\mathfrak{a}$ és un subgrup abelià de $\mathcal{O}_K$ d'índex $\mathcal{N}(\mathfrak{a})$. Com que la immersió canònica és un morfisme injectiu d'anells, això implica que $\sigma(\mathfrak{a})$ és un subgrup d'índex $\mathcal{N}(\mathfrak{a})$ de $\sigma(\mathcal{O}_K)$; en conseqüència, podem obtenir un domini fonamental per a $\sigma(\mathfrak{a})$ fent la reunió disjunta de $\mathcal{N}(\mathfrak{a})$ traslladats d'un domini fonamental per a $\sigma(\mathcal{O}_K)$. Això fa que la malla de $\sigma(\mathfrak{a})$ sigui $\mathcal{N}(\mathfrak{a})$ vegades la malla de $\sigma(\mathcal{O}_K)$; això acaba la demostració. □

4.4 Finitud del grup de classes d'ideals

El grup de classes d'ideals d'un anell de Dedekind no és, en general, un grup finit. Un dels teoremes més importants en l'estudi de la teoria algebraica de nombres algebraics és el que assegura aquesta finitud en el cas dels anells dels enters dels cossos de nombres. L'objectiu d'aquesta secció és establir aquest teorema. Convé començar per la demostració del resultat següent.

Proposició 4.4.1 (La fita de Minkowski)**.** *Siguin K un cos de nombres, $A := \mathcal{O}_K$ el seu anell d'enters, $n := [K : \mathbb{Q}]$ el grau, r_1 el nombre d'immersions reals de K, r_2 el nombre*

de parelles d'immersions complexes conjugades no reals de K, Δ el discriminant absolut de l'extensió $A|\mathbb{Z}$; és a dir, el generador positiu de l'ideal discriminant $\Delta(A|\mathbb{Z})$, i $\mathfrak{a} \subseteq A$ un ideal no nul. Aleshores, existeix un element $a \in \mathfrak{a}$, $a \neq 0$, tal que per a la seva norma se satisfà la desigualtat

$$|\mathrm{N}_{K|\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\Delta|^{1/2} \mathcal{N}(\mathfrak{a}).$$

Demostració: Considerem la immersió canònica σ de K en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Per a tot nombre real positiu ε, el conjunt $X_\varepsilon \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ format pels elements $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$ tals que $\sum_{i=1}^{r_1} |x_i| + 2\sum_{j=1}^{r_2} |z_j| \leq \varepsilon$ és compacte, convex i simètric respecte de l'origen; per tant, és mesurable Lebesgue. El càlcul de la seva mesura dóna

Lema 4.4.2. $\mu(X_\varepsilon) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{\varepsilon^n}{n!}$.

Demostració: El conjunt X_ε no només depèn de ε, sinó que també depèn de les constants r_1 i r_2 tals que $r_1 + 2r_2 = n$. Posem $m(r_1, r_2, \varepsilon) := \mu(X_\varepsilon)$. Calcularem aquesta mesura per inducció sobre les constants r_1 i r_2. Clarament, $m(1, 0, \varepsilon) = 2\varepsilon$ i $m(0, 1, \varepsilon) = \frac{\pi\varepsilon^2}{4}$ ja que, en el primer cas, el conjunt és un segment i, en el segon, el conjunt és un cercle. El pas de r_1 a $r_1 + 1$ es pot fer de la manera següent: X_ε és ara un subconjunt de $\mathbb{R}^{r_1+1} \times \mathbb{C}^{r_2}$ i ens podem fixar en el component real de subíndex $r_1 + 1$; la mesura $m(r_1 + 1, r_2, \varepsilon)$ es pot calcular, integrant "per llesques", com la integral

$$\int_{-\varepsilon}^{\varepsilon} m(r_1, r_2, \varepsilon - |x|)dx.$$

Per hipòtesi d'inducció, $m(r_1, r_2, \varepsilon - |x|) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(\varepsilon - |x|)^{r_1+2r_2}}{(r_1 + 2r_2)!}$ que, dut a la integral, dóna el valor $m(r_1 + 1, r_2, \varepsilon) = 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \frac{\varepsilon^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!}$, com calia veure. El pas de r_2 a $r_2 + 1$ es fa de manera semblant integrant sobre el disc $|z| \leq \varepsilon/2$; concretament, cal calcular la integral

$$\int_{|z| \leq \varepsilon/2} m(r_1, r_2, \varepsilon - 2|z|)d\mu(z),$$

on $d\mu(z)$ denota la mesura de Lebesgue de $\mathbb{C}$. Si fem el canvi de variables habitual a coordenades polars, $z = \rho e^{i\theta}$, resulta que $d\mu(z) = \rho d\rho d\theta$ i cal calcular la integral doble

$$\begin{aligned} m(r_1, r_2 + 1, \varepsilon) &= \int_0^{\varepsilon/2} \int_0^{2\pi} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(\varepsilon - 2\rho)^{r_1+2r_2}}{(r_1 + 2r_2)!} \rho d\rho d\theta \\ &= 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{2\pi}{(r_1 + 2r_2)!} \int_0^{\varepsilon/2} (\varepsilon - 2\rho)^{r_1+2r_2} \rho d\rho \\ &= 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2+1} \frac{\varepsilon^{r_1+2r_2+2}}{(r_1 + 2r_2 + 2)!}, \end{aligned}$$

després de calcular la darrera integral per parts. Això acaba el càlcul de la mesura del conjunt X_ε. □

A continuació, donat l'ideal $\mathfrak{a}$, podem elegir $\varepsilon > 0$ de manera que

$$\varepsilon^n = \left(\frac{4}{\pi}\right)^{r_2} n!|\Delta|^{1/2}\mathcal{N}(\mathfrak{a}),$$

on Δ és el discriminant absolut de l'extensió $A|\mathbb{Z}$. Això ens permet assegurar que la mesura de X_ε és exactament $\mu(X_\varepsilon) = 2^n\mu(\sigma(\mathfrak{a}))$. En virtut del teorema de Minkowski, existeix un element no nul $a \in \mathfrak{a}$ tal que $\sigma(a) \in X_\varepsilon$; el càlcul de la norma de a dóna $|\mathrm{N}_{K|\mathbb{Q}}(a)| = \prod_{i=1}^{r_1} |\sigma_i(a)| \prod_{j=1}^{r_2} |\sigma_{r_1+j}(a)|^2$ i la desigualtat de la mitjana geomètrica que

$$|\mathrm{N}_{K|\mathbb{Q}}(a)| \leq \left(\frac{1}{n}\sum_{i=1}^{r_1} |\sigma_i(a)| + \frac{2}{n}\sum_{j=1}^{r_2} |\sigma_{r_1+j}(a)|\right)^n,$$

que admet $\dfrac{\varepsilon^n}{n^n}$ com a fita superior. El resultat es dedueix del fet, ja demostrat i utilitzat a bastament, que $n = r_1 + 2r_2$. □

Corol·lari 4.4.3. *Amb les mateixes notacions que a la proposició anterior, tota classe d'ideals de A conté un representant enter $\mathfrak{a}$ tal que per a la seva norma absoluta se satisfà la desigualtat*

$$\mathcal{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\Delta|^{1/2}.$$

Demostració: Com que tota classe d'ideals conté un representant enter, podem prendre un representant enter $\mathfrak{b}$ de la classe inversa de la donada. Sigui $a \in \mathfrak{b}$ un element per al qual se satisfà la desigualtat de la proposició anterior. Com que $a \in \mathfrak{b}$, l'ideal $\mathfrak{a} := a\mathfrak{b}^{-1}$ és enter i se satisfà l'enunciat, ja que $\mathcal{N}(aA) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$. □

El resultat principal que volem demostrar en aquesta secció és el teorema de finitud del grup de classes d'ideals dels anells dels enters dels cossos de nombres.

Teorema 4.4.4 (Dirichlet)**.** *Sigui A l'anell dels enters d'un cos de nombres K. Aleshores, el grup de classes d'ideals de l'anell A és finit.*

Demostració: Apliquem la fita de Minkowski; tota classe d'ideals conté un ideal enter no nul de norma fitada per una constant que només depèn del cos. Però, per a tot nombre enter m, el conjunt dels ideals enters no nuls $\mathfrak{a} \subseteq A$ tals que $\mathcal{N}(\mathfrak{a}) = m$ és un conjunt finit; en efecte, de $\#A/\mathfrak{a} = m$ es dedueix immediatament que $m \in \mathfrak{a}$, de manera que $\mathfrak{a}$ divideix l'ideal mA. Així, d'ideals de norma fitada només n'hi ha un nombre finit i, en conseqüència, només hi ha un nombre finit de classes d'ideals. □

4.5 Teoremes de finitud

Una conseqüència important dels resultats de la secció anterior és el següent.

Teorema 4.5.1 (Hermite-Minkowski)**.** *Siguin $K \neq \mathbb{Q}$ un cos de nombres, A l'anell dels enters de K i Δ el generador positiu de l'ideal discriminant $\Delta(A|\mathbb{Z})$. Aleshores, $\Delta > 1$. En particular, existeix algun nombre primer p que ramifica en K.*

DEMOSTRACIÓ: La demostració d'aquest teorema es pot fer còmodament a partir del resultat següent.

Corol·lari 4.5.2. *Sigui $n := [K : \mathbb{Q}]$ el grau de K. Aleshores,*

$$\Delta \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

En particular, el quocient $\dfrac{n}{\log(\Delta)}$ està fitat superiorment per una constant independent del cos $K \neq \mathbb{Q}$.

DEMOSTRACIÓ: Com que per a tot ideal enter no nul $\mathfrak{a}$ és $\mathcal{N}(\mathfrak{a}) \geq 1$, el corol·lari **4.4.3** ens permet escriure la desigualtat $|\Delta|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}$; però $\pi < 4$ i $2r_2 \leq n$, de manera que $|\Delta| \geq u_n := \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$. Ara bé, per a la successió de terme general u_n se satisfan les propietats següents: $u_2 = \pi^2/4$ i $u_{n+1} \geq 3\pi u_n/4$, ja que el quocient u_{n+1}/u_n és l'expressió $\frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n}$, que és fitada inferiorment per $3\pi/4$ en virtut de la fórmula del binomi; per tant, s'obté la desigualtat $u_n \geq u_2\left(\frac{3\pi}{4}\right)^{n-2}$ que dóna la que volíem demostrar.

D'altra banda, si prenem logaritmes obtindrem la fita uniforme del quocient $\dfrac{n}{\log|\Delta|}$. □

Ara, la demostració del teorema d'Hermite-Minkowski és immediata si tenim en compte que, per a $n \geq 2$ és $\left(\frac{\pi}{3}\right)\left(\frac{3\pi}{4}\right)^{n-1} \geq \left(\frac{\pi}{3}\right)\left(\frac{3\pi}{4}\right) > 1$. □

Observació 4.5.3. Aquest resultat dista molt de ser general. En efecte, veurem que hi ha cossos de nombres que admeten extensions finites (fins i tot abelianes) que són no ramificades a tots els ideals primers del seu anell d'enters. Això succeeix, també, en un cas molt important: el cas local.

Encara més, demostrarem més endavant que tot cos local (que ja definirem) admet extensions no ramificades de grau arbitràriament gran, i totes elles són abelianes; en canvi, tot cos de nombres té només un nombre finit d'extensions abelianes no ramificades a tots els ideals primers del seu anell d'enters.

El resultat següent dóna informació sobre la quantitat de cossos de nombres "petits" que poden ramificar només en un conjunt donat de nombres primers.

Teorema 4.5.4 (Hermite)**.** *Sigui $D \in \mathbb{N}$ un nombre enter positiu qualsevol. El conjunt format pels cossos de nombres de discriminant absolut fitat per D és un conjunt finit; és a dir, si Δ_K denota el generador positiu de l'ideal discriminant d'un cos de nombres, aleshores és $\Delta_K > D$ llevat, potser, d'un nombre finit de cossos de nombres K.*

DEMOSTRACIÓ: El corol·lari que hem utilitzat en la demostració del teorema d'Hermite-Minkowski ens permet assegurar que el grau d'un cos de nombres està fitat superiorment pel logaritme d'una potència fixa del seu discriminant; per tant, és suficient demostrar

que el conjunt dels cossos de nombres de grau i discriminant donats és un conjunt finit. A més a més, per a n donat, només hi ha un nombre finit de parelles de nombres naturals r_1, r_2 tals que $n = r_1 + 2r_2$; per tant, podem suposar, també, que r_1, r_2 són fixos. Suposem, doncs, que $n = r_1 + 2r_2$, i que K és un cos de nombres de grau n i discriminant absolut Δ que admet exactament r_1 immersions reals. Cal veure que només podem elegir K entre un nombre finit de cossos.

Considerem el subconjunt $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definit de la manera següent:

(a) si $r_1 > 0$, prenem X com el producte dels discs de centre l'origen i radi $1/2$ a cada component complex no real, de l'interval $-1/2 \leq x \leq 1/2$ a cada factor $\mathbb{R}$ llevat del primer (si és que n'hi ha), i l'interval centrat a l'origen de longitud $2^n \left(\frac{2}{\pi}\right)^{r_2} |\Delta|^{1/2}$ en el primer component;

(b) si $r_1 = 0$, prenem X com el producte de discs de radi $1/2$ centrats a l'origen de cada factor $\mathbb{C}$ llevat del primer, i el rectangle definit per les condicions $|z - \overline{z}| \leq 2^{n-1}\pi \left(\frac{2}{\pi}\right)^{r_2} |\Delta|^{1/2}$, $|z + \overline{z}| \leq 1/2$, en el primer component $\mathbb{C}$.

En qualsevol cas, el conjunt X és un producte d'intervals i discs tancats, de manera que és compacte, simètric respecte de l'origen i convex, i el càlcul de la seva mesura dóna immediatament que $\mu(X) = 2^{n-r_2}|\Delta|^{1/2} = 2^n \mu(\sigma(\mathcal{O}_K))$. Per tant, existeix un nombre enter no nul $a \in A$ tal que $\sigma(a) \in X$. Veiem que a és un element primitiu de l'extensió $K|\mathbb{Q}$.

En efecte, els conjugats de a són els nombres $\sigma_i(a)$ i $\overline{\sigma_i(a)}$, comptats tantes vegades com el grau de l'extensió $K|\mathbb{Q}(a)$. Per a $i > 1$, els nombres $\sigma_i(a)$ i $\overline{\sigma_i(a)}$ són de mòdul menor que 1 per construcció de X. Si tenim en compte la fórmula $\mathrm{N}_{K|\mathbb{Q}}(a) = \prod_{i=1}^{n} \sigma_i(a)$, i prenem mòduls, observarem que $|\sigma_1(a)| > 1$, ja que la norma de a és un nombre enter per ser a un enter algebraic no nul. En particular, si $r_1 > 0$ obtenim que $\sigma_1(a)$ és diferent de tots els altres conjugats, de manera que el grau de l'extensió $K|\mathbb{Q}(a)$ és 1 i a és un element primitiu de K. Si $r_1 = 0$, el mateix argument demostra que és $|\sigma(a)| = |\overline{\sigma_1(a)}| > 1$, de manera que $\sigma_1(a)$ és diferent de tots els $\sigma_i(a)$ i dels $\overline{\sigma_i(a)}$ per a $i > 1$; però, per construcció de X, la part real de $\sigma_1(a)$ és de mòdul menor o igual que $1/4$, de manera que $\sigma_1(a)$ no pot ser real ja que és de mòdul > 1; en particular, també $\sigma_1(a)$ és diferent de $\overline{\sigma_1(a)}$ i, en conseqüència, a és un element primitiu de K.

Ara ja estem; en efecte, els conjugats de a són nombres complexos (o reals) fitats per construcció del conjunt X; per tant, també són fitats els valors dels polinomis simètrics elementals construïts amb aquests nombres; com que aquests valors són els coeficients del polinomi $\mathrm{Irr}(a, \mathbb{Q})(X)$, i aquests coeficients són nombres enters, ja que a és un enter algebraic, només hi ha un nombre finit de possibilitats per al polinomi $\mathrm{Irr}(a, \mathbb{Q})(X)$ i, en conseqüència, un nombre finit de possibilitats per a l'element primitiu a. □

Observació 4.5.5. Aquest resultat admet altres formulacions interessants. Per exemple, si fixem un conjunt finit de nombres primers i un nombre enter $N > 1$, aleshores el conjunt format pels cossos de nombres de grau $n \leq N$ que no ramifiquen fora dels primers fixats és, també, un conjunt finit.

4.6 El teorema de Dirichlet de les unitats

En aquesta secció es tracta de fer l'estudi del grup de les unitats dels cossos de nombres. Així com per a l'estudi de l'estructura lineal ha anat bé la immersió canònica dels cossos de nombres en $\mathbb{R}^n$, ara convindrà fer quelcom semblant; haurem de considerar alguna immersió que tingui en compte la multiplicativitat del grup. Això es fa "prenent logaritmes".

Siguin K un cos de nombres, A l'anell dels enters de K, r_1 el nombre d'immersions reals de K, r_2 el de parelles d'immersions complexes conjugades no reals, $n = r_1 + 2r_2$ el grau de l'extensió, i designem per U el grup dels elements invertibles de A.

La immersió canònica de K en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ és un morfisme d'anells; convé prendre logaritmes a cada component a fi d'obtenir un morfisme de grups. Concretament, considerem l'aplicació $\log : K^* \longrightarrow \mathbb{R}^{r_1+r_2}$ definida per la fórmula

$$u \mapsto (\log|\sigma_1(u)|, \ldots, \log|\sigma_{r_1}(u)|, \log|\sigma_{r_1+1}(u)|, \ldots, \log|\sigma_{r_1+r_2}(u)|).$$

Igual que en el cas de la immersió canònica, ens oblidem de la meitat dels components complexos no reals; això és degut al fet que si consideréssim també els altres r_2 components no obtindríem components diferents dels anteriors, ja que el mòdul d'un nombre complex coincideix amb el del seu conjugat. D'altra banda, per a $u, v \in K^*$ se satisfà la igualtat $\log(uv) = \log(u) + \log(v)$, de manera que log és un morfisme del grup multiplicatiu K^* en el grup additiu $\mathbb{R}^{r_1+r_2}$. S'anomena la immersió logarítmica de K, en contraposició a la immersió canònica. El teorema que es tracta de provar és el següent.

Teorema 4.6.1 (Dirichlet)**.** *El grup de les unitats U de A és el producte del grup, finit, de les arrels de la unitat de K, per un grup abelià lliure de rang $r := r_1 + r_2 - 1$.*

Demostració: Farem la demostració d'aquest teorema en diverses etapes. Acabem de veure que la immersió logarítmica és un morfisme de grups.

Lema 4.6.2. *Sigui H l'hiperplà de $\mathbb{R}^{r+1}$ format pels elements $(x_1, \ldots, x_{r+1})$ tals que $x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0$. Aleshores, $\log(U) \subseteq H$.*

Demostració: Com que les unitats de A són elements de A de norma ± 1, resulta que per a les seves imatges se satisfà l'equació

$$\sum_{i=1}^{r_1} \log|\sigma_i(u)| + 2\sum_{j=1}^{r_2} \log|\sigma_{r_1+j}(u)| = \sum_{i=1}^{r_1+2r_2} \log|\sigma_i(u)| = \log|\mathrm{N}_{K|\mathbb{Q}}(u)| = 0,$$

de manera que la imatge de U està inclosa en H. □

Lema 4.6.3. *Per a tot subconjunt compacte $X \subseteq \mathbb{R}^{r+1}$, el conjunt dels elements $u \in U$ tals que $\log(u) \in X$ és finit. En particular, $\log(U)$ és un subgrup discret de $\mathbb{R}^{r+1}$.*

Demostració: Sigui $X \subseteq \mathbb{R}^{r+1}$ un subconjunt compacte. Aleshores, X és un conjunt fitat, de manera que si $u \in U$ és tal que $\log(u) \in X$, aleshores els conjugats de u són fitats i la fita només depèn de X. Per tant, els polinomis simètrics elementals dels conjugats de u són fitats; és a dir, els coeficients (enters) del polinomi irreductible de u sobre $\mathbb{Q}$ són fitats. Això implica que només hi ha un nombre finit de possibilitats per a aquests polinomis i, en conseqüència, un nombre finit d'elements $u \in U$ tals que $\log(u) \in X$. □

Corol·lari 4.6.4. *El nucli del morfisme* $\log : U \longrightarrow \mathbb{R}^{r+1}$ *està format exactament per les arrels de la unitat de* K.

Demostració: El nucli de log és la antiimatge del compacte $\{0\}$, de manera que és un subgrup finit de U. Per tant, és un subgrup finit del grup multiplicatiu d'un cos i, en conseqüència, és cíclic i format per arrels de la unitat. D'altra banda, totes les arrels de la unitat de K són elements invertibles de A i són nombres complexos de mòdul 1; com que els seus conjugats també són arrels de la unitat, també són de mòdul 1 i, en conseqüència, pertanyen al nucli de log. □

Com que H és isomorf a $\mathbb{R}^r$ i $\log(U)$ és un subgrup discret de $\mathbb{R}^{r+1}$, hem demostrat que el quocient de U pel subgrup de les arrels de la unitat de K és (isomorf a) un subgrup discret de $\mathbb{R}^r$; per tant, un grup abelià lliure de rang $\leq r$. En particular, si $r = 0$ ja hem acabat la demostració i podem suposar que $r \geq 1$. Només resta veure que la imatge $\log(U)$ és de rang exactament r. Per a això, és suficient demostrar que $\log(U)$ conté r vectors linealment independents. I, per a veure aquest fet, només cal comprovar que si ω és una forma lineal no nul·la definida en H, aleshores existeix un element $u \in U$ tal que $\omega(\log(u)) \neq 0$; és a dir, que $\log(U)$ no està inclòs en el nucli de cap forma lineal no nul·la. Per tant, la resta de la prova consisteix a cercar aquesta unitat u.

Com que H és de dimensió r i cap dels components de H no és nul, la projecció de $\mathbb{R}^{r+1}$ en els primers r components dóna un isomorfisme de H en $\mathbb{R}^r$; per tant, una forma lineal en H es pot pensar definida per una fórmula $\omega(x_1, \ldots, x_r) = c_1x_1 + \cdots + c_rx_r$, on $c_1, \ldots, c_r \in \mathbb{R}$ són constants que només depenen de la forma ω i no del punt $(x_1, \ldots, x_r) \in \mathbb{R}^r$. En particular, podem pensar $\omega(\log(u))$ com la forma ω aplicada als primers r components de $\log(u)$.

Lema 4.6.5. *Siguin* $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2}$ *nombres reals estrictament positius. Posem* $\varepsilon_{r_1+r_2+j} := \varepsilon_{r_1+j}$ *per a* $1 \leq j \leq r_2$ *i suposem que*

$$\varepsilon := \prod_{i=1}^{n} \varepsilon_i = \left(\frac{2}{\pi}\right)^{r_2} |\Delta|^{1/2}.$$

Aleshores, existeix $a \in A$, $a \neq 0$, *tal que per a tots els components* $\log|\sigma_i(a)|$ *se satisfan les desigualtats*

$$0 \leq \log(\varepsilon_i) - \log|\sigma_i(a)| \leq \log(\varepsilon)$$

i, a més a més, $|\mathrm{N}_{K|\mathbb{Q}}(a)| \leq \varepsilon$.

Demostració: Sigui $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ el conjunt dels elements $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$ tals que $|x_i| \leq \varepsilon_i$, $1 \leq i \leq r_1$, i $|z_j| \leq \varepsilon_{r_1+j}$, $1 \leq j \leq r_2$. Clarament, X és un subconjunt compacte, convex i simètric respecte de l'origen, i la seva mesura de Lebesgue és exactament

$$\mu(X) = \prod_{i=1}^{r_1}(2\varepsilon_i)\prod_{j=1}^{r_2}(\pi\varepsilon_{r_1+j}^2) = 2^{r_1}\pi^{r_2}\varepsilon = 2^{r_1+r_2}|\Delta|^{1/2} = 2^{n-r_2}|\Delta|^{1/2} = 2^n\mu(\sigma(A)).$$

Per tant, el teorema de Minkowski ens permet assegurar l'existència d'un element no nul $a \in A$ tal que $\sigma(a) \in X$; això és dir que per als components $\sigma_i(a)$ se satisfan les desigualtats $|\sigma_i(a)| \leq \varepsilon_i$, per a $1 \leq i \leq n$. Com que a és un enter algebraic no nul, és

$|\mathrm{N}_{K|\mathbb{Q}}(a)| \geq 1$, de manera que obtenim les desigualtats

$$1 \leq |\mathrm{N}_{K|\mathbb{Q}}(a)| = \prod_{i=1}^{n} |\sigma_i(a)| \leq \varepsilon.$$

D'altra banda, si ens fixem en un índex i obtenim que

$$|\sigma_i(a)|^{-1} = |\mathrm{N}_{K|\mathbb{Q}}(a)|^{-1} \prod_{j\neq i} |\sigma_j(a)| \leq |\mathrm{N}_{K|\mathbb{Q}}(a)|^{-1} \prod_{j\neq i} \varepsilon_j \leq \prod_{j\neq i} \varepsilon_j = \varepsilon\varepsilon_i^{-1}$$

que dóna $\varepsilon_i\varepsilon^{-1} \leq |\sigma_i(a)| \leq \varepsilon_i$ per a $1 \leq i \leq n$.

Les desigualtats desitjades s'obtenen en prendre logaritmes. □

Aplicarem aquest resultat de la manera següent: donada la forma lineal ω definida per l'equació $\omega(x_1, \ldots, x_r) = c_1x_1 + \cdots + c_rx_r$, elegim nombres reals positius ε_i per als quals se satisfacin les condicions del lema i sigui M un nombre real fix tal que $M > \sum_{i=1}^{r} |c_i| \log(\varepsilon)$. Aleshores, per a l'element $a \in A$ que proporciona el lema se satisfà la desigualtat

$$\left| \omega(\log(a)) - \sum_{i=1}^{r} c_i \log(\varepsilon_i) \right| < M.$$

El final de la demostració consisteix a prendre una successió d'elements $a_h \in A$ per als quals se satisfacin les condicions anteriors i alguna més. Concretament, per a tot nombre natural $h > 0$, podem elegir els elements ε_i, $1 \leq i \leq r$, del lema de manera que se satisfaci la igualtat $\sum_{i=1}^{r} c_i \log(\varepsilon_i) = 2hM$, ja que algun coeficient c_i és no nul; després, triem ε_{r+1} de manera que se satisfaci la condició del lema. Ara, per a l'element a_h que ens proporciona el lema, se satisfà la desigualtat $|\omega(\log(a_h)) - 2hM| < M$; és a dir,

$$(2h-1)M < \omega(\log(a_h)) < (2h+1)M.$$

Això produeix una successió d'enters algebraics $a_h \in A$ per als quals se satisfan les desigualtats anteriors i, a més a més, són de norma fitada per ε. En conseqüència, els ideals a_hA són tots de norma $\mathcal{N}(aA) \leq \varepsilon$; per tant, són en nombre finit. Això implica que existeixen nombres naturals diferents h, k tals que $a_hA = a_kA$ i, per tant, existeix una unitat $u \in U$ tal que $a_k = ua_h$. Si suposem que $h < k$, obtenim les desigualtats

$$\omega(\log(a_h)) < (2h+1)M \leq (2k-1)M < \omega(\log(a_k)),$$

de manera que $\omega(\log(u)) = \omega(\log(a_k)) - \omega(\log(a_h)) > 0$, i obtenim la unitat $u \in U$ tal que $\omega(\log(u)) \neq 0$ que desitjàvem trobar. □

Definició 4.6.6. S'anomena sistema fonamental d'unitats (o conjunt fonamental d'unitats) d'un cos de nombres K tot conjunt $\{u_1, \ldots, u_r\}$ d'unitats de l'anell dels enters de K tal que tota unitat $u \in U$ s'expressa de manera única en la forma

$$u = \eta u_1^{m_1} \cdots u_r^{m_r},$$

on η és una arrel de la unitat del cos K i els m_i són nombres enters.

Amb aquesta definició, el teorema de Dirichlet de les unitats admet la formulació equivalent següent.

Corol·lari 4.6.7. *Tot cos de nombres admet un sistema fonamental d'unitats* $u_1, \ldots, u_r \in U$. □

4.7 Unitats dels cossos quadràtics

Un cas senzill de càlcul de les unitats d'un cos de nombres és el cas dels cossos quadràtics. Suposem, doncs, que D és un nombre enter lliure de quadrats i posem $K := \mathbb{Q}(\sqrt{D})$, A l'anell dels enters de K, U el grup de les unitats de A, i $W \subseteq U$ el grup de les arrels de la unitat de K.

Proposició 4.7.1. *Si $D < 0$, és a dir, si K és un cos quadràtic imaginari, aleshores $U = W$. A més a més,*

$$W = \begin{cases} \{1, -1\}, & \text{si } D \neq -1, -3, \\ \{1, -1, i, -i\}, & \text{si } D = -1, \\ \{1, -1, \rho, -\rho, \rho^2, -\rho^2\}, & \text{si } D = -3, \end{cases}$$

on $\rho := \dfrac{-1 + \sqrt{-3}}{2}$ és una arrel cúbica primitiva de la unitat.

Demostració: En efecte, en el cas $D < 0$ no hi ha cap immersió real de K, de manera que el rang del grup de les unitats és $r = r_1 + r_2 - 1 = 0$, ja que de $2 = r_1 + 2r_2$ i $r_1 = 0$ es dedueix que $r_2 = 1$ i, per tant, que $r = 0$. En conseqüència, el grup de les unitats no té part lliure i coincideix amb el grup de les arrels de la unitat del cos K.

D'altra banda, si K conté una arrel n-èsima de la unitat ζ, aleshores el grau de K és divisible per $\varphi(n)$, ja que $\mathbb{Q}(\zeta) \subseteq K$; les úniques possibilitats perquè K sigui de grau 2 són que $\varphi(n) = 1$ o $\varphi(n) = 2$; i això només succeeix per als valors $n \in \{1, 2, 3, 4, 6\}$. Com que per a tot cos de nombres és $\{\pm 1\} \subseteq W$, la proposició és immediata. □

El cas $D > 0$ és una mica més complicat; en efecte, en aquest cas les dues immersions de K són reals, de manera que $r_1 = 2$, $r_2 = 0$ i el rang del grup de les unitats de K és $r = 1$. Com que les úniques arrels de la unitat de $\mathbb{R}$ són ± 1, el grup de les arrels de la unitat de K és $W = \{1, -1\}$. Això significa que existeix una unitat $u \in U$ tal que totes les unitats de A són els nombres $\pm u^m$, amb $m \in \mathbb{Z}$. A més a més, podem triar u de manera que sigui $u > 1$. En efecte, com que $-1 \in W$, podem suposar que $u > 0$ i després, com que $u \in U$ equival a $u^{-1} \in U$ i exactament un dels dos elements és > 1, llevat que $u = 1$, podem canviar, si convé, el generador u per u^{-1}. En definitiva, hem provat el resultat següent.

Proposició 4.7.2. *Suposem que $D > 0$. Aleshores, el grup W de les arrels de la unitat de $\mathbb{Q}(\sqrt{D})$ és el grup $\{1, -1\}$. Existeix una unitat $u > 1$ de l'anell dels enters de $\mathbb{Q}(\sqrt{D})$ tal que totes les altres unitats s'escriuen de manera única en la forma $\pm u^m$ amb $m \in \mathbb{Z}$.* □

Aquesta unitat $u > 1$ és una unitat fonamental de $\mathbb{Q}(\sqrt{D})$; s'anomena **la** unitat fonamental; és la més petita de totes les unitats $v > 1$ de l'anell dels enters de $\mathbb{Q}(\sqrt{D})$. Existeixen algoritmes per a calcular aquesta unitat de manera explícita.

Proposició 4.7.3. *Sigui $D > 0$ un nombre enter lliure de quadrats. La unitat fonamental de $\mathbb{Q}(\sqrt{D})$ és el nombre $u := \dfrac{a + b\sqrt{D}}{2}$ on b és el menor nombre enter positiu tal que un dels dos nombres $Db^2 \pm 4$ és un quadrat i $a > 0$ és el nombre enter positiu tal que $a^2 = Db^2 \pm 4$ on es pren el signe menys si les dues equacions tenen solució. A més a més, la norma de la unitat fonamental u és exactament el signe que fa que l'equació tingui solució, i -1 si totes dues en tenen.*

DEMOSTRACIÓ: Posem $K := \mathbb{Q}(\sqrt{D})$ i sigui $u > 1$ una unitat de A; podem escriure u en la forma $u = \dfrac{a+b\sqrt{D}}{2}$ on a, b són nombres enters de la mateixa paritat i tots dos parells si $D \not\equiv 1 \pmod 4$. Com que $D > 1$, si $a, b > 0$, aleshores $u > 1$; si $a, b < 0$, aleshores $u < -1$; i si $ab < 0$, aleshores $|u| < 1$. Per tant, les unitats $u > 1$ de K s'escriuen en la forma $u = \dfrac{a+b\sqrt{D}}{2}$ amb $a, b > 0$ nombres enters de la mateixa paritat, tots dos parells si $D \not\equiv 1 \pmod 4$. En particular, el càlcul de la norma de u dóna $\mathrm{N}(u) = \dfrac{a+b\sqrt{D}}{2}\,\dfrac{a-b\sqrt{D}}{2} = \dfrac{a^2-Db^2}{4} = \pm 1$, de manera que l'equació $a^2 - Db^2 = \pm 4$ té solució, amb el signe igual a la norma de la unitat u. A més a més, la menor unitat $u > 1$ ha de ser la unitat fonamental. Resta veure, doncs, que la menor unitat $u > 1$ s'obté en prendre els menors nombres enters $a, b > 0$ que satisfan l'equació $a^2 - Db^2 = \pm 4$.

Observem que podem escriure l'equació en la forma $a^2 \mp 4 = Db^2$, de manera que en fer b més petit i mantenir el signe també a és més petit; a més a més, si per algun valor de b les dues equacions tenen solució, el menor valor de a correspon a l'equació amb signe $+1$ i hi ha una unitat de norma -1; en aquest cas, la unitat fonamental és de norma -1, ja que la norma és multiplicativa. Finalment, un senzill càlcul demostra que si tenim nombres enters $a, b, a', b' > 0$ tals que $b' < b$ i que $a^2 + 4 = Db^2$ i $a'^2 - 4 = Db'^2$, aleshores també ha de ser $a' < a$. Així, el resultat queda demostrat completament, ja que a valors menors de b corresponen valors menors de a. □

4.8 Exemples

L'objectiu d'aquesta secció és donar alguns exemples d'aplicació de tècniques d'aquest capítol i dels anteriors al càlcul explícit d'alguns invariants dels anells dels enters d'alguns cossos de nombres.

Exemple 4.8.1. Considerem, en primer lloc, el cos $K := \mathbb{Q}(\sqrt{-23})$.

Com que $-23 \equiv 1 \pmod 4$, l'anell dels enters és l'anell $A := \mathbb{Z}[\omega]$ on $2\omega = 1 + \sqrt{-23}$ i el discriminant absolut és $\Delta = -23$. En particular, l'únic primer que ramifica és 23. D'altra banda, com que K és un cos quadràtic imaginari, obtenim immediatament el valor de les constants $r_1 = 0$ i $r_2 = 1$; en particular, el grup de les unitats de A és el grup $\{1, -1\}$. Anem a estudiar el grup de classes d'ideals, $H := \mathrm{Cl}(A)$.

Per a la fita de Minkowski, $\left(\dfrac{4}{\pi}\right)^{r_2} \dfrac{n!}{n^n}|\Delta|^{1/2}$, tenim que

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\Delta|^{1/2} = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{23} < \left(\frac{2}{\pi}\right)\sqrt{25} = \frac{10}{\pi} < 4,$$

de manera que cada classe d'ideals té un representant de norma ≤ 3. En conseqüència, el grup de classes d'ideals, H, està generat per tots els ideals primers de A de norma 2 i de norma 3, si n'hi ha; aquests ideals han de dividir els ideals $2A$ i $3A$. Però les lleis de descomposició dels primers en els cossos quadràtics ens permeten assegurar de seguida que $2A = \mathfrak{p}_2\mathfrak{p}_2'$ i que $3A = \mathfrak{p}_3\mathfrak{p}_3'$, on $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_3$, i $\mathfrak{p}_3'$ són ideals primers diferents de A de grau residual 1, ja que $-23 \equiv 1 \pmod 8$ i $\left(\dfrac{-23}{3}\right) = 1$. A més a més, com que els

productes $\mathfrak{p}_2\mathfrak{p}_2'$ i $\mathfrak{p}_3\mathfrak{p}_3'$ són ideals principals, el grup de classes d'ideals de A està generat per les classes dels ideals $\mathfrak{p}_2$ i $\mathfrak{p}_3$.

D'altra banda, $\mathrm{N}\left(\dfrac{1+\sqrt{-23}}{2}\right) = 6$, de manera que l'ideal generat per aquest element és producte d'un ideal de norma 2 i un de norma 3; en conseqüència, o bé el producte $\mathfrak{p}_2\mathfrak{p}_3$ és principal, o bé ho és el producte $\mathfrak{p}_2\mathfrak{p}_3'$, de manera que el grup de classes d'ideals de A està generat per la classe de l'ideal $\mathfrak{p}_2$. Aquest ideal no pot ser principal, ja que per a tot element $\alpha := \dfrac{a+b\sqrt{-23}}{2} \in A$ és $\mathrm{N}(\alpha) = \dfrac{a^2+23b^2}{4} \neq 2$; a més a més, l'element $\alpha := \dfrac{3+\sqrt{-23}}{2}$ és de norma $\mathrm{N}(\alpha) = 8$, de manera que l'ideal αA és el producte de tres ideals primers de norma 2; això dóna les possibilitats $\alpha A = \mathfrak{p}_2^3$, o bé $\alpha A = 2\mathfrak{p}_2$. La darrera és impossible, ja que això ens diria que $\mathfrak{p}_2$ és l'ideal generat per l'element enter $\dfrac{3+\sqrt{-23}}{4}$, que no és enter algebraic. Per tant, el cub de l'ideal $\mathfrak{p}_2$ és un ideal principal i, per tant, el grup de classes d'ideals de A és un grup cíclic de 3 elements.

Exemple 4.8.2. El cos $K := \mathbb{Q}(\theta)$, on θ és una arrel del polinomi $f(X) := X^3 + X + 1$.

En primer lloc, el polinomi $f(X)$ és irreductible, ja que ho és mòdul 2; d'altra banda, com que tots els coeficients no nuls són positius, $f(X)$ no té cap arrel real positiva, i la regla de Descartes ens permet assegurar que en té exactament una de negativa; per tant, $f(X)$ només té una arrel real. En conseqüència, $r_1 = r_2 = r = 1$. El discriminant de les potències de θ és exactameent -31. En efecte, de $\theta^3 + \theta + 1 = 0$ s'obté successivament que

$$\theta(\theta^2+1) = -1, \quad \theta = \frac{-1}{\theta^2+1}, \quad \theta^2 = \frac{1}{\theta^4+2\theta^2+1}, \quad (\theta^2)^3 + 2(\theta^2)^2 + (\theta^2) - 1 = 0$$

que, juntament amb les fórmules

$$\theta^3 = -\theta - 1, \qquad \text{i} \qquad \theta^4 = -\theta^2 - \theta,$$

permet obtenir les traces

$$\mathrm{T}(\theta) = 0, \quad \mathrm{T}(\theta^2) = -2, \quad \mathrm{T}(\theta^3) = -3, \quad \mathrm{T}(\theta^4) = 2,$$

de manera que el discriminant de les potències de θ és el determinant

$$\begin{vmatrix} 3 & 0 & -2 \\ 0 & -2 & -3 \\ -2 & -3 & 2 \end{vmatrix} = -31.$$

D'aquí ja podem deduir dues coses importants; d'una banda, que el discriminant de l'extensió és -31, ja que -31 és lliure de quadrats; de l'altra, com que el discriminant de les potències de θ coincideix amb el discriminant del cos, les potències de θ han de formar una $\mathbb{Z}$-base de l'anell dels enters de K. En particular, l'anell dels enters és $A := \mathbb{Z}[\theta]$. D'altra banda, podem fitar la constant de Minkowski per $\dfrac{4}{\pi}\dfrac{3!}{3^3}\sqrt{31} < 2$, de manera que l'anell A és principal.

Les arrels de la unitat de K són exactament 1 i -1, ja que podem pensar que θ és real, de manera que $K \subseteq \mathbb{R}$. Resta calcular una unitat fonamental. Ja hem vist més amunt que $\eta := 1 + \theta^2$ és una unitat de A; i és clar que és $\eta > 1$. Veurem que η és una unitat fonamental de A. Per a això, demostrarem un resultat previ.

Lema 4.8.3. *Sigui $K \subseteq \mathbb{R}$ un cos cúbic tal que $r_1 = r_2 = 1$. Aleshores, tota unitat positiva $u \in A$ és de norma 1 i, si $u > 1$ i Δ designa el discriminant absolut de l'extensió $A|\mathbb{Z}$, se satisfà la desigualtat $|\Delta| < 4u^3 + 24$.*

Demostració: La norma d'una unitat i la norma de la seva inversa coincideixen, de manera que podem suposar que $u > 1$; com que $u \neq \pm 1$, u és un element primitiu de l'extensió $K|\mathbb{Q}$, i el seu polinomi irreductible és de la forma $(X-u)(X-\alpha)(X-\overline{\alpha})$, on $\alpha \in \mathbb{C}$, $\alpha \notin \mathbb{R}$, i $\overline{\alpha}$ designa el complex conjugat de α; això és degut al fet que $r_2 = 1$. La norma de u és, doncs, el producte dels conjugats de u, de manera que és $\mathrm{N}(u) = u\alpha\overline{\alpha} > 0$; per tant, ha de ser $\mathrm{N}(u) = 1$.

Com que el discriminant de les potències de u és un múltiple del discriminant de l'extensió $A|\mathbb{Z}$, és suficient demostrar que $|D(1,u,u^2)| \leq 4u^3+24$. Podem escriure $u = r^2$, $\alpha = r^{-1}e^{ix}$, $\overline{\alpha} = r^{-1}e^{-ix}$, amb $r, x \in \mathbb{R}$, $r > 0$, de manera que el discriminant de les potències de u es pot calcular per la fórmula

$$\begin{aligned} D(1,u,u^2) &= \begin{vmatrix} 1 & 1 & 1 \\ r^2 & r^{-1}e^{ix} & r^{-1}e^{-ix} \\ r^4 & r^{-2}e^{2ix} & r^{-2}e^{-2ix} \end{vmatrix}^2 \\ &= \left(e^{2ix} - e^{-2ix} - (e^{ix} - e^{-ix})(r^3 + r^{-3})\right)^2 \\ &= \left(2i\sin(2x) - 2i(r^3 + r^{-3})\sin(x)\right)^2 \\ &= -4sin^2(x)\left(2\cos(x) - (r^3 + r^{-3})\right)^2. \end{aligned}$$

Considerem la funció $g : \mathbb{R} \longrightarrow \mathbb{R}$ definida per la fórmula

$$g(x) := 4sin(x)\,(cos(x) - a)\,,$$

on $2a := r^3 + r^{-3}$. Com que el valor absolut del discriminant $D(1,u,u^2)$ és el quadrat del valor en x de la funció g, és suficient demostrar que $|g(x)|^2 < 4u^3 + 24$ per a tot nombre real x. Com que la funció g és contínua i periòdica, té màxim i mínim i el màxim de $|g(x)|^2$ és el quadrat d'un dels extrems de g; per tant, és suficient provar que el quadrat d'aquests extrems és menor que $4u^3+24$. Sigui $x_0 \in \mathbb{R}$ un punt on $g(x)$ tingui un extrem; aleshores, la derivada de g s'ha d'anul·lar en x_0, de manera que $\cos(x_0)$ ha de ser una arrel del polinomi $2t^2 - at - 1$; posem $t_0 := \cos(x_0)$. La igualtat $at_0 = 2t_0^2 - 1$ aplicada successivament dóna la cadena d'igualtats

$$\begin{aligned} |g(x_0)|^2 &= 16\sin^2(x_0)\,(\cos(x_0) - a)^2 \\ &= 16(1 - t_0^2)\left(t_0^2 - 2at_0 + a^2\right) \\ &= 16(1 - t_0^2)\left(a^2 + 2 - 3t_0^2\right) \\ &= 16\left(a^2 - t_0^4 - t_0^2 + 1\right) \\ &= 4r^6 + 4r^{-6} + 8 - 16t_0^4 - 16t_0^2 + 16 \\ &= 4u^3 + 24 + 4\left(r^{-6} - 4t_0^4 - 4t_0^2\right), \end{aligned}$$

de manera que és suficient veure que $r^{-6} < 4t_0^2$. Ara bé, si $t_0 \geq 0$, aleshores $4t_0^2 = 2 + 2at_0 \geq 2$ i, com que $r^{-6} = u^{-3} < 1$, la desigualtat queda provada. Finalment, si $t_0 < 0$, alsehores $t_0 < \dfrac{-1}{2r^3} < 0$, ja que el valor del polinomi $2t^2 - at - 1$ en $\dfrac{-1}{2r^3}$ és $\dfrac{3(1-r^6)}{4r^6} < 0$ i el valor en t_0 és zero; en elevar al quadrat obtenim la desigualtat que desitjàvem. □

Amb aquest resultat a la nostra disposició, podem procedir a demostrar que η és la menor de les unitats de A que és > 1 i, per tant, una unitat fonamental.

En primer lloc, se satisfà la igualtat $\eta^3 = \eta^2 + 1$ (comprovació immediata), que s'obté en calcular el polinomi $\mathrm{Irr}(\eta, \mathbb{Q})(X)$. Si apliquem el lema, com que el discriminant absolut de K és -31, per a tota unitat $u > 1$ de A i, en particular, per a la unitat fonamental $u > 1$ de A, se satisfà la desigualtat $31 < 4u^3 + 24$; és a dir, $u^3 > 7/4$. Ara bé, si fos $\eta \geq 7/4$, obtindríem la desigualtat contradictòria

$$\frac{7}{4} \leq \eta = \frac{\eta^3}{\eta^2} = 1 + \frac{1}{\eta^2} \leq 1 + \frac{16}{49} = \frac{65}{49} < \frac{70}{49} < \frac{70}{40} = \frac{7}{4}.$$

Per tant, η no pot ser divisible pel cub de u. Però η és una potència de u; si veiem que η no és el quadrat d'una unitat positiva, haurem obtingut $\eta = u$ i, en conseqüència, η és una unitat fonamental de A.

Com que $\eta = -\theta^{-1}$, obtenim que $A = \mathbb{Z}[\eta]$, de manera que si η fos un quadrat, l'equació $\eta = (a + b\eta + c\eta^2)^2$ hauria de tenir solucions enteres a, b, c. Però els nombres $1, \eta, \eta^2$ són $\mathbb{Q}$-linealment independents i l'equació anterior es pot escriure en la forma

$$\eta = (a^2 + c^2 + 2bc) + (c^2 + 2ab)\eta + (c^2 + 2bc + 2ac + b^2)\eta^2,$$

si tenim en compte l'expressió de les potències de η que s'obtenen a partir de la igualtat $\eta^3 = \eta^2 + 1$; per tant, s'han de satisfer les igualtats

$$\begin{aligned} a^2 + c^2 + 2bc &= 0 \\ c^2 + 2ab &= 1 \\ c^2 + 2bc + 2ac + b^2 &= 0. \end{aligned}$$

Això ens ensenya que c és senar i, després, que a i b també són senars; aleshores, la reducció mòdul 4 de l'equació $c^2 + 2ab = 1$ duu a contradicció. Per tant, η no és el quadrat de cap element de A i això acaba la prova.

Capítol 5

Ramificació superior

Aquest capítol es dedica a fer l'estudi dels grups de ramificació superior; abans, però, fem l'estudi del diferent i de la seva relació amb el discriminant i la ramificació. L'estudi d'aquests conceptes serà bàsic per a la prova del teorema de Kronecker-Weber.

5.1 El diferent

Hem vist en el capítol 3, secció 6, que el discriminant és un invariant associat a una extensió entera finita i separable d'anells de Dedekind i que determina els ideals primers de l'anell base que ramifiquen a l'extensió (cf. la proposició **3.7.1**). En aquesta secció es tracta de definir un invariant de l'anell extensió que ens doni la informació de manera més precisa: concretament, el diferent de l'extensió dóna compte dels ideals de l'anell extensió que són ramificats sobre la seva base.

De manera similar al cas del discriminant, considerem un domini íntegrament tancat A, el seu cos de fraccions K, i una extensió finita i separable $L|K$; ara, però, en comptes de considerar la clausura entera de A en L considerarem, de manera més general, un subanell B de L tal que l'extensió $B|A$ sigui entera i que L sigui el cos de fraccions de B.

Definició 5.1.1. El codiferent $\mathcal{C}(B|A)$ és el subconjunt de L format per tots els elements $b \in L$ tals que $\mathrm{T}_{L|K}(bB) \subseteq A$.

Com que l'extensió $B|A$ és entera i A és íntegrament tancat, la traça dels elements de B està en A, de manera que se satisfà la inclusió $B \subseteq \mathcal{C}(B|A)$; d'altra banda, és immediat de la definició que $\mathcal{C}(B|A)$ és un B-submòdul de L; encara més, és el més gran dels B-submòduls $M \subseteq L$ tals que $\mathrm{T}_{L|K}(M) \subseteq A$.

Proposició 5.1.2. *Amb les notacions i les hipòtesis precedents, el codiferent $\mathcal{C}(B|A)$ és un ideal fraccionari de B.*

Demostració: Si demostrem que $\mathcal{C}(B|A)$ està inclòs en un B-submòdul finitament generat de L, en prendre un denominador comú $b \in B$ d'un conjunt finit de generadors obtindrem la inclusió $b\mathcal{C}(B|A) \subseteq B$ i haurem acabat. Per tant, només cal veure que $\mathcal{C}(B|A)$ està inclòs en un B-submòdul finitament generat de L i és suficient demostrar que $\mathcal{C}(B|A)$ està inclòs en un A-submòdul finitament generat de L.

El càlcul que segueix ja ha estat usat anteriorment. Considerem una K-base de L, $\{e_1, \ldots, e_n\}$, formada per elements $e_i \in B$. Per a tot element $b \in \mathcal{C}(B|A)$ podem escriure una igualtat $b = a_1e_1 + \cdots + a_ne_n$ amb els elements a_i en K; si D denota el discriminant $D := D(e_1, \ldots, e_n) \in A$, com que la traça dels elements be_j està en A per definició de $\mathcal{C}(B|A)$, obtenim les relacions $Da_i \in A$, de manera que $\mathcal{C}(B|A) \subseteq \bigoplus_{i=1}^{n} D^{-1}Ae_i$, que és un A-submòdul finitament generat de L. □

Observació 5.1.3. En el cas que B és la clausura entera de A en L, disposem d'una altra caracterització de l'ideal codiferent. Com que la forma bilineal traça $\mathrm{T}_{L|K} : L \times L \longrightarrow K$ és no degenerada (recordem que l'extensió $L|K$ és separable, per definició), l'aplicació

$$L \xrightarrow{\varphi} \mathrm{Hom}_K(L, K), \qquad b \mapsto \mathrm{T}_{L|K}(b \cdot *),$$

és un isomorfisme de K-espais vectorials. Per definició del codiferent, la imatge d'un element $b \in \mathcal{C}(B|A)$ defineix, per restricció, una aplicació A-lineal de B en A. D'aquesta manera, obtenim una aplicació A-lineal injectiva $\mathcal{C}(B|A) \xrightarrow{\varphi} \mathrm{Hom}_A(B, A)$. D'altra banda, com que B és la clausura entera de A en L i A és íntegrament tancat, tot element de L es pot escriure en la forma b/s, on $b \in B$ i $s \in A$, $s \neq 0$. Això permet estendre de manera única tota aplicació A-lineal $B \xrightarrow{f} A$ a una aplicació K-lineal $L \xrightarrow{f} K$; l'isomorfisme $L \xrightarrow{\varphi} \mathrm{Hom}_K(L, K)$ ens proporciona un element $b \in L$ tal que $f = \mathrm{T}_{L|K}(b \cdot *)$; i aquest element b pertany a $\mathcal{C}(B|A)$ per definició del codiferent. Per tant, resulta que l'aplicació $\mathcal{C}(B|A) \xrightarrow{\varphi} \mathrm{Hom}_A(B, A)$ és un isomorfisme. En definitiva, hem provat el resultat següent.

Proposició 5.1.4. *Suposem que B és la clausura entera de A en L. Aleshores, l'aplicació*

$$\mathcal{C}(B|A) \xrightarrow{\varphi} \mathrm{Hom}_A(B, A), \qquad b \mapsto \mathrm{T}_{L|K}(b \cdot *),$$

és un isomorfisme de A-mòduls. □

Definició 5.1.5. S'anomena diferent de l'extensió $B|A$ l'ideal fraccionari invers de l'ideal codiferent; és a dir, l'ideal $(B : \mathcal{C}(B|A))$. Es designa sovint amb el símbol $\mathcal{D}(B|A)$, encara que també es fan servir els $\mathcal{D}_{B|A}$, o $\mathcal{D}(L|K)$ o $\mathcal{D}_{L|K}$ quan no hi ha perill de confusió sobre quins són els anells que es tracten.

El diferent és un ideal enter no nul de B, ja que $B \subseteq \mathcal{C}(B|A)$. En el cas que B sigui un anell de Dedekind, se satisfà la igualtat $\mathcal{C}(B|A)\mathcal{D}(B|A) = B$, i l'ideal diferent admet una factorització en ideals primers $\mathcal{D}(B|A) = \prod_{\mathfrak{P}} \mathfrak{P}^{d(\mathfrak{P})}$, on els exponents $d(\mathfrak{P})$ són enters no negatius, nuls per a tots els ideals primers no nuls de B llevat, potser, dels d'un conjunt finit. L'exponent $d(\mathfrak{P})$ s'anomena l'exponent diferencial de $\mathfrak{P}$ sobre A. Una caracterització útil del diferent (i del codiferent) és la següent.

Proposició 5.1.6. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i separable, B la clausura entera de A en L, i $\mathfrak{a} \subseteq K$, $\mathfrak{b} \subseteq L$, ideals fraccionaris no nuls. Les propietats següents són equivalents:*

$$(a)\ \mathrm{T}_{L|K}(\mathfrak{b}) \subseteq \mathfrak{a}; \quad (b)\ \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{C}(B|A); \quad (c)\ \mathfrak{b} \subseteq \mathfrak{a}\mathcal{C}(B|A); \quad (d)\ \mathcal{D}(B|A)\mathfrak{b} \subseteq \mathfrak{a}B.$$

DEMOSTRACIÓ: La propietat (a) és equivalent a la propietat $\mathfrak{a}^{-1}\mathrm{T}_{L|K}(\mathfrak{b}) \subseteq A$, que ho és a $\mathrm{T}_{L|K}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq A$, en virtut de la linealitat de la traça; però aquesta és (b) per definició de codiferent. Les altres dues s'obtenen per multiplicació. □

Igual que en el cas del discriminant, i per a anells de Dedekind, l'ideal diferent es comporta bé per localització.

Proposició 5.1.7. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i separable, B la clausura entera de A en L i S un subconjunt multiplicativament tancat de A. Aleshores,*

$$\mathcal{D}(S^{-1}B|S^{-1}A) = S^{-1}\mathcal{D}(B|A).$$

DEMOSTRACIÓ: Clarament, és suficient demostrar la propietat per als ideals codiferent i invertir. Sigui $b \in \mathcal{C}(B|A)$; aleshores, $\mathrm{T}_{L|K}(bB) \subseteq A$ i, per la K-linealitat de l'aplicació $\mathrm{T}_{L|K}$, també $\mathrm{T}_{L|K}(bS^{-1}B) \subseteq S^{-1}A$; per tant, $b \in \mathcal{C}(S^{-1}B|S^{-1}A)$ i com que $\mathcal{C}(S^{-1}B|S^{-1}A)$ és un $S^{-1}B$-submòdul de L, també $S^{-1}\mathcal{C}(B|A) \subseteq \mathcal{C}(S^{-1}B|S^{-1}A)$. Resta veure l'altra inclusió.

Sigui $b \in \mathcal{C}(S^{-1}B|S^{-1}A)$; això és dir que $\mathrm{T}_{L|K}(bS^{-1}B) \subseteq S^{-1}A$ i, per tant, que $\mathrm{T}_{L|K}(bB) \subseteq S^{-1}A$. Com que l'extensió $L|K$ és separable, A és noetherià i íntegrament tancat, i B és la clausura entera de A en L, ja sabem que B és un A-mòdul finitament generat; d'aquí es dedueix que podem elegir un element $s \in S$ tal que $\mathrm{T}_{L|K}(sbB) = s\mathrm{T}_{L|K}(bB) \subseteq A$, de manera que $sb \in \mathcal{C}(B|A)$ i, per tant, $b \in S^{-1}\mathcal{C}(B|A)$. Això acaba la prova. □

Igual que pel cas dels índexs de ramificació, els graus residuals, o les traces i les normes, una de les fórmules més útils per als diferents és la fórmula de la transitivitat sobre cadenes d'extensions.

Proposició 5.1.8. *Suposem que A és un anell de Dedekind, K el seu cos de fraccions, $K'|K$ i $L|K'$ extensions finites i separables, i A' i B les clausures enteres de A en K' i L, respectivament. Aleshores, se satisfà la igualtat d'ideals de B*

$$\mathcal{D}(B|A) = \mathcal{D}(B|A') \cdot \mathcal{D}(A'|A)B.$$

DEMOSTRACIÓ: A partir de la definició i si fem servir la transitivitat de les traces, per a tot ideal fraccionari no nul $\mathfrak{b} \subseteq L$ podem escriure la successió de propietats equivalents:

$$\begin{aligned}
\mathfrak{b} \subseteq \mathcal{C}(B|A') &\iff \mathrm{T}_{L|K'}(\mathfrak{b}) \subseteq A' \\
&\iff \mathcal{C}(A'|A)\mathrm{T}_{L|K'}(\mathfrak{b}) \subseteq \mathcal{C}(A'|A) \\
&\iff \mathrm{T}_{K'|K}(\mathcal{C}(A'|A)\mathrm{T}_{L|K'}(\mathfrak{b})) \subseteq A \\
&\iff \mathrm{T}_{K'|K}(\mathrm{T}_{L|K'}(\mathcal{C}(A'|A)\mathfrak{b})) \subseteq A \\
&\iff \mathrm{T}_{L|K}(\mathcal{C}(A'|A)\mathfrak{b}) \subseteq A \\
&\iff \mathcal{C}(A'|A)\mathfrak{b} \subseteq \mathcal{C}(B|A) \\
&\iff \mathfrak{b} \subseteq \mathcal{D}(A'|A)\mathcal{C}(B|A),
\end{aligned}$$

de manera que $\mathcal{C}(B|A') = \mathcal{D}(A'|A)\mathcal{C}(B|A)$; només resta passar els codiferents a l'altre costat de la igualtat. □

5.2 Relació entre el diferent i el discriminant

De la mateixa manera que l'ideal discriminant es pot calcular a partir de fórmules més o menys senzilles, també el diferent es pot calcular efectivament; com a mínim, en alguns casos senzills.

Definició 5.2.1. Sigui A' un domini d'integritat i sigui B la clausura entera de A' en el seu cos de fraccions. S'anomena conductor de B en A' el conjunt dels elements $b \in A'$ tals que $bB \subseteq A'$; és un ideal alhora de A' i de B; de fet, és el més gran dels ideals de A' que és un ideal de B. En particular, condició necessària i suficient perquè sigui $A' = B$ és que el conductor sigui A'.

Proposició 5.2.2. *Siguin A un domini noetherià íntegrament tancat, K el seu cos de fraccions, $L|K$ una extensió finita i separable, B la clausura entera de A en L, $b \in B$ un element primitiu de l'extensió $L|K$, $A' := A[b]$, i $f(X) := \mathrm{Irr}(b, K)(X)$ el polinomi minimal de b sobre K. Aleshores:*

(a) $f(X) \in A[X]$.

(b) *El codiferent $\mathcal{C}(A'|A)$ és l'ideal fraccionari de A' generat per* $\dfrac{1}{f'(b)}$.

(c) *Si A és un anell de Dedekind i $\mathfrak{C}(B|A')$ denota el conductor de B en A', se satisfà la igualtat d'ideals $f'(b)B = \mathfrak{C}(B|A')\mathcal{D}(B|A)$.*

Demostració: El primer apartat és immediat, ja que A és íntegrament tancat i b és enter sobre A.

Per a la segona part, observem que, donat un element qualsevol $y \in L$, podem escriure $y = g(b)$ per a un cert polinomi $g(X) \in K[X]$ de grau $\leq n-1$, ja que $\{1, b, b^2, \ldots, b^{n-1}\}$ és una K-base de L; si $b = b_1, b_2, \ldots, b_n$ són els diferents conjugats de b sobre K, aleshores podem escriure

$$g(X) = \sum_{i=1}^{n} g(b_i) \frac{f(X)}{f'(b_i)(X - b_i)}, \tag{5.2.1}$$

ja que tots dos són polinomis de grau $\leq n-1$ que prenen el mateix valor en tots els b_i; i, si definim la traça d'un polinomi coeficient a coeficient, l'expressió anterior es pot escriure en la forma

$$g(X) = \mathrm{T}_{L|K}\left(\frac{y f(X)}{f'(b)(X - b)}\right).$$

Això ens permet demostrar de seguida la inclusió $\mathcal{C}(A'|A) \subseteq f'(b)^{-1}A'$. En efecte; si $x \in \mathcal{C}(A'|A)$, per a $y := xf'(b)$ se satisfà que $g(X) \in A[X]$, ja que els polinomis $\dfrac{f(X)}{X - b}$ són de coeficients en A' i $x \in \mathcal{C}(A'|A)$; per tant, $xf'(b) = g(b) \in A'$, com volíem veure.

Per a provar l'altra inclusió és suficient demostrar que $\mathrm{T}_{L|K}(b^{n-1}/f'(b)) = 1$ i que, per a $0 \leq j \leq n-2$, se satisfan les igualtats $\mathrm{T}_{L|K}(b^j/f'(b)) = 0$, ja que aquests elements formen una A-base del A'-mòdul $f'(b)^{-1}A'$. Però si apliquem la fórmula (5.2.1) de més amunt a l'element $y := b^{j+1}$, $0 \leq j \leq n-2$, obtenim la identitat

$$X^{j+1} = \sum_{i=1}^{n} b_i^{j+1} \frac{f(X)}{f'(b_i)(X - b_i)}$$

que, en fer $X = 0$ i tenir en compte que $f(0) \neq 0$, dóna les fórmules volgudes per a $0 \leq j \leq n-2$; d'altra banda, si $y = b^n$, tenim que

$$X^n - f(X) = \sum_{i=1}^{n} b_i^n \frac{f(X)}{f'(b_i)(X - b_i)}.$$

Si fem $X = 0$ i canviem el signe, obtenim les identitats

$$f(0) = f(0) \sum_{i=1}^{n} \frac{b_i^{n-1}}{f'(b_i)} = f(0) \mathrm{T}_{L|K} \left(\frac{b^{n-1}}{f'(b)} \right),$$

de manera que, en dividir per $f(0)$, obtenim la igualtat que faltava. Això acaba la demostració de l'apartat (b).

Per a veure la darrera afirmació, observem que $\mathcal{C}(B|A) \subseteq \mathcal{C}(A'|A) \subseteq f'(b)^{-1}A'$, en virtut de (b) i de la definició del codiferent; per tant, tenim la inclusió $f'(b)\mathcal{C}(B|A) \subseteq A'$ i que $f'(b)\mathcal{C}(B|A)$ és un ideal de B, de manera que, en virtut de la definició de conductor, $f'(b)\mathcal{C}(B|A) \subseteq \mathfrak{C}(B|A')$; és a dir, la inclusió $f'(b)B \subseteq \mathfrak{C}(B|A')\mathcal{D}(B|A)$.

Resta veure l'altra inclusió. Donats elements arbitraris $x \in \mathfrak{C}(B|A')$ i $y \in B$, el producte xy és un element de A'; per tant, podem aplicar l'apartat (b) i obtenim que $\mathrm{T}(xy/f'(b)) \in A$, en virtut de la definició de codiferent. Per tant, $x/f'(b) \in \mathcal{C}(B|A)$, de manera que $x\mathcal{D}(B|A) \subseteq f'(b)B$; això acaba la prova, ja que x és arbitrari. □

Corol·lari 5.2.3. *Amb les mateixes notacions, si A és un anell de Dedekind, aleshores condició necessària i suficient perquè $\mathcal{D}(B|A) = f'(b)B$ és que sigui $B = A[b]$.* □

El resultat següent ens ensenya la relació entre el diferent i la ramificació; en particular, ens ensenya que, per a la situació que ens ocupa, el diferent és un invariant més fi que el discriminant.

Proposició 5.2.4. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i separable, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A, $d(\mathfrak{P})$ l'exponent diferencial de $\mathfrak{P}$ sobre A, i $e(\mathfrak{P}|\mathfrak{p})$ l'índex de ramificació de $\mathfrak{P}$ sobre $\mathfrak{p}$. Aleshores, $d(\mathfrak{P}) \geq e(\mathfrak{P}|\mathfrak{p}) - 1$. A més a més, perquè se satisfaci la igualtat és condició necessària i suficient que*

(a) *l'índex de ramificació $e(\mathfrak{P}|\mathfrak{p})$ no sigui divisible per la característica residual de $A/\mathfrak{p}$; i*

(b) *l'extensió residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ sigui separable.*

Demostració: Sigui $S := A - \mathfrak{p}$; la proposició **5.1.7** ens ensenya que l'exponent diferencial de $\mathfrak{P}$ coincideix amb l'exponent diferencial de l'ideal primer $S^{-1}\mathfrak{P} \subseteq S^{-1}B$ sobre la seva contracció $S^{-1}\mathfrak{p} \subseteq S^{-1}A$; però ara tenim l'avantatge que $S^{-1}A$ és local principal, que $S^{-1}B$ és principal, i que els únics ideals primers no nuls de $S^{-1}B$ són els ideals primers que contrauen a l'únic ideal primer no nul de $S^{-1}A$. A més a més, tenim igualtats $e(S^{-1}\mathfrak{P}_i|S^{-1}\mathfrak{p}) = e(\mathfrak{P}_i|\mathfrak{p})$ entre els índexs de ramificació. Per tant, podem suposar d'entrada que A és local principal; siguin π un generador d'aquest ideal, $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ els ideals primers de B que contrauen a $\mathfrak{p}$, $e_i := e(\mathfrak{P}_i|\mathfrak{p})$ els índexs de ramificació, i $d_i := d(\mathfrak{P}_i)$ els exponents diferencials. Com que el codiferent de l'extensió

$B|A$ és l'ideal fraccionari $\mathcal{C}(B|A) = \prod_{i=1}^{g} \mathfrak{P}_i^{-d_i}$, la desigualtat quedarà provada si veiem que $\prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i} \subseteq \mathcal{C}(B|A)$.

Sigui $b \in \prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i}$; aleshores, $b\pi \in \prod_{i=1}^{g} \mathfrak{P}_i$, ja que $\pi B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$; en conseqüència, per a tot índex i se satisfà la relació $b\pi \in \mathfrak{P}_i$. D'aquí podem concloure que $\mathrm{T}_{L|K}(b\pi) \in \mathfrak{p}$; en efecte, el fet que $b\pi$ sigui un element de tots els ideals primers que divideixen $\mathfrak{p}$ es manté si canviem L per la seva clausura normal sobre K, de manera que tots els conjugats de $b\pi$ també estan a tots els ideals primers que divideixen $\mathfrak{p}$; per tant, la seva traça, que és un element de A, pertany a tots els ideals primers que divideixen $\mathfrak{p}$; és a dir, per a tot índex i, se satisfà la relació $\mathrm{T}_{L|K}(b\pi) \in A \cap \mathfrak{P}_i = \mathfrak{p} = \pi A$. En conseqüència, $\pi \mathrm{T}_{L|K}(b) = \mathrm{T}_{L|K}(b\pi) \in \pi A$ o, equivalentment, $\mathrm{T}_{L|K}(b) \in A$; per tant, i com que $\prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i}$ és un B-submòdul de L, obtenim que $b \in \mathcal{C}(B|A)$, com volíem provar.

A continuació, es tracta de caracteritzar la igualtat. Per a això, suposem que se satisfan les propietats (a) i (b). Com que l'extensió residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ és separable, existeix un element $\overline{b} \in B/\mathfrak{P}$ tal que la seva traça és no nul·la en $A/\mathfrak{p}$; se tenim en compte que els ideals $\mathfrak{P}_i^{e_i}$, $i \geq 2$, són comaximals, podem prendre un representant $b \in B$ de $\overline{b}$ de manera que per a tot índex $i \geq 2$ sigui $b \in \mathfrak{P}_i^{e_i}$. La classe residual mòdul $\mathfrak{p}$ de la traça $\mathrm{T}_{L|K}(b)$ és $e_1 \mathrm{T}_{(B/\mathfrak{P})|(A/\mathfrak{p})}(\overline{b})$ (recordem que la matriu de la multiplicació per $\overline{b}$ en el quocient $B/\mathfrak{p}B \cong \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$ es pot prendre formada per caixes a la diagonal, e_i vegades la caixa de la multiplicació per la classe residual de b en $B/\mathfrak{P}_i$ per a cada índex i). L'elecció de $\overline{b}$ i la hipòtesi (a) ens permeten assegurar que aquesta classe residual és no nul·la; per tant, $\mathrm{T}_{L|K}(b) \notin \mathfrak{p} = \pi A$, de manera que $\mathrm{T}_{L|K}(b/\pi) = \pi^{-1}\mathrm{T}_{L|K}(b) \notin A$; en canvi, $b/\pi \in \mathfrak{P}_1^{-e_1}$, ja que $\pi \in \mathfrak{P}_1^{e_1}$ i $b \in B$. Això diu que $b/\pi \notin \mathcal{C}(B|A)$, de manera que hem construït un element de $\mathfrak{P}_1^{-e_1}$ que no és de $\mathcal{C}(B|A)$; dit d'una altra manera, l'exponent de $\mathfrak{P}$ en $\mathcal{C}(B|A)$ ha de ser estrictament menor que e_1; per tant, $d_1 = e_1 - 1$.

Recíprocament, cal demostrar que si alguna de les hipòtesis (a) o (b) no se satisfà, aleshores per a l'exponent de $\mathfrak{P}$ en el diferent de l'extensió se satisfà la desigualtat estricta $d_1 > e_1 - 1$. Per a això, prenem un element qualsevol b de l'ideal fraccionari $\mathfrak{P}_1^{-e_1} \prod_{i \neq 1} \mathfrak{P}_i^{1-e_i}$; aleshores, $b\pi \in \mathfrak{P}_i$ per a tot índex $i \neq 1$ i la classe residual mòdul $\mathfrak{p}$ de la traça $\mathrm{T}_{L|K}(b\pi)$ és l'element $e_1 \mathrm{T}_{(B/\mathfrak{P})|(A/\mathfrak{p})}(\overline{b}\overline{\pi})$, que és zero trivialment si e_1 és múltiple de la característica residual, i també si l'extensió residual no és separable, ja que, en aquest cas, la traça és nul·la. Per tant, $\pi \mathrm{T}_{L|K}(b) = \mathrm{T}_{L|K}(b\pi) \in \mathfrak{p} = \pi A$ i $\mathrm{T}_{L|K}(b) \in A$; per tant, i com que $\mathfrak{P}_1^{-e_1} \prod_{i \neq 1} \mathfrak{P}_i^{1-e_i}$ és un B-submòdul de L, és $b \in \mathcal{C}(B|A)$, de manera que $\mathfrak{P}_1^{-e_1} \prod_{i \neq 1} \mathfrak{P}_i^{1-e_i} \subseteq \mathcal{C}(B|A)$ i $d_1 \geq e_1$. □

Corol·lari 5.2.5. *Els ideals primers de B que ramifiquen són exactament els que divideixen el diferent $\mathcal{D}(B|A)$.* □

Es tracta de demostrar, finalment, que el discriminant és la norma del diferent i d'obtenir, en conseqüència, una fórmula de transitivitat per al discriminant.

Proposició 5.2.6. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i separable i B la clausura entera de A en L. Aleshores, $\Delta(B|A) = \mathrm{N}_{L|K}(\mathcal{D}(B|A))$.*

Demostració: Exercici. □

Corol·lari 5.2.7. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $K'|K$ i $L|K'$ extensions finites i separables, A' la clausura entera de A en K' i B la clausura entera de A (i de A') en L. Aleshores,*

$$\Delta(B|A) = \Delta(A'|A)^{[L:K']}\mathrm{N}_{K'|K}(\Delta(B|A')).$$

Demostració: Només cal prendre normes en la fórmula de transitivitat del diferent i tenir en compte la transitivitat de la norma. □

5.3 Grups de descomposició i d'inèrcia

Ja hem definit en el capítol 3 els grups de descomposició i d'inèrcia. En aquesta secció es tracta de fer-ne un estudi sistemàtic; en particular, de les seves propietats generals i de les dels cossos de descomposició i d'inèrcia, que també introduirem. Això servirà de base per a la definició i l'estudi dels grups de ramificació superior.

Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Suposem que l'extensió $L|K$ és de Galois i sigui $G := \mathrm{Gal}\,(L|K)$. Recordem que el grup de descomposició de l'ideal primer $\mathfrak{P}$ és el grup $G_{-1}(\mathfrak{P}|\mathfrak{p}) := D(\mathfrak{P}|\mathfrak{p})$ format per tots els automorfismes $\sigma \in G$ tals que $\sigma(\mathfrak{P}) = \mathfrak{P}$, i que el grup d'inèrcia de $\mathfrak{P}$ és el grup $G_0(\mathfrak{P}|\mathfrak{p}) := I(\mathfrak{P}|\mathfrak{p})$ format pels automorfismes $\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ que actuen trivialment en el quocient $B/\mathfrak{P}$; a més a més, disposem d'una successió exacta de grups

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,((B/\mathfrak{P})|(A/\mathfrak{p})) \longrightarrow 1.$$

Comencem per estudiar el comportament d'aquests grups en cadenes d'extensions de Galois.

Proposició 5.3.1. *Amb les mateixes notacions i hipòtesis anteriors, suposem que $K' \subseteq L$ és un subcòs de L que conté K i siguin A' la clausura entera de A en K' i $\mathfrak{P}' := \mathfrak{P} \cap A'$ la contracció de $\mathfrak{P}$ a A'. Aleshores, els grups de descomposició i d'inèrcia de $\mathfrak{P}$ sobre la seva contracció $\mathfrak{P}'$ s'obtenen tallant els grups sobre $\mathfrak{p}$ amb el grup de Galois $\mathrm{Gal}\,(L|K')$; és a dir, $G_i(\mathfrak{P}|\mathfrak{P}') = G_i(\mathfrak{P}|\mathfrak{p}) \cap \mathrm{Gal}\,(L|K')$, per a $i = -1, 0$.*

Demostració: És immediata a partir de les definicions. □

Si, a més a més, la subextensió $K'|K$ també és de Galois, aleshores té sentit considerar els grups $G_i(\mathfrak{P}'|\mathfrak{p})$, $i = -1, 0$.

Proposició 5.3.2. *Suposem que l'extensió $K'|K$ també és de Galois. Aleshores, hi ha un diagrama commutatiu*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_0(\mathfrak{P}|\mathfrak{P}') & \longrightarrow & G_0(\mathfrak{P}|\mathfrak{p}) & \longrightarrow & G_0(\mathfrak{P}'|\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_{-1}(\mathfrak{P}|\mathfrak{P}') & \longrightarrow & G_{-1}(\mathfrak{P}|\mathfrak{p}) & \longrightarrow & G_{-1}(\mathfrak{P}'|\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{K}'\right) & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{K}\right) & \longrightarrow & \mathrm{Gal}\left(\overline{K}'|\overline{K}\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

que té les files i les columnes exactes i on $\overline{L}$, $\overline{K}$, $\overline{K}'$, designen els cossos residuals $B/\mathfrak{P}$, $A/\mathfrak{p}$, i $A'/\mathfrak{P}'$, respectivament.

Demostració: L'exactitud de les columnes és simultània a la definició dels grups d'inèrcia (cf. la definició **3.5.5**), i l'exactitud de la tercera fila és la teoria de Galois aplicada a la cadena d'extensions residuals. D'altra banda, la comprovació de la commutativitat del diagrama és immediata. Si demostrem l'exactitud de la segona fila, la de la primera és un exercici trivial de fer quadrar diagrames. I per a veure aquesta exactitud, és suficient demostrar l'exhaustivitat del morfisme $G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}'|\mathfrak{p})$, ja que les altres parts de la demostració també són immediates a partir de la successió exacta

$$1 \longrightarrow \mathrm{Gal}\,(L|K') \longrightarrow \mathrm{Gal}\,(L|K) \longrightarrow \mathrm{Gal}\,(K'|K) \longrightarrow 1$$

que proporciona la teoria de Galois. A més a més, donat $\sigma' \in D(\mathfrak{P}'|\mathfrak{p})$, aquesta mateixa successió ens proporciona una antiimatge $\sigma \in \mathrm{Gal}\,(L|K)$ de σ'; l'element σ pot no pertànyer a $D(\mathfrak{P}|\mathfrak{p})$, però transforma $\mathfrak{P}$ en un ideal primer $\sigma(\mathfrak{P})$ de B. Com que la imatge de σ en $\mathrm{Gal}\,(K'|K)$ deixa $\mathfrak{P}'$ invariant, la restricció de $\sigma(\mathfrak{P})$ a A' també és $\mathfrak{P}'$, de manera que $\mathfrak{P}$ i $\sigma(\mathfrak{P})$ són conjugats per $\mathrm{Gal}\,(L|K')$; és a dir, existeix un element $\tau \in \mathrm{Gal}\,(L|K')$ tal que $\tau\sigma(\mathfrak{P}) = \mathfrak{P}$; en particular, obtenim que $\tau\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ i la seva imatge en $\mathrm{Gal}\,(K'|K)$ coincideix amb la imatge de σ, perquè $\tau \in \mathrm{Gal}\,(L|K')$. Per tant, hem trobat una antiimatge de σ en $G_{-1}(\mathfrak{P}|\mathfrak{p})$, com volíem. □

Observació 5.3.3. Sovint es demostra aquest resultat amb la hipòtesi addicional que l'extensió residual $\overline{L}|\overline{K}$ és separable, de manera que, aleshores, és de Galois; de fet, aquesta hipòtesi només l'hem feta servir en la demostració de la proposició quan hem parlat de l'exactitud de la tercera fila del diagrama. Ara bé, aquesta successió és exacta sense necessitat de la hipòtesi de separabilitat. Per a veure aquest fet, observem el fets següents: en primer lloc, per a la definició de la successió només cal que l'extensió $\overline{K}'|\overline{K}$ sigui normal; en segon lloc, l'exhaustivitat del segon morfisme només utilitza la normalitat de l'extensió $\overline{L}|\overline{K}$, quan assegurem que una $\overline{K}$-immersió de $\overline{L}$ que estengui un $\overline{K}$-automorfisme donat de $\overline{K}'$ és automàticament un $\overline{K}$-automorfisme de $\overline{L}$; i, finalment, el nucli d'aquest morfisme és exactament el grup de Galois $\mathrm{Gal}\left(\overline{L}|\overline{K}'\right)$, sense necessitat de cap propietat de normalitat ni de separabilitat.

5.4 Cossos de descomposició i d'inèrcia

Mantinguem les notacions i les hipòtesis de la secció anterior. Escriurem D, I, per designar els grups de descomposició i d'inèrcia, respectivament, de l'ideal $\mathfrak{P}$ sobre la seva contracció.

Definició 5.4.1. Els cossos fixos de L pels subgrups $D := G_{-1}(\mathfrak{P}|\mathfrak{p})$, $I := G_0(\mathfrak{P}|\mathfrak{p})$, L^D, L^I, s'anomenen, respectivament, el cos de descomposició i el cos d'inèrcia en $\mathfrak{P}$.

Així, tenim una successió de cossos $K \subseteq L^D \subseteq L^I \subseteq L$ tal que les extensions $L|L^I$, $L|L^D$, i $L^I|L^D$ són extensions de Galois amb grups respectius $\mathrm{Gal}\left(L|L^I\right) = I$, $\mathrm{Gal}\left(L|L^D\right) = D$, i $\mathrm{Gal}\left(L^I|L^D\right) \cong \mathrm{Gal}\left(\overline{L}|\overline{K}\right)$, el grup de Galois de l'extensió residual. En particular, obtenim els graus de les extensions: d'una banda, si posem $e := e(\mathfrak{P}|\mathfrak{p})$ i $f := f(\mathfrak{P}|\mathfrak{p})$, aleshores $[L : L^D] = ef = n/g$, ja que $g := g(\mathfrak{p})$ és l'índex del grup d'isotropia de l'acció de $\mathrm{Gal}\,(L/K)$ en el conjunt dels ideals primers de B que divideixen $\mathfrak{p}$; és a dir, l'índex del grup de descomposició D; en conseqüència, $[L^D : K] = g$. D'altra banda, el grau $[L^I : L^D]$ és el grau de separabilitat de l'extensió residual $\overline{L}/\overline{K}$, ja que és una extensió normal i, per tant, l'ordre del seu grup de Galois és el grau de separabilitat; en particular, si l'extensió residual $\overline{L}/\overline{K}$ és de característica $p > 0$, i escrivim el grau de separabilitat en la forma $f_s = f_s(\mathfrak{P}/\mathfrak{p})$, obtenim que el quocient f/f_s és una certa potència p^i de p: el grau d'inseparabilitat; amb aquestes notacions, podem escriure els graus $[L^I : L^D] = f_s$, i, en conseqüència, $[L : L^I] = ep^i$. Aquests graus fan pensar en si el primer $\mathfrak{P}$ serà totalment ramificat en l'extensió $L|L^I$, i si la contracció de $\mathfrak{P}$ al cos L^D és un ideal primer que no descompon en l'extensió $L|L^D$. Això és, efectivament, d'aquesta manera.

Proposició 5.4.2. *Siguin $\mathfrak{P}_I$ i $\mathfrak{P}_D$ les contraccions de $\mathfrak{P}$ a les clausures enteres B_I, B_D, de A en L^I, L^D, respectivament. Aleshores:*

(a) *$\mathfrak{P}$ és l'unic ideal primer de B que divideix $\mathfrak{P}_I$ i $\mathfrak{P}_D$;*

(b) *l'extensió de $\mathfrak{P}_I$ a B és l'ideal $\mathfrak{P}^e$, on $e := e(\mathfrak{P}|\mathfrak{p})$ és l'índex de ramificació de $\mathfrak{P}$ sobre $\mathfrak{p}$, i el grau residual $f(\mathfrak{P}|\mathfrak{P}_I)$ és el grau d'inseparabilitat, p^i, de l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$; i*

(c) *l'extensió de $\mathfrak{P}_D$ a B_I és l'ideal $\mathfrak{P}_I$, i el grau residual $f(\mathfrak{P}_I|\mathfrak{P}_D)$ és el grau de separabilitat, f_s, de l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$.*

Demostració: El grup de descomposició $D(\mathfrak{P}|\mathfrak{P}_D)$ coincideix amb el grup $D(\mathfrak{P}|\mathfrak{p})$ perquè l'extensió $L|L^D$ és de Galois de grup de Galois $D(\mathfrak{P}|\mathfrak{p})$; per tant, la primera afirmació és immediata. En particular, les altres dues propietats són equivalents. Si ara apliquem les dues proposicions anteriors al càlcul dels grups de descomposició i d'inèrcia del primer $\mathfrak{P}_I$ en l'extensió de Galois $L^I|L^D$, podem mirar el diagrama commutatiu de més avall i obtenim immediatament les igualtats:

$$\begin{aligned} D(\mathfrak{P}|\mathfrak{P}_D) = D(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^D\right), \\ I(\mathfrak{P}|\mathfrak{P}_D) = I(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^I\right), \\ D(\mathfrak{P}|\mathfrak{P}_I) = I(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^I\right), \\ I(\mathfrak{P}|\mathfrak{P}_I) = I(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^I\right), \end{aligned}$$

de manera que el grup d'inèrcia $I(\mathfrak{P}_I|\mathfrak{P}_D)$ és trivial i el grup de Galois de l'extensió residual $(B_I/\mathfrak{P}_I)|(B_D/\mathfrak{P}_D)$ és isomorf al grup de Galois $\mathrm{Gal}\left(L^I|L^D\right)$; en particular, el grau residual $f(\mathfrak{P}_I|\mathfrak{P}_D)$ coincideix amb el grau de l'extensió; és a dir, aquest grau és f_s i $\mathfrak{P}_I$ és no ramificat sobre $\mathfrak{P}_D$. D'aquí es dedueix immediatament la validesa de les propietats (b) i (c).

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I(\mathfrak{P}|\mathfrak{P}_I) & \longrightarrow & I(\mathfrak{P}|\mathfrak{P}_D) & \longrightarrow & I(\mathfrak{P}_I|\mathfrak{P}_D) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & D(\mathfrak{P}|\mathfrak{P}_I) & \longrightarrow & D(\mathfrak{P}|\mathfrak{P}_D) & \longrightarrow & D(\mathfrak{P}_I|\mathfrak{P}_D) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{L}^I\right) & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{L}^D\right) & \longrightarrow & \mathrm{Gal}\left(\overline{L}^I|\overline{L}^D\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

□

Observació 5.4.3. En general, el grup de descomposició no és un subgrup normal del grup de Galois; però si ho és, la descomposició de $\mathfrak{p}$ en B_D és donada per la fórmula

$$\mathfrak{p}B_D = \mathfrak{P}_{D,1} \cdots \mathfrak{P}_{D,g},$$

on $\mathfrak{P}_{D,i}$, són ideals primers diferents de B_D de grau residual $f(\mathfrak{P}_{D,i}|\mathfrak{p}) = 1$ i $g = g(\mathfrak{p})$ és el nombre d'ideals primers de B que divideixen $\mathfrak{p}$.

Demostració: En aquest cas, l'extensió $L^D|K$ és de Galois i, per tant, tots els ideals primers de B_D que divideixen $\mathfrak{p}$ tenen el mateix índex de ramificació i el mateix grau residual; però si ens fixem en l'ideal de B_D contracció de $\mathfrak{P}$, obtenim que l'índex de ramificació i el grau residual de $\mathfrak{P}$ sobre $\mathfrak{p}$ són els de $\mathfrak{P}$ sobre la seva contracció $\mathfrak{P} \cap B_D$; per tant, l'índex de ramificació i el grau residual de $\mathfrak{P} \cap B_D$ sobre $\mathfrak{p}$ són tots dos trivials, és a dir, iguals a 1, i el nombre d'ideals primers de B que divideixen $\mathfrak{P} \cap B_D$ també és 1, de manera que el nombre d'ideals primers de B_D que divideixen $\mathfrak{p}$ coincideix amb el nombre d'ideals primers de B que divideixen $\mathfrak{p}$. □

Podem resumir aquests fets en el resultat següent.

Corol·lari 5.4.4. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Suposem que l'extensió $L|K$ és de Galois i siguin $D := G_{-1}(\mathfrak{P}|\mathfrak{p})$, $I := G_0(\mathfrak{P}|\mathfrak{p})$, els grups de descomposició i d'inèrcia de $\mathfrak{P}$ sobre $\mathfrak{p}$. Aleshores, l'extensió $L|K$ "trenca" en una extensió $L|L^I$ que és totalment ramificada en $\mathfrak{P}$ de manera que $L^I|K$ és no ramificada en $\mathfrak{P}_I := \mathfrak{P} \cap B_I$. A més a més, l'extensió $L^I|K$ també "trenca" en una extensió $L^I|L^D$ que és no ramificada en $\mathfrak{P}_I$ i tal que $\mathfrak{P}_D := \mathfrak{P}_I \cap B_D$ no descompon en B_I. Si l'extensió $L^D|K$ és de Galois (és a dir, si el grup de descomposició és normal en $\mathrm{Gal}\,(L|K)$), aleshores, el primer $\mathfrak{p}$ descompon completament en l'extensió $L^D|K$.* □

5.5 Automorfisme de Frobenius

L'estudi de les extensions de Galois finites de cossos de nombres que són no ramificades en un ideal primer duu de manera natural a la introducció de l'automorfisme de Frobenius. Aquesta secció es dedica a la seva introducció i a l'estudi de les seves propietats.

Efectivament, en el cas dels cossos de nombres, els cossos residuals de les extensions són cossos finits; per tant, són extensions cícliques i, en particular, separables. Més generalment, siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i de Galois, $G := \mathrm{Gal}\,(L|K)$ el seu grup de Galois, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul, i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A, i suposem que l'extensió $B|A$ és no ramificada en $\mathfrak{P}$ i que el cos residual $A/\mathfrak{p}$ és un cos finit de q elements i característica p.

En aquestes condicions, el grup d'inèrcia $G_0(\mathfrak{P}|\mathfrak{p})$ és trivial i el grup de descomposició $G_{-1}(\mathfrak{P}|\mathfrak{p})$ és isomorf de manera natural al grup de Galois de l'extensió residual; per tant, $G_{-1}(\mathfrak{P}|\mathfrak{p})$ és un grup cíclic d'ordre $f := f(\mathfrak{P}|\mathfrak{p})$. Podem considerar, doncs, l'automorfisme $F_{\mathfrak{P}} \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ que pensat en el grup de Galois de l'extensió residual sigui l'automorfisme de Frobenius; això és dir que $F_{\mathfrak{P}}$ és definit unívocament per la condició

$$F_{\mathfrak{P}}(b) - b^q \in \mathfrak{P}$$

per a tot element $b \in B$.

Definició 5.5.1. L'automorfisme $F_{\mathfrak{P}} \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ s'anomena l'automorfisme de Frobenius associat a $\mathfrak{P}$; és un generador del grup de descomposició $G_{-1}(\mathfrak{P}|\mathfrak{p})$ i és d'ordre $f(\mathfrak{P}|\mathfrak{p})$. S'acostuma a designar per $(\mathfrak{P}, B|A)$ o per $\left(\dfrac{B|A}{\mathfrak{P}}\right)$; quan no hi ha dubte dels anells, també se sol escriure $(\mathfrak{P}, L|K)$ i $\left(\dfrac{L|K}{\mathfrak{P}}\right)$.

Observem que si $\mathfrak{P}$ és no ramificat sobre $\mathfrak{p}$, aleshores $\sigma(\mathfrak{P})$ també és no ramificat sobre $\mathfrak{p}$ per a tot element $\sigma \in \mathrm{Gal}\,(L|K)$; com que l'extensió $L|K$ és de Galois, això significa que l'automorfisme de Frobenius està definit per a tot ideal primer de B que divideix $\mathfrak{p}$.

Proposició 5.5.2. *Suposem que $B|A$ és no ramificada en $\mathfrak{P}$, sigui $\mathfrak{P}' \subseteq B$ un altre ideal primer no nul de B que divideixi $\mathfrak{p}$ i sigui $\sigma \in \mathrm{Gal}\,(L|K)$ un automorfisme qualsevol tal que $\mathfrak{P}' = \sigma(\mathfrak{P})$. Aleshores, se satisfà la igualtat*

$$\left(\frac{B|A}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{B|A}{\mathfrak{P}}\right)\sigma^{-1}$$

en el grup de Galois $\mathrm{Gal}\,(L|K)$.

Demostració: En efecte, ja sabem que els grups de descomposició són conjugats, ja que són els grups d'isotropia de l'acció del grup de Galois sobre el conjunt dels ideals primers de B que divideixen $\mathfrak{p}$. Ara, la demostració és una simple comprovació: els elements $\left(\dfrac{B|A}{\sigma(\mathfrak{P})}\right)$ i $\sigma\left(\dfrac{B|A}{\mathfrak{P}}\right)\sigma^{-1}$ estan tots dos en el grup de descomposició $G_{-1}(\sigma(\mathfrak{P})|\mathfrak{p})$ i satisfan la condició de congruència; per la unicitat de l'automorfisme de Frobenius, coincideixen. □

Seguidament, es tracta de fer l'estudi del comportament de l'automorfisme de Frobenius per a cadenes d'extensions de Galois no ramificades.

Proposició 5.5.3. *Siguin K' un subcòs de L que conté K, A' la clausura entera de A en K', i $\mathfrak{P}' := \mathfrak{P} \cap A'$ la contracció de $\mathfrak{P}$ a A'. L'extensió $L|K'$ és una extensió de Galois i també és no ramificada en $\mathfrak{P}$. Aleshores, l'automorfisme de Frobenius $\left(\frac{B|A'}{\mathfrak{P}}\right)$ és la potència f'-èsima de l'automorfisme de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$, on f' és el grau residual $f' := f(\mathfrak{P}'|\mathfrak{p})$. Si, a més a més, l'extensió $K'|K$ és de Galois, aleshores l'extensió $A'|A$ és no ramificada en $\mathfrak{P}'$ i l'automorfisme de Frobenius $\left(\frac{K'|K}{\mathfrak{P}'}\right)$ és la restricció a $\mathrm{Gal}\,(K'|K)$ de l'automorfisme de Frobenius $\left(\frac{L|K}{\mathfrak{P}}\right)$.*

Demostració: Tots els automorfismes que intervenen en l'enunciat estan definits i només cal comprovar que se satisfan les congruències que defineixen els automorfismes de Frobenius. I per a això, només cal tenir en compte quins són els cossos residuals (finits). □

Observació 5.5.4. Suposem, ara, que tenim dues extensions de Galois $L_i|K$ tals que el cos L és el cos composició dels L_i; siguin $\mathfrak{P}_i := \mathfrak{P} \cap B_i$, les restriccions de $\mathfrak{P}$ a la clausura entera B_i de A en L_i, $i = 1, 2$. Aleshores, les extensions $B_i|A$ són no ramificades en $\mathfrak{P}_i$ i els automorfismes de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$ $\left(\frac{B_i|A}{\mathfrak{P}_i}\right)$ estan definits. D'altra banda, com que el grup de Galois de l'extensió $L|K$ s'injecta, per restricció en cada component, en el producte cartesià dels grups de Galois $\mathrm{Gal}\,(L_i|K)$, podem identificar $\mathrm{Gal}\,(L|K)$ amb un subgrup de $\mathrm{Gal}\,(L_1|K) \times \mathrm{Gal}\,(L_2|K)$. Amb aquesta identificació, l'automorfisme de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$ és la parella $\left(\left(\frac{B_i|A}{\mathfrak{P}_i}\right), \left(\frac{B_i|A}{\mathfrak{P}_i}\right)\right)$.

L'automorfisme de Frobenius dóna una caracterització molt senzilla dels ideals primers de l'anell base que descomponen completament. Recordem que es diu que un ideal primer $\mathfrak{p} \subseteq A$ descompon completament en un cos L extensió de K quan l'extensió de $\mathfrak{p}$ a la clausura entera de A en L és el producte de tants ideals primers diferents com el grau $[L : K]$ de l'extensió.

Corol·lari 5.5.5. *Suposem que l'extensió $L|K$ és de Galois i no ramificada en $\mathfrak{p}$. Condició necessària i suficient perquè $\mathfrak{p}$ descompongui completament en B és que per a qualsevol ideal primer $\mathfrak{P} \subseteq B$ que divideixi $\mathfrak{p}$ en B, l'automorfisme de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$ sigui trivial.*

Demostració: En efecte, l'automorfisme de Frobenius és un generador del grup de descomposició i condició necessària i suficient perquè aquest grup sigui trivial és que l'índex de ramificació i el grau residual de qualsevol ideal primer $\mathfrak{p}$ siguin tots dos iguals a 1. Aquesta condició, però, és equivalent a dir que l'ideal primer $\mathfrak{p}$ descompon completament. □

Corol·lari 5.5.6. *Suposem que el cos L és el cos composició de dos subcossos $L_i \subseteq L$, $i = 1, 2$, que contenen K, com a l'observació anterior. Aleshores, condició necessària i suficient perquè $\mathfrak{p}$ descompongui completament en L és que descompongui completament en cada una de les extensions $L_i|K$.*

Observació 5.5.7. En el cas que l'extensió $L|K$ sigui abeliana, l'automorfisme de Frobenius $\left(\frac{L|K}{\mathfrak{P}}\right)$ no depèn de l'ideal primer $\mathfrak{P}$ de B que divideix $\mathfrak{p}$; en aquest cas, s'acostuma a designar per $\left(\frac{L|K}{\mathfrak{p}}\right)$ i s'anomena l'automorfisme de Frobenius de $\mathfrak{p}$.

5.6 Grups de ramificació superior

L'eina bàsica de la demostració que farem del teorema de Kronecker-Weber és el concepte i les propietats dels grups de ramificació superior. Aquests grups són una generalització natural del grup d'inèrcia, del qual són subgrups i n'hereten algunes propietats.

Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i de Galois, $G := \mathrm{Gal}\,(L|K)$ el grup de Galois, i B la clausura entera de A en L. Recordem que G actua de manera natural en B i que actua transitivament en el conjunt dels ideals primers $\mathfrak{P} \subseteq B$ que divideixen un ideal primer donat $\mathfrak{p} \subseteq A$. A més a més, hem definit el grup de descomposició $G_{-1}(\mathfrak{P}|\mathfrak{p})$ d'un ideal primer fix $\mathfrak{P} \subseteq B$ sobre la seva contracció $\mathfrak{p} := \mathfrak{P} \cap A$, com el subgrup de G format pels elements $\sigma \in G$ que deixen $\mathfrak{P}$ invariant; és a dir, pels elements $\sigma \in G$ que actuen en l'anell quocient $B/\mathfrak{P}$; anàlogament, hem definit el grup d'inèrcia $G_0(\mathfrak{P}|\mathfrak{p})$ com el conjunt dels elements $\sigma \in G$ que actuen en l'anell quocient $B/\mathfrak{P}$ com la identitat; equivalentment, els elements $\sigma \in G_{-1}$ tals que per a tot element $b \in B$ se satisfà que $\sigma(b) - b \in \mathfrak{P}$.

Definició 5.6.1. Sigui $k \geq -1$ un nombre enter. El conjunt

$$G_k(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p}) : \sigma(b) - b \in \mathfrak{P}^{k+1}, \text{ per a tot } b \in B\},$$

format pels elements $\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ que actuen trivialment en l'anell quocient $B/\mathfrak{P}^{k+1}$, és un subgrup normal de $G_{-1}(\mathfrak{P}|\mathfrak{p})$; s'anomena el k-èsim grup de ramificació de $\mathfrak{P}$ sobre $\mathfrak{p}$. En efecte, és el nucli del morfisme natural de grups

$$G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Aut}(B/\mathfrak{P}^{k+1}).$$

Per comoditat de notació, escriurem G_k en lloc de $G_k(\mathfrak{P}|\mathfrak{p})$.

Observació 5.6.2. Notem que el subíndex k associat al grup és una unitat inferior a l'exponent de $\mathfrak{P}$ que utilitzem en l'anell quocient $B/\mathfrak{P}^{k+1}$ sobre el qual demanem que l'acció sigui trivial. D'altra banda, la definició coincideix amb la donada prèviament per als grups de descomposició i d'inèrcia i generalitza aquesta darrera. A més a més, per a tot $k \geq -1$, el grup G_{k+1} és un subgrup de G_k, de manera que disposem d'una successió de subgrups de G_{-1}

$$G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k \supseteq G_{k+1} \supseteq \ldots$$

Com que l'anell B és noetherià, se satisfà la propietat $\bigcap_{k \geq -1} \mathfrak{P}^k = (0)$, de manera que, com que G_{-1} és finit, existeix $n_0 \in \mathbb{Z}$ tal que per a $k \geq n_0$ és $G_k = (1)$. Per tant, els subgrups G_k formen una cadena normal de G_{-1}.

Dels grups de ramificació ens interessen els quocients G_k/G_{k+1}, que podem formar en virtut de la definició. Ja sabem que el grup quocient G_{-1}/G_0 és isomorf al grup de Galois de l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$. Per a estudiar l'estructura dels quocients per a $k \geq 0$, comencem per establir el resultat següent.

Proposició 5.6.3. *Per a tot nombre enter $k \geq 1$, el grup quocient G_k/G_{k+1} és abelià.*

DEMOSTRACIÓ: La demostració és una conseqüència elemental de l'estudi dels commutadors $[\sigma, \tau] := \sigma\tau\sigma^{-1}\tau^{-1}$, per a $\sigma \in G_k$, $\tau \in G_n$, $k, n \geq 0$. Se satisfà el resultat següent.

Lema 5.6.4. *Amb les notacions anteriors, $[\sigma, \tau] \in G_{k+n}$.*

DEMOSTRACIÓ: Comencem per veure que per a tot $b \in \mathfrak{P}^{n+1}$ és $\sigma b - b \in \mathfrak{P}^{k+n+1}$. Per a això, és suficient considerar elements b de la forma $b := b_1 \cdot b_2 \cdots b_{n+1}$ tals que $b_j \in \mathfrak{P}$, ja que aquests elements generen $\mathfrak{P}^{n+1}$ com a grup abelià additiu. Podem escriure la identitat

$$\sigma(b) - b = \sum_{j=1}^{n+1} \sigma(b_1) \cdots \sigma(b_{j-1})(\sigma(b_j) - b_j) b_{j+1} \cdots b_{n+1},$$

que mostra que l'element $\sigma(b) - b$ pertany a $\mathfrak{P}^{k+n+1}$, ja que $\sigma(b_j) - b_j \in \mathfrak{P}^{k+1}$ perquè $b_j \in B$ i $\sigma \in G_k$. Anàlogament, per a tot $c \in \mathfrak{P}^{k+1}$ és $\tau(c) - c \in \mathfrak{P}^{k+n+1}$.

Prenem, ara, un element qualsevol $x \in B$ i posem $y := \sigma^{-1}\tau^{-1}(x)$, $b := \tau(y) - y$, i $c := \sigma(y) - y$. Per l'elecció de σ i τ, se satisfan les propietats $b \in \mathfrak{P}^{n+1}$, $c \in \mathfrak{P}^{k+1}$, de manera que $\sigma(b) - b, \tau(c) - c \in \mathfrak{P}^{k+n+1}$; en restar, obtenim que

$$\begin{aligned} \sigma(b) - b - \tau(c) + c &= \sigma(\tau(y) - y) - (\tau(y) - y) - \tau(\sigma(y) - y) + (\sigma(y) - y) \\ &= \sigma\tau(y) - \tau\sigma(y) \in \mathfrak{P}^{k+n+1}; \end{aligned}$$

és a dir, $[\sigma, \tau](x) - x \in \mathfrak{P}^{k+n+1}$. Per tant, $[\sigma, \tau] \in G_{k+n}$. □

Ara podem acabar fàcilment la prova de la proposició; només cal prendre $n = k$ i obtenim que $[\sigma, \tau] \in G_{2k}$; com que $k \geq 1$, és $2k \geq k + 1$ i el grup quocient G_k/G_{k+1} és abelià. □

El resultat que proporciona aquesta proposició no és tan general com és possible. En el cas dels cossos de nombres, però, els cossos residuals són finits i, en conseqüència, les extensions residuals són separables. A causa d'aquest fet, i que només tractarem el cas dels cossos de nombres, ens situarem en la hipòtesi restrictiva que l'extensió residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ sigui separable. En aquest cas, podem demostrar el resultat següent, que no és vàlid en general.

Proposició 5.6.5. *Suposem que l'extensió residual en $\mathfrak{P}$ és separable. Aleshores:*

(a) *El quocient G_0/G_1 és isomorf a un subgrup (finit) del grup multiplicatiu $(B/\mathfrak{P})^*$; en particular, és cíclic d'ordre primer amb la característica residual (si aquesta és positiva).*

(b) *Per a $k \geq 1$, els quocients G_k/G_{k+1} són isomorfs a subgrups (finits) del grup additiu del cos residual $B/\mathfrak{P}$; en particular, si $B/\mathfrak{P}$ és un cos de característica $p > 0$, els quocients són p-grups abelians elementals; i si la característica residual és 0, els quocients són trivials i $G_1 = (0)$.*

DEMOSTRACIÓ: Si localitzem en $S := A - \mathfrak{p}$, ni els grups de ramificació ni els cossos residuals no canvien, de manera que podem suposar que A i B són anells principals. Sigui $\pi \in \mathfrak{P}$ un generador de l'ideal $\mathfrak{P}$. Anem a definir morfismes de grups abelians

$G_0 \longrightarrow (B/\mathfrak{P})^*$ i $G_k \longrightarrow B/\mathfrak{P}$. Donat $\sigma \in G_0$, l'element $\sigma(\pi)$ també pertany a $\mathfrak{P}$, ja que σ deixa invariant $\mathfrak{P}$; però no pot ser que $\sigma(\pi) \in \mathfrak{P}^2$ ja que, en aplicar σ^{-1}, també seria $\pi \in \mathfrak{P}^2$; per tant, existeix $u_\sigma \in B$, $u_\sigma \notin \mathfrak{P}$, tal que $\sigma(\pi) = u_\sigma\pi$. Aquest element està unívocament determinat per σ, per exemple, per ser B un domini d'integritat. Si ara prenem $\tau \in G_0$, la igualtat $\sigma(\pi) = u_\sigma\pi$ es transforma en $u_{\tau\sigma}\pi = \tau\sigma(\pi) = \tau(u_\sigma)u_\tau\pi$, de manera que $u_{\tau\sigma} = \tau(u_\sigma)u_\tau$. Si reduïm mòdul $\mathfrak{P}$, com que $\tau \in G_0$, és $\tau(u_\sigma) \equiv u_\sigma \pmod{\mathfrak{P}}$, i, per tant, $u_{\tau\sigma} \equiv u_\sigma u_\tau \pmod{\mathfrak{P}}$. D'aquesta manera definim una aplicació multiplicativa $G_0 \longrightarrow B/\mathfrak{P}$; com que $u_\sigma \in B$ i $u_\sigma \notin \mathfrak{P}$, la imatge està inclosa en $(B/\mathfrak{P})^*$, de manera que s'obté un morfisme de grups. El nucli d'aquest morfisme està format pels elements $\sigma \in G_0$ tals que $u_\sigma \equiv 1 \pmod{\mathfrak{P}}$; és a dir, tals que $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$. Ara bé, dir que $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$ equival a dir que per a tot element $b \in B$ és $\sigma(b) \equiv b \pmod{\mathfrak{P}^2}$. En efecte, en el cas separable, el cos residual en $\mathfrak{P}$ coincideix amb el cos residual de B_I en $\mathfrak{P}_I := \mathfrak{P} \cap B_I$, i, per tant, podem escriure b en la forma $b = c + d$, per a alguns elements $c \in B_I$ i $d \in \mathfrak{P}$; com que $c \in B_I$ i $\sigma \in G_0$, és $\sigma(c) = c$, de manera que només cal veure que $\sigma(d) \equiv d \pmod{\mathfrak{P}^2}$. Però si escrivim $d = a\pi$, $a \in B$, aleshores, $\sigma(d) - d = \sigma(a\pi) - a\pi = \sigma(a)(\sigma(\pi) - \pi) + \pi(\sigma(a) - a) \in \mathfrak{P}^2$, ja que $\sigma(\pi) - \pi \in \mathfrak{P}^2$, $\sigma(a) \in B$, i $\sigma(a) - a \in \mathfrak{P}$ per ser $\sigma \in G_0$. Dit d'una altra manera, el nucli del morfisme $G_0 \longrightarrow (B/\mathfrak{P})^*$ és exactament G_1. Això demostra la primera part.

La segona part es demostra anàlogament. Donat $\sigma \in G_k$, $k \geq 1$, $\sigma(\pi) - \pi \in \mathfrak{P}^{k+1}$, de manera que existeix $u_\sigma \in B$, unívocament determinat per σ, tal que $\sigma(\pi) - \pi = u_\sigma\pi^{k+1}$. Si ara prenem $\tau \in G_k$, la igualtat $\sigma(\pi) - \pi = u_\sigma\pi^{k+1}$ es transforma en

$$\begin{aligned} u_{\tau\sigma}\pi^{k+1} &= \tau\sigma(\pi) - \pi \\ &= \tau(\sigma(\pi) - \pi) + (\tau(\pi) - \pi) \\ &= \tau(u_\sigma\pi^{k+1}) + u_\tau\pi^{k+1} \\ &= \tau(u_\sigma)\tau(\pi)^{k+1} + u_\tau\pi^{k+1} \\ &= \tau(u_\sigma)(\pi + u_\tau\pi^{k+1})^{k+1} + u_\tau\pi^{k+1} \\ &= \pi^{k+1}(\tau(u_\sigma)(1 + u_\tau\pi^k)^{k+1} + u_\tau); \end{aligned}$$

si dividim per π^{k+1}, obtenim que $u_{\tau\sigma} \equiv \tau(u_\sigma) + u_\tau \pmod{\mathfrak{P}}$, ja que $k \geq 1$; i com que $\tau(u_\sigma) \equiv u_\sigma \pmod{\mathfrak{P}}$, perquè $\tau \in G_0$, obtenim que $u_{\tau\sigma} \equiv u_\sigma + u_\tau \pmod{\mathfrak{P}}$. Si reduïm mòdul $\mathfrak{P}$, obtenim un morfisme additiu de grups $G_k \longrightarrow B/\mathfrak{P}$. El nucli d'aquest morfisme està format pels elements $\sigma \in G_k$ tals que $u_\sigma \equiv 0 \pmod{\mathfrak{P}}$; és a dir, tals que $\sigma(\pi) - \pi \in \mathfrak{P}^{k+2}$. Ara bé, dir que $\sigma(\pi) - \pi \in \mathfrak{P}^{k+2}$ equival a dir que per a tot element $b \in B$ és $\sigma(b) - b \in \mathfrak{P}^{k+2}$. En efecte; com abans, podem escriure b en la forma $b = c + d$, per a alguns elements $c \in B_I$ i $d \in \mathfrak{P}$; com que $c \in B_I$ i $\sigma \in G_k \subseteq G_0$, és $\sigma(c) = c$, de manera que només cal veure que $\sigma(d) - d \in \mathfrak{P}^{k+2}$. Però si escrivim $d = a\pi$, $a \in B$, aleshores, $\sigma(d) - d = \sigma(a\pi) - a\pi = \sigma(a)(\sigma(\pi) - \pi) + \pi(\sigma(a) - a) \in \mathfrak{P}^{k+2}$, ja que $\sigma(\pi) - \pi \in \mathfrak{P}^{k+2}$, per hipòtesi, $\sigma(a) \in B$, i $\sigma(a) - a \in \mathfrak{P}^{k+1}$ per ser $\sigma \in G_k$. Dit d'una altra manera, el nucli del morfisme $G_k \longrightarrow B/\mathfrak{P}$ és exactament G_{k+1}, com es volia demostrar. □

Corol·lari 5.6.6. *Suposem que el cos residual és de característica positiva p; aleshores, G_1 és un p-grup abelià i el quocient G_0/G_1 és un grup abelià d'ordre no divisible per p.* □

Definició 5.6.7. Es diu que una extensió $B|A$ d'anells de Dedekind és moderadament ramificada en un ideal primer no nul $\mathfrak{P} \subseteq B$, o que $\mathfrak{P}$ és moderadament ramificat sobre $\mathfrak{p}$, quan l'extensió residual en $\mathfrak{P}$ és separable i, a més a més, l'índex de ramificació $e(\mathfrak{P}|\mathfrak{p})$ no és divisible per la característica residual en $\mathfrak{P}$; en cas contrari, l'extensió s'anomena

salvatgement ramificada, i es diu que el primer $\mathfrak{P}$ és salvatgement ramificat sobre $\mathfrak{p}$. En el cas Galoisià, dir moderadament ramificada en $\mathfrak{P}$ equival a dir que el grup de ramificació $G_1(\mathfrak{P}|\mathfrak{p})$ és trivial.

Corol·lari 5.6.8. *Suposem que els cossos residuals són finits. Aleshores, el grup de descomposició és un grup resoluble.*

Demostració: En efecte, acabem de provar que si l'extensió residual és separable, aleshores el grup d'inèrcia és resoluble, ja que la cadena dels grups de ramificació G_k, $k \geq 0$, és abeliana; d'altra banda, si l'extensió residual és resoluble, com que el grup quocient G_{-1}/G_0 és isomorf al grup de Galois de l'extensió residual, la cadena G_k, $k \geq -1$, és abeliana; i aquest és el cas si els cossos residuals són finits. □

5.7 El grup d'inèrcia moderada

En el cas d'extensions de Galois de cossos de nombres o, més generalment, en què l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$ és separable, podem considerar el cos L^{G_1} fix pel grup G_1; aleshores, l'extensió totalment ramificada en $\mathfrak{P}$, $L|L^I$, "trenca" en una extensió moderadament ramificada $L^{G_1}|L^I$ i una extensió, $L|L^{G_1}$, totalment ramificada de grau potència de la característica residual. En particular, la ramificació total encara es pot estudiar per etapes: una moderadament ramificada i una salvatgement ramificada.

Definició 5.7.1. El grup G_0/G_1 s'anomena el grup d'inèrcia moderada en $\mathfrak{P}$; és un grup d'ordre la part lliure de p de l'índex de ramificació $e(\mathfrak{P}|\mathfrak{p})$, on p denota la característica residual.

Per a un ús posterior, convé establir el resultat següent.

Proposició 5.7.2. *Suposem que el cos residual $A/\mathfrak{p}$ és de cardinal finit q i de característica positiva p. El grup d'inèrcia moderada de l'extensió $B|A$ en $\mathfrak{P}$, G_0/G_1, és un grup cíclic d'ordre divisor de $q^f - 1$, on $f := f(\mathfrak{P}|\mathfrak{p})$ denota el grau residual en $\mathfrak{P}$ de l'extensió. Si suposem que el grup G_{-1}/G_1 és abelià, aleshores, l'ordre de G_0/G_1 és divisor de $q - 1$.*

Demostració: La primera part és immediata, ja que el quocient G_0/G_1 s'identifica a un subgrup del grup multiplicatiu $(B/\mathfrak{P})^*$; veiem la segona.

Igual que a la demostració de la proposició de més amunt, podem suposar que A és local i, per tant, que $\mathfrak{P}$ és un ideal principal; sigui, doncs, $\pi \in \mathfrak{P}$ un generador de $\mathfrak{P}$. Observem que si $\sigma \in G_{-1}$, aleshores $\sigma(\pi) = u_\sigma \pi$ per a un cert element enter $u_\sigma \in B$; en particular, ja hem vist que si $\sigma \in G_0$, aleshores $u_\sigma \notin \mathfrak{P}$ i l'assignació de la classe residual de u_σ a σ, defineix el morfisme injectiu de grups $G_0/G_1 \longrightarrow (B/\mathfrak{P})^*$.

Com que el grup quocient G_0/G_1 és cíclic, podem considerar un element $\sigma \in G_0$ que generi el quocient G_0/G_1; es tracta de demostrar que l'ordre de σ com a automorfisme de G_0/G_1 és un divisor de $q - 1$. Per a això, podem considerar un element $\varphi \in G_{-1}$ tal que la reducció mòdul $\mathfrak{P}$ de l'automorfisme $\varphi : B \longrightarrow B$ sigui l'automorfisme de Frobenius del cos finit $B/\mathfrak{P}$ sobre $A/\mathfrak{p}$; recordem que l'automorfisme de Frobenius de $B/\mathfrak{P}$ és donat per l'assignació $b \mapsto b^q$. En particular, podem escriure $\sigma(\pi) = u_\sigma \pi$, $\varphi(\pi) = u_\varphi \pi$, i $\varphi\sigma\varphi^{-1}(\pi) = v\pi$, per a certs elements $u_\sigma, u_\varphi, v \in B$.

Amb aquestes notacions, podem observar que se satisfan les igualtats següents: d'una banda, de la segona es dedueix immediatament que $\varphi^{-1}(\pi) = \varphi^{-1}(u_\varphi)^{-1}\pi$; d'altra banda, la hipòtesi que el quocient G_{-1}/G_1 és abelià ens ensenya que $u_\sigma - v \in \mathfrak{P}$, ja que l'acció dels dos automorfismes $\varphi\sigma\varphi^{-1}$ i σ coincideix mòdul $\mathfrak{P}^2$, de manera que $\varphi\sigma\varphi^{-1}(\pi) - \sigma(\pi) \in \mathfrak{P}^2$; i podem dividir per π. Finalment, podem escriure:

$$\varphi\sigma\varphi^{-1}(\pi) = \varphi\sigma(\varphi^{-1}(u_\varphi)^{-1}\pi) = \varphi(\sigma\varphi^{-1}(u_\varphi)^{-1}u_\sigma\pi) = \varphi\sigma\varphi^{-1}(u_\varphi)^{-1}\varphi(u_\sigma)u_\varphi\pi;$$

és a dir, $v = \varphi\sigma\varphi^{-1}(u_\varphi)^{-1}\varphi(u_\sigma)u_\varphi$. Si tenim en compte que $\sigma \in G_0$, obtenim que σ és la identitat en $B/\mathfrak{P}$, de manera que

$$v \equiv \varphi\varphi^{-1}(u_\varphi)^{-1}\varphi(u_\sigma)u_\varphi = \varphi(u_\sigma) = u_\sigma^q \pmod{\mathfrak{P}},$$

per definició de φ. D'aquí es dedueix immediatament que $u_\sigma^{q-1} \equiv 1 \pmod{\mathfrak{P}}$, ja que $u_\sigma \notin \mathfrak{P}$; d'aquesta manera, σ és d'ordre divisor de $q-1$, com volíem demostrar. □

5.8 Grups de ramificació i diferent

L'objectiu d'aquesta secció és proporcionar una fórmula explícita per al càlcul del diferent d'una extensió en alguns casos particulars importants. Convé, però, establir algunes propietats dels grups de ramificació respecte de cadenes d'extensions.

Proposició 5.8.1. *Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i de Galois, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció en A, $G := \mathrm{Gal}\,(L|K)$ el grup de Galois, $H \subseteq G$ un subgrup qualsevol de G, $K' := L^H$ el cos fix, $A' := B \cap K'$ la clausura entera de A en K' i $\mathfrak{P}' := \mathfrak{P} \cap A'$ la contracció de $\mathfrak{P}$ a A'. Aleshores, els grups de ramificació de $\mathfrak{P}$ sobre $\mathfrak{P}'$ es poden calcular per la fórmula*

$$G_k(\mathfrak{P}|\mathfrak{P}') = G_k(\mathfrak{P}|\mathfrak{p}) \cap H.$$

Demostració: Immediata a partir de la definició dels grups de ramificació, ja que $H = \mathrm{Gal}\,(L|K')$. □

Corol·lari 5.8.2. *Si, a més a més, el grup H és un dels grups de ramificació, posem $G_k(\mathfrak{P}|\mathfrak{p})$, aleshores, els grups de ramificació $G_i(\mathfrak{P}|\mathfrak{P}')$ són exactament el grup $G_k(\mathfrak{P}|\mathfrak{p})$ per a $0 \leq i \leq k$, i $G_i(\mathfrak{P}|\mathfrak{P}') = G_i(\mathfrak{P}|\mathfrak{p})$, per a $i > k$.* □

Seguidament es tracta de fer el càlcul dels exponents del diferent en funció dels ordres dels grups de ramificació. Per a això, ens situarem en el cas local, cosa que podem fer sempre ja que el diferent i els grups de ramificació es conserven per localització, i totalment ramificat, cosa que podem fer si ens restringim a l'extensió donada pel grup d'inèrcia.

Proposició 5.8.3. *Amb les mateixes notacions que a la proposició anterior, suposem que A és un anell de Dedekind local, que l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$ és separable, i que l'extensió $B|A$ és totalment ramificada en $\mathfrak{P}$. Aleshores, l'exponent de $\mathfrak{P}$ en el diferent $\mathcal{D}(B|A)$ és donat per la suma finita*

$$\sum_{k\geq 0}(\#G_k(\mathfrak{P}|\mathfrak{p}) - 1).$$

DEMOSTRACIÓ: Com que l'extensió és totalment ramificada, $\mathfrak{P}$ és l'únic ideal primer de B que divideix $\mathfrak{p}$, i com que A és local, els anells A i B són principals. Triem un generador π de $\mathfrak{P}$ i sigui $f(X) := \mathrm{Irr}(\pi, K)(X)$ el polinomi mònic irreductible de $A[X]$ que té π com a arrel. Assegurem que en aquest cas π és un element primitiu de l'extensió $L|K$ i $B = A[\pi]$.

En efecte, això és una conseqüència del resultat més general que segueix.

Lema 5.8.4. *En aquesta situació, és $B = A[\pi]$ i el polinomi $f(X) := \mathrm{Irr}(\pi, K)(X)$ és un polinomi d'Eisenstein respecte del generador de l'ideal maximal $\mathfrak{p}$ de A.*

DEMOSTRACIÓ: Sigui $e := e(\mathfrak{P}|\mathfrak{p}) = [L : K]$ l'índex de ramificació, que coincideix amb el grau perquè l'extensió és totalment ramificada i l'extensió residual és separable. Comencem per demostrar que els elements 1, π, π^2, $\ldots$, π^{e-1} són K-linealment independents. De manera més general, suposem que tenim una igualtat de la forma

$$b = a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1},$$

amb els elements $a_i \in K$ i $b \in L$. Per a tot índex i, $1 \leq i \leq e-1$, tal que a_i sigui no nul, sigui $v_i \in \mathbb{Z}$ l'exponent de la potència exacta de $\mathfrak{p}$ que conté l'element a_i; aquesta potència només és no negativa quan $a_i \in A$ i, en cas contrari, l'ideal $\mathfrak{p}^{v_i}$ només és un ideal fraccionari. Com que l'extensió de $\mathfrak{p}$ a l'anell B és l'ideal $\mathfrak{P}^e$, i com que π és un generador de $\mathfrak{P}$, els elements $a_i\pi^i$ tals que $a_i \neq 0$ pertanyen exactament a l'ideal $\mathfrak{P}^{i+ev_i}$. Els exponents són tots diferents, ja que ho són mòdul e. D'aquí resulta que la suma $a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}$ pertany a l'ideal $\mathfrak{P}^t$ i no a $\mathfrak{P}^{t+1}$, on t és el mínim dels exponents $i + ev_i$ tals que $a_i \neq 0$. En particular, si $b = 0$, ha de ser $a_i = 0$ per a tot índex i, ja que 0 pertany a totes les potències positives de $\mathfrak{P}$; això ens diu que els elements 1, π, $\ldots$, π^{e-1} són K-linealment independents.

Però encara ens diu més; si $b \in A$, aleshores t ha de ser un múltiple no negatiu de e, ja que la potència exacta de $\mathfrak{P}$ que conté b és e vegades la potència exacta de $\mathfrak{p}$ que conté b en A. En particular, si $b \in A$, aleshores $t \geq 0$ i t és divisible per e; per tant, tots els v_i han de ser no negatius, i $b \in A[\pi]$; això demostra la igualtat $B = A[\pi]$.

Finalment, ja hem fet notar que el polinomi $f(X)$ és de coeficients en A; a més a més, com que les potències $1, \pi, \pi^2, \ldots, \pi^{e-1}$ són K-linealment independents, $f(X)$ és un polinomi de grau e, ja que el grau no pot sobrepassar el de l'extensió i ha de ser més gran o igual que e. Si posem $f(X) = X^e - (a_0 + a_1X + \cdots + a_{e-1}X^{e-1})$, obtenim la igualtat $\pi^e = a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}$ amb $a_i \in A$; com que π^e pertany exactament a l'ideal $\mathfrak{P}^e$, resulta que $t = e$, i això només s'aconsegueix quan $t = ev_0$, ja que, en cas contrari, t no és divisible per e. Dit d'una altra manera, $v_0 = 1$, i $v_i \geq 1$ per a tot índex $i \geq 1$ tal que $a_i \neq 0$; com que $\mathfrak{p}$ és principal, resulta que $a_0 \in \mathfrak{p} - \mathfrak{p}^2$ és un generador de $\mathfrak{p}$ i tots els altres coeficients a_i pertanyen a $\mathfrak{p}$; és a dir, $f(X)$ és un polinomi d'Eisenstein respecte de $\mathfrak{p}$. □

En conseqüència, el conductor de B en $A[\pi]$ és trivial i, per tant, el diferent de l'extensió és l'ideal, potència de $\mathfrak{P}$, generat per $f'(\pi)$. Calculem aquest ideal. Si considerem la derivada en π del polinomi $f(X)$, podem escriure $f(X) = \prod_{\sigma\in G}(X - \sigma(\pi))$, de manera que $f'(\pi)$ és el producte $f'(\pi) = \prod_{\sigma\neq 1}(\pi - \sigma(\pi)) = \prod_{k\geq 0}\prod_{\sigma\in G_k - G_{k+1}}(\pi - \sigma(\pi))$, ja que $G_0 = G_{-1} = G$ perquè l'extensió és totalment ramificada. Ara, per a $\sigma \in G_k$, $\sigma \notin G_{k+1}$, ha de ser

$b - \sigma(b) \in \mathfrak{P}^{k+1}$ per a tot element $b \in B$; en particular, $\pi - \sigma(\pi) \in \mathfrak{P}^{k+1}$; d'altra banda, $\pi - \sigma(\pi) \notin \mathfrak{P}^{k+2}$, ja que en aquest cas, obtindríem que $\sigma \in G_{k+1}$ com a la demostració de la proposició **5.6.5**. Així, l'exponent de $\mathfrak{P}$ en el diferent $\mathcal{D}(B|A) = f'(\pi)B$ és la suma

$$\begin{aligned}\sum_{k\geq 0} \sum_{\sigma \in G_k - G_{k+1}} (k+1) &= \sum_{k\geq 0} (k+1)(\#G_k - \#G_{k+1}) \\ &= \sum_{k\geq 0} (k+1)[(\#G_k - 1) - (\#G_{k+1} - 1)] \\ &= \sum_{k\geq 0} (\#G_k - 1),\end{aligned}$$

ja que G_k és trivial a partir d'un lloc endavant. Això acaba la prova. □

Capítol 6

El teorema de Kronecker-Weber

Aquest capítol es dedica a fer la demostració del teorema de Kronecker-Weber, que ja ha estat enunciat en el primer capítol. De fet, és un dels punts culminants del curs i l'excusa que hem utilitzat per a fer la introducció dels mètodes generals de ramificació i geometria dels nombres que se solen utilitzar en la teoria algebraica de nombres. Recordem-ne l'enunciat.

Teorema 6.0.5 (Kronecker-Weber)**.** *Sigui $K|\mathbb{Q}$ una extensió abeliana. Aleshores, existeix una arrel de la unitat, ζ, tal que $K \subseteq \mathbb{Q}(\zeta)$.*

6.1 El cas moderadament ramificat

Notem que ja hem demostrat aquest teorema en el cas que l'extensió $K|\mathbb{Q}$ sigui quadràtica. Ara convé fer la reducció de la prova al cas de les extensions cícliques de grau potència d'un nombre primer. Concretament, podem començar per establir el resultat següent.

Proposició 6.1.1. *Si el teorema de Kronecker-Weber se satisfà per a totes les extensions cícliques de grau potència de primer, aleshores se satisfà per a totes les extensions abelianes.*

Demostració: Només cal considerar que tota extensió abeliana descompon com a producte linealment disjunt d'extensions cícliques de grau potència de primer. Això és deduieix del fet que tot grup abelià descompon com a producte directe de p-subgrups i aquests com a producte directe de subgrups cíclics; concretament, suposem que $G := \mathrm{Gal}\,(K|\mathbb{Q})$ descompon com a producte $G := \prod_{i=1}^{r} G_i$, on p_i és un nombre primer qualsevol i G_i és un p_i-grup cíclic. Sigui K_i el subcòs de K fix pel subgrup $\prod_{j\neq i} G_j$ de G; aleshores, $K_i|\mathbb{Q}$ és una extensió cíclica de grau potència d'un nombre primer p_i; per hipòtesi, per a cada índex i existeix una arrel de la unitat ζ_i tal que $K_i \subseteq \mathbb{Q}(\zeta_i)$. Siguin $n_i \in \mathbb{Z}$, $1 \leq i \leq r$, tals que ζ_i és una arrel primitiva n_i-èsima de la unitat, $n := \mathrm{mcm}\{n_i\}_{1\leq i\leq r}$ i ζ una arrel primitiva n-èsima de la unitat. Com que K és el cos composició dels cossos K_i, obtenim que $K \subseteq \mathbb{Q}(\zeta)$, com es volia provar. □

Recordem que tota extensió de $\mathbb{Q}$ és ramificada en algun nombre primer (cf. **4.5.1**). Ara, es tracta de fer la reducció de la prova del teorema de Kronecker-Weber al cas en

què el conjunt dels nombres primers que ramifiquen consisteix només en el primer que divideix el grau; dit d'una altra manera, per a la prova del teorema podrem suposar que l'extensió és cíclica de grau potència d'un nombre primer p i no ramificada a tot nombre primer ℓ diferent de p.

Efectivament. Suposem que $K|\mathbb{Q}$ és cíclica de grau potència d'un nombre primer p i que $\ell \neq p$ és un nombre primer que ramifica. Sigui $\mathfrak{L}$ un ideal primer de l'anell dels enters del cos K que divideix ℓ; en particular, l'extensió $K|\mathbb{Q}$ és moderadament ramificada en $\mathfrak{L}$; és a dir, el grup de ramificació $G_1(\mathfrak{L}|\ell)$ és trivial. Com que l'ordre del grup d'inèrcia en $\mathfrak{L}$ és un divisor del grau, ha de ser una potència de p, posem p^m; i com que el cos residual de $\mathbb{Z}$ en ℓ és el cos $\mathbb{F}_\ell$, el fet que el quocient $G_{-1}(\mathfrak{L}|\ell)/G_1(\mathfrak{L}|\ell)$ sigui abelià ens permet assegurar que l'ordre del grup d'inèrcia divideix $\ell - 1$ (cf. la proposició **5.7.2**); per tant, $\ell \equiv 1 \pmod{p^m}$. Ara bé, l'extensió $\mathbb{Q}(\zeta_\ell)|\mathbb{Q}$ és cíclica, no ramificada fora de ℓ i totalment ramificada en ℓ; en conseqüència, existeix un únic subcòs $L \subseteq \mathbb{Q}(\zeta_\ell)$ tal que l'extensió $L|\mathbb{Q}$ és cíclica, totalment ramificada en ℓ, no ramificada fora de ℓ i de grau p^m.

Considerem el cos composició KL. Com que les extensions $K|\mathbb{Q}$ i $L|\mathbb{Q}$ són abelianes de grau potència de p, també la composició $KL|\mathbb{Q}$ és una extensió abeliana de grau potència de p, posem p^{n+t}, on $t \leq m$ i $p^n := [K : \mathbb{Q}]$. Siguin $\mathfrak{L}'$ un ideal primer de l'anell dels enters de KL que divideixi $\mathfrak{L}$, $I' := G_0(\mathfrak{L}'|\ell)$ el grup d'inèrcia de $\mathfrak{L}'$ sobre el primer ℓ, i $H := \mathrm{Gal}\,(L|\mathbb{Q}) \cong \mathbb{Z}/p^m\mathbb{Z}$ el grup de Galois.

El morfisme de restricció $\mathrm{Gal}\,(KL|\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(K|\mathbb{Q})$ aplica el grup d'inèrcia I' en el grup d'inèrcia $G_0(\mathfrak{L}|\ell)$, de manera que s'obté una inclusió $I' \subseteq G_0(\mathfrak{L}|\ell) \times H$, per via de la identificació de $\mathrm{Gal}\,(KL|\mathbb{Q})$ amb un subgrup del producte $\mathrm{Gal}\,(K|\mathbb{Q}) \times \mathrm{Gal}\,(L|\mathbb{Q})$. D'altra banda, l'ordre del grup d'inèrcia I' és múltiple de p^m, ja que l'índex de ramificació de $\mathfrak{L}'$ sobre ℓ és divisible per l'índex de ramificació de $\mathfrak{L}$ sobre ℓ; i, com abans, els grups de ramificació superiors $G_i(\mathfrak{L}'|\ell)$, $i \geq 1$, són trivials, ja que l'extensió és de grau potència de p i p no divideix la característica residual ℓ; per tant, el grup d'inèrcia I' és cíclic. A més a més, l'ordre dels elements del grup producte $G_0(\mathfrak{L}|\ell) \times H$ és un divisor de p^m, ja que tot dos grups són cíclics d'ordre p^m; com que l'ordre de I' és com a mínim p^m i I' és cíclic, l'ordre de I' és exactament p^m. Així, si designem per K' el subcòs de KL fix pel subgrup I', l'extensió $K'|\mathbb{Q}$ és no ramificada en ℓ; i com que $L|\mathbb{Q}$ és totalment ramificada en ℓ, ha de ser $K' \cap L = \mathbb{Q}$; per tant, el subcòs $K'L \subseteq KL$ és de grau $[K'L : \mathbb{Q}] = [K' : \mathbb{Q}][L : \mathbb{Q}] = [KL : \mathbb{Q}]$, ja que el grau de l'extensió $K'|\mathbb{Q}$ és el grau de l'extensió $KL|\mathbb{Q}$ dividit per l'índex de ramificació de $\mathfrak{L}'$ sobre ℓ, que és exactament el mateix que el grau de l'extensió $L|\mathbb{Q}$; en conseqüència, obtenim la igualtat de cossos $K'L = KL$.

D'aquesta manera, si demostrem que el cos K' és ciclotòmic, com que L també ho és, ho és la seva composició $K'L = KL$, de manera que el cos K, essent subcòs d'un cos ciclotòmic, també és un cos ciclotòmic. Ara, però, el cos K' no ramifica en ℓ, per construcció, i els seus primers de ramificació formen un subconjunt del conjunt dels primers de ramificació de l'extensió $K|\mathbb{Q}$; com que el conjunt de primers de ramificació de l'extensió $K|\mathbb{Q}$ és finit, podem repetir l'argument i suposar que l'extensió $K|\mathbb{Q}$ és no ramificada fora dels ideals primers que divideixen p.

En aquests moments ja podem demostrar el teorema de Kronecker-Weber per al cas moderadament ramificat. Però podem dir encara més.

Proposició 6.1.2. *Sigui $K|\mathbb{Q}$ una extensió abeliana de grau potència d'un nombre primer p, $[K : \mathbb{Q}] = p^m$, que només ramifica en un primer $\ell \neq p$. Aleshores, $\ell \equiv 1 \pmod{p^m}$,*

l'extensió $K|\mathbb{Q}$ és totalment ramificada en ℓ, i K és l'únic subcòs de $\mathbb{Q}(\zeta_\ell)$ de grau p^m. En conseqüència, també, l'extensió $K|\mathbb{Q}$ és cíclica.

Demostració: Per a la primera part, podem suposar que l'extensió $K|\mathbb{Q}$ és cíclica de grau potència d'un nombre primer p. Sigui ℓ un primer diferent de p que ramifica; acabem de provar que $\ell \equiv 1 \pmod{p^m}$. A més a més, les extensions $K|\mathbb{Q}$ i $L|\mathbb{Q}$ de la discussió anterior només ramifiquen en el primer ℓ; per tant, l'extensió $K'|\mathbb{Q}$ és no ramificada arreu; com que tot cos de nombres $K' \neq \mathbb{Q}$ ramifica en algun primer, ha de ser $K' = \mathbb{Q}$; en conseqüència, $K \subseteq KL = K'L = L$ i L és l'únic subcòs de grau p^m de $\mathbb{Q}(\zeta_\ell)$. El final és clar; si no suposem que l'extensió $K|\mathbb{Q}$ és cíclica, podem considerar K com la composició d'extensions cícliques; cada una d'elles és un subcòs de $\mathbb{Q}(\zeta_\ell)$ de manera que K també. Com que l'extensió $\mathbb{Q}(\zeta_\ell)|\mathbb{Q}$ és cíclica, hem acabat. □

Corol·lari 6.1.3. *Sigui $K|\mathbb{Q}$ una extensió abeliana i moderadament ramificada a tots els ideals primers. Aleshores, existeix una arrel de la unitat ζ i $K \subseteq \mathbb{Q}(\zeta)$.*

Demostració: En virtut de la proposició **6.1.1**, podem suposar que l'extensió $K|\mathbb{Q}$ és cíclica. D'altra banda, la reducció successiva de K a K' en la discussió precedent a la proposició anterior permet suposar que el cos K només ramifica en un ideal primer; i, en aquest cas, la proposició anterior acaba la prova. □

Observació 6.1.4. En particular, si $K|\mathbb{Q}$ és una extensió abeliana, $\ell_1, \ldots, \ell_k$ els primers que ramifiquen, i si el grau de l'extensió no és divisible per cap dels primers ℓ_i, aleshores el cos K és un subcòs del cos ciclotòmic $\mathbb{Q}(\zeta)$, on ζ és una arrel n-èsima de la unitat per a $n = \ell_1 \cdots \ell_k$.

6.2 El cas cíclic de grau potència d'un primer senar

Hem vist que per a establir el teorema de Kronecker-Weber és suficient demostrar-lo per al cas de les extencions cícliques de grau potència d'un nombre primer p i que només ramifiquen en p. Es tracta de veure'l en el cas en què p és un primer senar. Necessitarem, però, el resultat següent, amb hipòtesis més generals.

Proposició 6.2.1. *Siguin p un nombre primer senar i $K|\mathbb{Q}$ una extensió abeliana de grau p^m que només ramifiqui en el primer p. Aleshores, $K|\mathbb{Q}$ és totalment ramificada en p i cíclica.*

Demostració: Siguin $\mathfrak{P}$ un ideal primer de l'anell dels enters de K que divideix p i $I := G_0(\mathfrak{P}|p)$ el grup d'inèrcia. El cos fix per I és un cos extensió de $\mathbb{Q}$ que no ramifica a cap ideal primer; per tant, en virtut del teorema d'Hermite-Minkowski $K^I = \mathbb{Q}$ i l'extensió $K|\mathbb{Q}$ és totalment ramificada en p; dit d'una altra manera, el grup d'inèrcia és tot el grup de Galois de l'extensió. En particular, l'extensió residual és trivial i el cos residual de K en $\mathfrak{P}$ és $\mathbb{F}_p$. Com que coneixem l'estructura dels quocients successius dels grups de ramificació, podem assegurar que el grup d'inèrcia coincideix amb el grup de ramificació G_1, i que per a tot nombre enter $k \geq 1$ el grup quocient G_k/G_{k+1} és un grup abelià trivial o cíclic d'ordre p. Per tant, l'extensió és totalment ramificada en p. Per a veure que l'extensió és cíclica es tracta d'aplicar el resultat següent.

Lema 6.2.2. *Suposem que $K|\mathbb{Q}$ és una extensió abeliana de grau p que només ramifica en p; aleshores, el grup de ramificació $G_2(\mathfrak{P}|p)$ és trivial.*

DEMOSTRACIÓ: Si localitzem en $S := \mathbb{Z} - p\mathbb{Z}$ podem suposar que $\mathfrak{P}$ és un ideal principal, i podem elegir un generador π de $\mathfrak{P}$. Sigui $f(X) := \mathrm{Irr}(\pi, \mathbb{Q})(X)$ el polinomi mònic irreductible de $\mathbb{Q}[X]$ que té π per arrel; de fet, com que π és enter sobre $S^{-1}\mathbb{Z}$, tenim que $f(X) \in S^{-1}\mathbb{Z}[X]$. Com que la cadena dels grups de ramificació esdevé trivial a partir d'un lloc endavant, podem considerar un enter k tal que $G_k \neq (1)$ però $G_{k+1} = (1)$; i com que $G_0 = G_1 \cong \mathbb{Z}/p\mathbb{Z}$, ha de ser $k \geq 1$. Es tracta de veure que $k = 1$.

Si considerem el valor en π del polinomi derivat del polinomi $f(X)$, obtenim les relacions $f'(\pi) \in \mathfrak{P}^{(k+1)(p-1)}$ i $f'(\pi) \notin \mathfrak{P}^{(k+1)(p-1)+1}$. En efecte, com que podem escriure $f(X) = \prod_{\sigma \in G_k} (X - \sigma(\pi))$, resulta que $f'(\pi)$ és el producte $f'(\pi) = \prod_{\sigma \neq 1}(\pi - \sigma(\pi))$; però com que $\sigma \in G_k$ i $\sigma \notin G_{k+1}$, ha de ser $b - \sigma(b) \in \mathfrak{P}^{k+1}$ per a tot element b enter de K sobre $S^{-1}\mathbb{Z}$; en particular, $\pi - \sigma(\pi) \in \mathfrak{P}^{k+1}$; d'altra banda, $\pi - \sigma(\pi) \notin \mathfrak{P}^{k+2}$, ja que en aquest cas, obtindríem que $\sigma \in G_{k+1}$ com a la demostració de la proposició **5.6.5**. Ara només cal multiplicar per a tots els automorfismes $\sigma \in G_k$, $\sigma \neq 1$. D'altra banda, podem escriure una igualtat de la forma

$$f'(\pi) = p\pi^{p-1} + (p-1)a_{p-1}\pi^{p-2} + \cdots + 2a_2\pi + a_1,$$

on els coeficients a_j són elements de $S^{-1}\mathbb{Z}$; és a dir, són nombres racionals que tenen denominadors enters no divisibles per p. Com que l'extensió $K|\mathbb{Q}$ és totalment ramificada i de grau p, l'extensió de p és l'ideal $\mathfrak{P}^p$, de manera que cada un dels coeficients a_j que siguin no nuls és un element d'una potència $\mathfrak{P}^{pn_j}$ amb $n_j \geq 0$. En particular, si v_j denota l'exponent de $\mathfrak{P}$ que conté el sumand $ja_j\pi^{j-1}$ però tal que $ja_j\pi^{j-1} \notin \mathfrak{P}^{v_j+1}$, obtenim que $v_j \equiv j-1 \pmod{p}$; en conseqüència, tots els sumands no nuls estan en potències diferents de $\mathfrak{P}$ i la suma està en la potència que té l'exponent v_j més petit. En particular, obtenim la desigualtat $(k+1)(p-1) \leq v_{p-1} = 2p-1$; com que $k \geq 1$ i $p > 2$, això implica que $k = 1$, de manera que $G_2 = (1)$, com volíem provar. □

Per a fer la demostració de la proposició, sabem que $G = G_0 = G_1$; sigui $k \geq 2$ tal que $G = G_k$ però $G_{k+1} \subsetneq G_k$; el grup quocient G_k/G_{k+1} és un grup abelià cíclic d'ordre p. Com que G és un p-grup abelià finit, si no fos cíclic hauria de tenir més de dos subgrups d'índex p (de fet, com a mínim n'hauria de tenir $p+1$); per tant, és suficient provar que G_{k+1} és l'únic subgrup de G d'índex p.

Suposem que H fos un subgrup d'índex p de G, i diferent de G_{k+1}; es tracta d'arribar a contradicció. Per a això, considerem els cossos fixos K^H i $K^{G_{k+1}}$ i siguin $\mathfrak{P}_H$ i $\mathfrak{P}_{k+1}$ les contraccions a aquests cossos de l'ideal primer $\mathfrak{P}$ de l'anell dels enters de K. El càlcul dels grups de ramificació de $\mathfrak{P}$ per a aquestes extensions es pot fer de manera senzilla. Com que $\mathrm{Gal}\left(K|K^{G_{k+1}}\right) = G_{k+1}$, obtenim les igualtats

$$G_i(\mathfrak{P}|\mathfrak{P}_{k+1}) = \begin{cases} G_i \cap G_{k+1} = G_{k+1}, & \text{si } 0 \leq i \leq k+1, \\ G_i \cap G_{k+1} = G_i, & \text{si } i > k+1; \end{cases}$$

$$G_i(\mathfrak{P}|\mathfrak{P}_H) = \begin{cases} G_i \cap H = H, & \text{si } 0 \leq i \leq k, \\ G_i \cap H \subsetneq G_{k+1}, & \text{si } i \geq k+1, \end{cases}$$

aquesta darrera igualtat perquè $H \neq G_{k+1}$ i tots dos són subgrups d'índex p de G. Aquests càlculs ens permeten comparar els exponents de $\mathfrak{P}$ en els diferents de les extensions $K|K^H$ i $K|K^{G_{k+1}}$ de la manera següent:

$$\sum_{i \geq 0}(\#G_i \cap H - 1) < \sum_{i \geq 0}(\#G_i \cap G_{k+1} - 1),$$

ja que els k primers sumands són iguals, el $k+1$-èsim satisfà la desigualtat estricta, i els següents satisfan la desigualtat $\leq$.

D'altra banda, el lema ens permet assegurar que l'exponent del diferent de les extensions $K^H|\mathbb{Q}$ i $K^{G_{k+1}}|\mathbb{Q}$ és el mateix, ja que els grups G_0 i G_1 de les dues extensions són cíclics d'ordre p i els grups G_2 són trivials. Si ara considerem el diferent de l'extensió $K|\mathbb{Q}$ i calculem l'exponent de $\mathfrak{P}$ en aquesta extensió a partir de la fórmula de la transitivitat del diferent per a cadenes d'extensions, obtenim una contradicció, ja que l'extensió a K dels ideals $\mathfrak{P}_H$ i $\mathfrak{P}_{k+1}$ és exactament el mateix ideal, $\mathfrak{P}^{p^{m-1}}$, perquè les extensions són totalment ramificades de grau p^{m-1}. En conseqüència, ha de ser $H = G_{k+1}$ i G és cíclic. □

Proposició 6.2.3. *Siguin p un nombre primer senar i $K|\mathbb{Q}$ una extensió cíclica de grau p^m que només ramifiqui en p. Aleshores, K és l'únic subcòs de $\mathbb{Q}(\zeta)$ de grau p^m, on ζ és una arrel primitiva p^{m+1}-èsima de la unitat.*

Demostració: En efecte, sigui K' l'únic subcòs de $\mathbb{Q}(\zeta)$ de grau p^m; aleshores, les dues extensions $K|\mathbb{Q}$ i $K'|\mathbb{Q}$ satisfan les condicions de l'enunciat; és a dir, són cícliques de grau p^m i només ramifiquen en p; per tant, el cos composició KK' és un cos extensió abeliana de $\mathbb{Q}$ que només ramifica en p i de grau potència de p; en virtut de la proposició anterior, ha de ser cíclica i de grau potència de p; com que conté dos cossos K i K' que tenen el mateix grau sobre $\mathbb{Q}$, ha de ser $K = K'$, com volíem veure. □

6.3 El cas cíclic de grau potència de 2

Hem reduït la demostració del teorema de Kronecker-Weber al cas de les extensions cícliques de grau potència de 2 que només ramifiquen en 2. Per a acabar la prova, comencem per demostrar el resultat següent.

Proposició 6.3.1. *Sigui $K|\mathbb{Q}$ una extensió abeliana de grau 2^m que només ramifica en 2 i suposem que $K \subseteq \mathbb{R}$. Aleshores, K és exactament el subcòs real maximal $\mathbb{Q}(\zeta + \zeta^{-1})$ del cos $\mathbb{Q}(\zeta)$, on ζ és una arrel primitiva 2^{m+2}-èsima de la unitat.*

Demostració: Sabem que tota extensió quadràtica de $\mathbb{Q}$ és ciclotòmica i que si només ramifica en 2 és un dels tres cossos $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, o $\mathbb{Q}(\sqrt{-2})$, que són els tres únics subcossos quadràtics de $\mathbb{Q}(\zeta)$, on ζ és una arrel primitiva $8 = 2^3$-èsima de la unitat; per tant, el resultat és clar en el cas $m = 1$, ja que $\mathbb{Q}(\sqrt{2})$ és l'únic d'aquests cossos que és real.

Suposem, doncs, que $m \geq 2$. Com que $K|\mathbb{Q}$ és abeliana de grau divisible per 2, K conté un subcòs quadràtic; el fet que el cos K sigui real i que l'extensió $K|\mathbb{Q}$ només ramifica en 2 imposa les mateixes restriccions a aquest subcòs quadràtic; per tant, K conté l'únic cos quadràtic real que només ramifica en 2. Això implica que el grup de Galois de l'extensió $K|\mathbb{Q}$ només té un subgrup d'índex 2 i, en conseqüència, és cíclic.

Comparem el cos K amb el cos $L := \mathbb{Q}(\zeta + \zeta^{-1})$. El cos composició KL és un cos real i l'extensió $KL|\mathbb{Q}$ és abeliana, no ramificada fora de 2 i de grau potència de 2; acabem de provar que l'extensió $KL|\mathbb{Q}$ és cíclica; com que conté K i L, que són del mateix grau sobre $\mathbb{Q}$, ha de ser $K = L$, com volíem demostrar. □

Ara podem acabar la demostració del teorema de Kronecker-Weber.

Proposició 6.3.2. *Sigui $K|\mathbb{Q}$ una extensió abeliana de grau 2^m i no ramificada fora de 2. Aleshores, K és un dels tres subcossos $\mathbb{Q}(\zeta^2)$, $\mathbb{Q}(\zeta+\zeta^{-1})$, $\mathbb{Q}(\zeta-\zeta^{-1})$ del cos ciclotòmic $\mathbb{Q}(\zeta)$, on ζ és una arrel primitiva 2^{m+2}-èsima de la unitat. Aquests cossos són els únics subcossos de $\mathbb{Q}(\zeta)$ de grau 2^m sobre $\mathbb{Q}$.*

Demostració: En efecte, el cos composició de K i $\mathbb{Q}(i)$, $K(i)$, és un cos extensió abeliana de $\mathbb{Q}$, no ramificada fora de 2, i de grau potència de 2, 2^n, amb $n \leq m+1$. Sigui $K(i)^+ := K(i) \cap \mathbb{R}$, el subcòs real maximal de $K(i)$; és un cos real, no ramificat fora de 2, i de grau 2^s, $s \leq n-1 \leq m$, ja que $i \notin K(i)^+$; per tant, $K(i)^+$ és subcòs de $\mathbb{Q}(\zeta+\zeta^{-1})$, que és l'únic cos real que satisfà aquestes condicions. Per a acabar, és suficient demostrar que $K(i)$ és el cos $K(i)^+(i)$ que, clarament, és un subcòs de $\mathbb{Q}(\zeta+\zeta^{-1})(i) = \mathbb{Q}(\zeta)$. Però $K(i)^+(i) \subseteq K(i)$ i els dos cossos són de grau 2 sobre $K(i)^+$; per tant, coincideixen. □

6.4 Conductor d'una extensió abeliana de $\mathbb{Q}$

Sigui $K|\mathbb{Q}$ una extensió abeliana. El teorema de Kronecker-Weber ens permet assegurar l'existència d'una arrel de la unitat ζ tal que $K \subseteq \mathbb{Q}(\zeta)$.

Definició 6.4.1. S'anomena conductor d'una extensió abeliana $K|\mathbb{Q}$ el menor nombre enter positiu n tal que $K \subseteq \mathbb{Q}(\zeta_n)$, on ζ_n és una arrel primitiva n-èsima de la unitat.

Observació 6.4.2. Si n és senar, aleshores $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$, de manera que el conductor d'una extensió abeliana de $\mathbb{Q}$ és un natural $n \not\equiv 2 \pmod 4$.

El teorema de Kronecker-Weber admet una formulació més precisa, en la qual es té en compte el conductor. En efecte, podem establir fàcilment el resultat següent.

Teorema 6.4.3 (Kronecker-Weber)**.** *Siguin $K|\mathbb{Q}$ una extensió abeliana, $p_1, p_2, \ldots, p_k$ els primers de $\mathbb{Z}$ que ramifiquen en K i posem $e_i := p_i^{r_i} e_i'$, amb e_i' no divisible per p_i, l'índex de ramificació de p_i, $1 \leq i \leq k$, en l'extensió $K|\mathbb{Q}$. Aleshores, el conductor n de K és donat per*

$$n = \begin{cases} p_1^{r_1+1} p_2^{r_2+1} \cdots p_k^{r_k+1}, & \text{si } p_i \neq 2 \text{ per a tot índex } i, \\ 2^{\varepsilon} p_1^{r_1+1} p_2^{r_2+1} \cdots p_k^{r_k+1}, & \text{si } p_1 = 2, \end{cases}$$

on $\varepsilon \in \{0, 1\}$.

Demostració: De fet, aquest resultat està inclòs en la successió de reduccions que hem fet de la prova del teorema. En efecte, la reducció al cas d'extensions cícliques de grau potència d'un primer s'ha fet prenent com a conductor de K el mínim múltiple comú dels conductors dels factors cíclics; d'altra banda, la reducció al cas salvatgement ramificat només afegeix una arrel $p_1 p_2 \cdots p_k$-èsima de la unitat, com a màxim. Finalment, en el cas $K|\mathbb{Q}$ cíclica, de grau potència de p, i no ramificada fora de p, hem pres una arrel primitiva p^{r+1}-èsima de la unitat, si $p \neq 2$, i $2^{r+2} = 2 \cdot 2^{r+1}$-èsima, si $p = 2$. Per tant, el valor n donat a l'enunciat és un múltiple del conductor.

D'altra banda, si $m = p_1^{r_1} p_2^{r_2+1} \cdots p_k^{r_k+1}$, l'índex de ramificació de p_1 en l'extensió $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ no és divisible per $p_1^{r_1}$, de manera que el conductor de K ha de ser divisible per $p_i^{r_i+1}$ per a tot primer p_i que ramifica en K. □

El valor de ε es pot determinar en cada cas a partir de la successió de subcossos K' que s'obtenen pel procediment descrit just després de la proposició **6.1.1**. Només cal notar que si ζ és una arrel primitiva 2^{m+2}-èsima de la unitat, i si $K = \mathbb{Q}(\zeta^2)$, aleshores $\varepsilon = 0$, mentre que si $K = \mathbb{Q}(\zeta + \zeta^{-1})$ o $K = \mathbb{Q}(\zeta - \zeta^{-1})$, aleshores $\varepsilon = 1$.

Corol·lari 6.4.4. *Siguin $K|\mathbb{Q}$ una extensió abeliana, n el seu conductor, i ζ una arrel primitiva n-èsima de la unitat. Aleshores, l'extensió $\mathbb{Q}(\zeta)|K$ és moderadament ramificada a tots els ideals primers de l'anell dels enters de K.*

Demostració: La potència d'un nombre primer p que divideix l'índex de ramificació $e_p(\mathbb{Q}(\zeta)|\mathbb{Q})$ és exactament la mateixa que divideix $e_p(K|\mathbb{Q})$; per tant, si $\mathfrak{p}$ és un ideal primer de l'anell dels enters de K que divideix p, l'índex de ramificació de $\mathfrak{p}$ en $\mathbb{Q}(\zeta)|K$ no és divisible per p. □

Observació 6.4.5. Si K és un cos de nombres i $L|K$ és una extensió abeliana, no és cert en general que $L \subseteq K(\zeta)$ per a cap arrel de la unitat ζ.

Per exemple, considerem el cos $\mathbb{Q}(\alpha)$, on $\alpha^3 - \alpha + 1 = 0$ i sigui $K := \mathbb{Q}(\sqrt{-23})$. L'extensió $K(\alpha)|K$ és cíclica de grau 3 i no ramifica a cap ideal primer de K; però $K(\alpha)$ no pot estar inclòs en cap cos $K(\zeta)$ per a arrels de la unitat ζ, ja que per ser $K \subseteq \mathbb{Q}(\zeta_{23})$, obtindríem que $\mathbb{Q}(\alpha)$ seria un subcòs de $\mathbb{Q}(\zeta, \zeta_{23})$, de manera que $\mathbb{Q}(\alpha)|\mathbb{Q}$ seria una extensió abeliana; però $\mathbb{Q}(\alpha)|\mathbb{Q}$ no és ni tan sols de Galois.

Capítol 7

Ramificació en el cas infinit

L'objectiu d'aquest capítol és fer un resum de les propietats de la ramificació i escriure-les sense la hipòtesi de finitud de les extensions. Per a això, ens hem de situar en el cas galoisià. Per tant, cal repassar, en primer lloc, la teoria de Galois en el cas general, no necessàriament finit. Per a exposicions més detallades de la teoria de Galois en el cas infinit, poden ser útils les referències [Neu 86], [Ri 72], o [Wa 82], entre moltes d'altres.

7.1 Teoria de Galois

Sigui $L|K$ una extensió algebraica, no necessàriament finita, de cossos. Aleshores, el cos L és el límit inductiu (si es vol, la reunió conjuntista) de tots els subcossos $K' \subseteq L$ tals que $K'|K$ és una extensió finita.

Definició 7.1.1. Es diu que l'extensió $L|K$ és de Galois quan és normal i separable.

En aquest cas, les extensions finites i de Galois $K'|K$ tals que $K' \subseteq L$ formen un sistema cofinal del sistema de totes les subextensions finites de $L|K$; per tant, el cos L també és el límit inductiu dels subcossos $K' \subseteq L$ tals que $K'|K$ és una subextensió finita i de Galois de $L|K$. A més a més, el grup de Galois $\mathrm{Gal}\,(L|K)$ és el límit projectiu dels grups de Galois $\mathrm{Gal}\,(K'|K)$ per a les subextensions finites i de Galois $K'|K$ de $L|K$. És a dir, $\mathrm{Gal}\,(L|K)$ és un grup profinit; per tant, un grup topològic que té una base d'entorns de l'element neutre formada pels grups de Galois $\mathrm{Gal}\,(L|K')$ on $K'|K$ descriu el conjunt de les subextensions finites i de Galois de $L|K$. Els grups $\mathrm{Gal}\,(L|K')$ són subgrups normals de $\mathrm{Gal}\,(L|K)$. En particular, $\mathrm{Gal}\,(L|K)$ és un grup topològic Hausdorff i compacte.

Recordem el teorema fonamental de la teoria de Galois.

Teorema 7.1.2. *Sigui $L|K$ qualsevol extensió de Galois de cossos. Existeix una aplicació bijectiva entre el conjunt dels subgrups tancats H de $\mathrm{Gal}\,(L|K)$ i el conjunt dels subcossos L' de L que contenen K donada per l'assignació*

$$H \mapsto L' := L^H$$

amb inversa donada per

$$L' \mapsto \mathrm{Gal}\,(L|L')\,.$$

Els subgrups oberts H es corresponen amb els subcossos L' tals que l'extensió $L'|K$ és finita. □

Exemple 7.1.3 (El grup de Galois absolut d'un cos finit)**.** Considerem com a cos base un cos finit $K := \mathbb{F}_q$ de cardinal q i característica p. És ben conegut que per a tot nombre enter $n \geq 1$ el cos $\mathbb{F}_q$ té una i només una extensió de grau n en una clausura algebraica fixa $L := \overline{\mathbb{F}}_p$ de $\mathbb{F}_q$; és el cos $\mathbb{F}_{q^n}$ format per 0 i les arrels (q^n-1)-èsimes de la unitat de $\overline{\mathbb{F}}_q$. En particular, l'extensió $\mathbb{F}_{q^n}|\mathbb{F}_q$ és una extensió cíclica de grau n, generada per l'automorfisme de Frobenius, $x \mapsto x^q$, de $\mathbb{F}_{q^n}$.

D'altra banda, aquesta mateixa assignació, per a $x \in \overline{\mathbb{F}}_q$, defineix un element Frob_q de $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$; s'anomena l'automorfisme de Frobenius de l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$. La restricció de Frob_q a $\mathbb{F}_{q^n}$ és l'automorfisme de Frobenius de l'extensió $\mathbb{F}_{q^n}|\mathbb{F}_q$. El cos fix pel subgrup de $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$ generat per Frob_q és el cos $\mathbb{F}_q$, de manera que l'adherència d'aquest subgrup és tot el grup de Galois. Dit d'una altra manera, el grup $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$ és generat topològicament per un sol element, Frob_q.

Això ens diu que el grup de Galois $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$ és (isomorf a) el límit projectiu dels grups $\mathbb{Z}/n\mathbb{Z}$; és a dir, $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right) \cong \widehat{\mathbb{Z}}$, la compleció profinita de $\mathbb{Z}$.

Exemple 7.1.4. Fixem un nombre primer senar p i, per a tot nombre enter $n \geq 1$, considerem una arrel primitiva p^n-èsima de la unitat, $\eta_n := \zeta_{p^n}$. Sigui $K_n := \mathbb{Q}(\eta_n)$ i posem $L := K_\infty$ el cos reunió dels cossos K_n. El grup de Galois de cada una de les extensions $K_n|\mathbb{Q}$ és un grup cíclic d'ordre $(p-1)p^{n-1}$ generat per un automorfisme de K_n determinat unívocament per la seva acció sobre η_n. A més a més, η_{n+1}^p és un element primitiu de l'extensió $K_n|\mathbb{Q}$, de manera que el morfisme natural donat per restricció,

$$\mathrm{Gal}\left(K_{n+1}|\mathbb{Q}\right) \longrightarrow \mathrm{Gal}\left(K_n|\mathbb{Q}\right),$$

aplica un generador en un generador. En conseqüència, el grup de Galois de l'extensió $K_\infty|\mathbb{Q}$ és isomorf al límit projectiu dels grups abelians $(\mathbb{Z}/p^{n+1}\mathbb{Z})^* \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$; és a dir, és isomorf al grup abelià ${\mathbb{Z}_p}^*$ format pels elements invertibles de l'anell $\mathbb{Z}_p$, límit projectiu dels anells $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Dit d'una altra manera, $\mathrm{Gal}\left(K_\infty|\mathbb{Q}\right)$ és isomorf al producte cartesià $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. En farem un estudi més detallat en el capítol 9.

En aquests exemples s'observa que el cos L és el límit inductiu d'una família numerable de subcossos $K' \subseteq L$ tals que $K'|K$ és una extensió finita. Encara més, en aquests exemples es pot demostrar que L és la reunió d'una successió numerable de tals subcossos. Però això no és cert en general; per exemple, podem considerar una quantitat no numerable d'elements algebraicament independents X_i sobre un cos k i formar el cos de fraccions K de l'anell de polinomis en aquestes indeterminades i coeficients en k. Es tracta de veure que si L és una clausura algebraica de K, aleshores no existeix cap família numerable de subcossos $K_n \subseteq L$ tals que $K_n|K$ sigui una extensió finita i L sigui el límit inductiu de la família de cossos K_n. Per exemple, aquest és el cas si prenem $k = \mathbb{Q}$ i $L = \mathbb{C}$.

En efecte, el límit inductiu d'una família numerable d'extensions finitament generades d'un cos K és un cos numerablement generat sobre K, mentre que l'extensió $L|K$ no pot ser numerablement generada ja que ha de contenir totes les arrels m-èsimes de totes les indeterminades X_i per a tots els enters $m \geq 2$, i aquestes generen una subextensió de L que no és numerablement generada sobre K.

Aquesta observació farà que, a partir d'ara, restringim l'estudi a situacions més planeres.

7.2 Grups de descomposició i d'inèrcia

Siguin A un domini íntegrament tancat de dimensió 1, K el seu cos de fraccions, $L|K$ una extensió de Galois, no necessàriament finita, i B la clausura entera de A en L. En particular, B és un domini d'integritat íntegrament tancat i de dimensió 1, ja que és una extensió entera d'un anell de dimensió 1. En general, però, i encara que A sigui un anell de Dedekind, B pot no ser un anell de Dedekind. Per a veure això, donem-ne un exemple concret.

Fixem un nombre primer p i considerem, per a tot nombre enter $n \geq 1$, una arrel primitiva p^n-èsima de la unitat, η_n, la successió de cossos $K_n := \mathbb{Q}(\eta_n)$, i posem K_∞ la reunió d'aquesta cadena de cossos. L'anell dels enters de cada un dels cossos $\mathbb{Q}(\eta_n)$ és l'anell $A_n := \mathbb{Z}[\eta_n]$ i la clausura entera de $\mathbb{Z}$ en K_∞ és l'anell A_∞, reunió dels anells A_n. D'altra banda, sigui $\mathfrak{P}_n$ l'ideal de A_n generat per l'element $1-\eta_n$; és l'únic ideal primer de A_n que divideix p. L'ideal $\mathfrak{P}_\infty$ de A_∞ generat per tots els elements $1-\eta_n$ és, doncs, la reunió de tots els ideals $\mathfrak{P}_n$; en conseqüència, $\mathfrak{P}_\infty$ no és l'ideal total de A_∞ i és un ideal maximal amb cos residual $\mathbb{F}_p$, que és el cos residual de $\mathfrak{P}_n$ en A_n per a tot n. Ara bé, l'ideal primer $\mathfrak{P}_\infty$ coincideix amb la seva potència p-èsima, ja que l'ideal generat per $1-\eta_n$ és la potència p-èsima de l'ideal generat per $1-\eta_{n+1}$ en l'anell A_{n+1}. En conseqüència, en A_∞ no hi ha descomposició única dels ideals com a producte d'ideals primers no nuls i A_∞ no pot ser un anell de Dedekind.

Tornem a la situació general. Malgrat que els anells A i B no siguin anells de Dedekind, donat un ideal primer no nul $\mathfrak{P} \subseteq B$, si posem $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A, l'ideal $\mathfrak{p}$ és un ideal primer no nul de A i podem, encara, definir els grups de descomposició i d'inèrcia de $\mathfrak{P}$ sobre $\mathfrak{p}$ per les fórmules

$$G_{-1}(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in \mathrm{Gal}\,(L|K) : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

$$G_0(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p}) : \sigma \text{ actua trivialment en el quocient } B/\mathfrak{P}\}.$$

En particular, aquesta definició s'aplica en el cas que l'anell A és la clausura entera de $\mathbb{Z}$ en un cos extensió algebraica de $\mathbb{Q}$, no necessàriament finita, i també en el cas d'un anell simetritzat d'aquest anell respecte de qualsevol sistema multiplicativament tancat. Aquestes són les situacions que ens interessen.

A partir d'ara, i pel que resta d'aquest capítol, donada una extensió de Galois $L|K$ de manera que K és el cos de fraccions d'un domini íntegrament tancat de dimensió 1, suposarem que l'extensió $L|K$ es pot escriure com el límit inductiu d'una família numerable de subextensions finites $K'|K$ de $L|K$. En aquest cas, podem elegir una successió (numerable) de subextensions de Galois finites $K_n|K$ de $L|K$ tals que per a tot nombre natural n és $K_n \subseteq K_{n+1}$ i el cos L és la reunió de la cadena de cossos K_n; en particular, això ho podrem fer sempre que el cos L sigui numerable; per exemple, un cos de nombres algebraics, no necessàriament finit sobre $\mathbb{Q}$.

Igual que en el cas finit, podem escriure el resultat següent.

Lema 7.2.1. *Sigui $\mathfrak{p}$ un ideal primer qualsevol de l'anell A. Aleshores, el grup de Galois $\mathrm{Gal}\,(L|K)$ actua transitivament en el conjunt dels ideals primers $\mathfrak{P}$ de B que divideixen $\mathfrak{p}$; és a dir, tals que $\mathfrak{P} \cap A = \mathfrak{p}$.*

Demostració: Siguin $\mathfrak{P}, \mathfrak{P}' \subseteq B$ dos ideals primers de B que tinguin la mateixa contracció a A, $\mathfrak{p} := \mathfrak{P} \cap A = \mathfrak{P}' \cap A$. Triem una successió de subextensions de Galois finites

$K_n|K$ de $L|K$ tals que $K_0 = K$, $K_n \subseteq K_{n+1}$ per a tot $n \geq 0$, i $L = \bigcup_{n\geq 0} K_n$; per a tot enter $n \geq 0$ denotem per A_n la clausura entera de A en K_n i siguin $\mathfrak{P}_n := \mathfrak{P} \cap A_n$ i $\mathfrak{P}'_n := \mathfrak{P}' \cap A_n$ les contraccions de $\mathfrak{P}$ i $\mathfrak{P}'$ a l'anell A_n. Com que l'extensió $K_n|K$ és finita i de Galois, existeix $\sigma_n \in \mathrm{Gal}\,(K_n|K)$ tal que $\sigma_n(\mathfrak{P}_n) = \mathfrak{P}'_n$; això s'ha enunciat en el capítol 3 amb la hipòtesi suplementària que l'anell A és de Dedekind, però aquesta hipòtesi no s'ha fet servir; de fet, només s'ha utilitzat que l'anell A és un domini íntegrament tancat. Si demostrem que podem elegir aquesta successió de manera que cada σ_n sigui la restricció de σ_{n+1} al cos K_n ja haurem acabat; en efecte, en aquest cas, existeix un automorfisme $\sigma \in \mathrm{Gal}\,(L|K)$ tal que la restricció de σ a cada un dels cossos K_n és l'automorfisme σ_n, ja que $\mathrm{Gal}\,(L|K)$ és el límit projectiu dels grups de Galois $\mathrm{Gal}\,(K_n|K)$; aleshores, l'ideal primer de B, $\sigma(\mathfrak{P})$, és la reunió dels ideals $\mathfrak{P}'_n = \sigma_n(\mathfrak{P}_n)$; per tant, $\sigma(\mathfrak{P}) = \mathfrak{P}'$, com calia demostrar.

Veiem, doncs, que podem elegir els automorfismes σ_n de manera que la restricció de σ_{n+1} al cos K_n sigui l'automorfisme σ_n i que $\sigma_{n+1}(\mathfrak{P}_{n+1}) = \mathfrak{P}'_{n+1}$. Per a això, donat σ_n, sigui $\tau_{n+1} \in \mathrm{Gal}\,(K_{n+1}|K)$ una extensió qualsevol de σ_n al cos K_{n+1}; aleshores, τ_{n+1} transforma l'ideal primer $\mathfrak{P}_{n+1}$ en un cert ideal primer $\tau_{n+1}(\mathfrak{P}_{n+1})$ de A_{n+1}; com que $\tau_{n+1}(\mathfrak{P}_{n+1})$ i $\mathfrak{P}'_{n+1}$ són ideals primers de A_{n+1} que contrauen a l'ideal primer $\mathfrak{P}'_n$ de A_n i l'extensió $K_{n+1}|K_n$ és finita i de Galois, existeix un element $\rho_{n+1} \in \mathrm{Gal}\,(K_{n+1}|K_n)$ tal que $\rho_{n+1}(\tau_{n+1}(\mathfrak{P}_{n+1})) = \mathfrak{P}'_{n+1}$; aleshores, podem prendre $\sigma_{n+1} := \rho_{n+1} \circ \tau_{n+1} \in \mathrm{Gal}\,(K_{n+1}|K_n)$ i aquest automorfisme estén σ_n, ja que τ_{n+1} l'estén i ρ_{n+1} és la identitat en K_n, i envia l'ideal $\mathfrak{P}_{n+1}$ a l'ideal $\mathfrak{P}'_{n+1}$; això és el que calia demostrar. □

Proposició 7.2.2. *Siguin A un domini íntegrament tancat de dimensió 1, K el seu cos de fraccions, $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \ldots$ una cadena d'extensions de Galois $K_n|K$, $L := \bigcup_{n\geq 0} K_n$ la reunió de la cadena, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Aleshores:*

(a) *l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$ és una extensió algebraica normal de cossos;*

(b) *els grups de descomposició i d'inèrcia $G_{-1}(\mathfrak{P}|\mathfrak{p})$ i $G_0(\mathfrak{P}|\mathfrak{p})$ són subgrups tancats de $\mathrm{Gal}\,(L|K)$; i*

(c) *la successió natural de morfismes de grups topològics*

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,((B/\mathfrak{P})|(A/\mathfrak{p})) \longrightarrow 1$$

és exacta.

Demostració: Siguin $A_n := B \cap K_n$ i $\mathfrak{P}_n := \mathfrak{P} \cap A_n$, per a tot $n \geq 0$. Aleshores, $B = \bigcup_{n\geq 0} A_n$, $\mathfrak{P} = \bigcup_{n\geq 0} \mathfrak{P}_n$, i $B/\mathfrak{P} = \bigcup_{n\geq 0}(A_n/\mathfrak{P}_n)$; en conseqüència, l'extensió residual $(B/\mathfrak{P})|(A/\mathfrak{p})$ és algebraica i normal, el grup de descomposició $G_{-1}(\mathfrak{P}|\mathfrak{p})$ és el límit projectiu dels grups de descomposició $G_{-1}(\mathfrak{P}_n|\mathfrak{p})$ i el grup d'inèrcia $G_0(\mathfrak{P}|\mathfrak{p})$ és el límit projectiu dels grups d'inèrcia $G_0(\mathfrak{P}_n|\mathfrak{p})$; en particular, tots dos són subgrups tancats de $\mathrm{Gal}\,(L|K)$.

Finalment, la successió exacta de grups profinits

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,((B/\mathfrak{P})|(A/\mathfrak{p})) \longrightarrow 1$$

s'obté per pas al límit projectiu de les successions

$$1 \longrightarrow G_0(\mathfrak{P}_n|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}_n|\mathfrak{p}) \longrightarrow \mathrm{Gal}\left(\frac{A_n}{\mathfrak{P}_n}\middle|\frac{A}{\mathfrak{p}}\right) \longrightarrow 1,$$

per a $n \geq 1$, perquè hi ha diagrames commutatius de morfismes continus de grups amb les files exactes

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G_0(\mathfrak{P}_{n+1}|\mathfrak{p}) & \longrightarrow & G_{-1}(\mathfrak{P}_{n+1}|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}\left(\dfrac{A_{n+1}}{\mathfrak{P}_{n+1}}\middle|\dfrac{A}{\mathfrak{p}}\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_0(\mathfrak{P}_n|\mathfrak{p}) & \longrightarrow & G_{-1}(\mathfrak{P}_n|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}\left(\dfrac{A_n}{\mathfrak{P}_n}\middle|\dfrac{A}{\mathfrak{p}}\right) & \longrightarrow & 1
\end{array}$$

on els morfismes verticals són donats per restricció. □

Definició 7.2.3. Direm que l'ideal primer $\mathfrak{P}$ és no ramificat sobre la seva contracció $\mathfrak{p}$ quan el grup d'inèrcia $G_0(\mathfrak{P}|\mathfrak{p})$ és trivial; això equival a dir que tots els ideals $\mathfrak{P}_n$ són no ramificats sobre $\mathfrak{p}$. Anàlogament, direm que $\mathfrak{P}$ és totalment ramificat quan el grup d'inèrcia $G_0(\mathfrak{P}|\mathfrak{p})$ és tot el grup de Galois $\mathrm{Gal}\,(L|K)$; això equival a dir que els ideals primers $\mathfrak{P}_n$ són totalment ramificats sobre $\mathfrak{p}$.

7.3 Extensions abelianes no finites de $\mathbb{Q}$

En aquesta secció ens situarem en el cas en què el cos base és el cos $\mathbb{Q}$ dels nombres racionals. Es tracta de resumir les propietats de les extensions abelianes de $\mathbb{Q}$.

Sigui p un nombre primer i sigui $\mu(p^\infty)$ el grup de totes les arrels de la unitat d'una clausura algebraica fixa de $\mathbb{Q}$ que són d'ordre potència de p. El cos $\mathbb{Q}(\mu(p^\infty))$ és un cos extensió abeliana de $\mathbb{Q}$ amb grup de Galois isomorf al grup abelià

$$\begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim \mathbb{Z}/p^n\mathbb{Z}, & \text{si } p \neq 2, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z} \times \varprojlim \mathbb{Z}/2^n\mathbb{Z}, & \text{si } p = 2. \end{cases}$$

És una extensió totalment ramificada en p i no ramificada fora de p. De fet, és el cos extensió abeliana maximal de $\mathbb{Q}$ que és no ramificada fora de p.

De manera més general, si S és un conjunt qualsevol de nombres primers, el cos composició $\mathbb{Q}_{ab}^S := \prod_{p\in S} \mathbb{Q}(\mu(p^\infty))$ és l'extensió abeliana maximal de $\mathbb{Q}$ no ramificada en tot primer $\ell \notin S$; el seu grup de Galois és isomorf al producte dels grups de Galois de les extensions $\mathbb{Q}(\mu(p^\infty))|\mathbb{Q}$ per a $p \in S$; és a dir,

$$\mathrm{Gal}\left(\mathbb{Q}_{ab}^S|\mathbb{Q}\right) \cong \begin{cases} \prod_{p\in S} \mathbb{Z}/(p-1)\mathbb{Z} \times \prod_{p\in S} \mathbb{Z}_p, & \text{si } 2 \notin S, \\ \mathbb{Z}/2\mathbb{Z} \times \prod_{p\in S} \mathbb{Z}/(p-1)\mathbb{Z} \times \prod_{p\in S} \mathbb{Z}_p, & \text{si } 2 \in S. \end{cases}$$

En general, doncs, el grup de Galois de l'extensió abeliana maximal de $\mathbb{Q}$ no ramificada fora d'un conjunt fixat de primers no és un grup finitament generat, ja que els grups $\mathbb{Z}_p$

no són grups numerables; però, en canvi, si S és finit, el grup de Galois de l'extensió $\mathbb{Q}_{ab}^S|\mathbb{Q}$ és un grup topològic finitament generat; en efecte, el producte dels grups $\mathbb{Z}_p$ per a $p \in S$ és un grup procíclic (és a dir, límit projectiu de grups cíclics) i, en conseqüència, és generat topològicament per un sol element; en conseqüència, el nombre de generadors topològics de $\mathrm{Gal}\left(\mathbb{Q}_{ab}^S|\mathbb{Q}\right)$ és $\leq \#S + 1$.

En general, donats un cos de nombres K, extensió finita de $\mathbb{Q}$, i un conjunt finit S d'ideals primers de l'anell dels enters de K, es pot parlar de l'extensió maximal de K no ramificada fora de S, $K^S|K$, i de l'extensió abeliana maximal de K no ramificada fora de S, $K_{ab}^S|K$; són extensions de Galois del cos K; ens podem preguntar sobre la generació finita o no del grup de Galois d'aquestes extensions. En general, no es coneix encara la resposta a aquesta pregunta. De fet, el grup $G_S^{ab} := \mathrm{Gal}\left(K_{ab}^S|K\right)$ és l'abelianitzat del grup $G_S := \mathrm{Gal}\left(K^S|K\right)$, de manera que el fet de tenir informació sobre aquest darrer pot donar llum sobre què succeeix per a G_S. I en el cas en què el grup G_S sigui finitament generat com a grup topològic, encara sorgeix la qüestió de donar fites bones per al nombre de generadors; i millor si aquestes fites només depenen del cos K i del cardinal del conjunt S. Aquesta pregunta és la que hem respost en el cas abelià sobre $\mathbb{Q}$ per a tot conjunt finit S de nombres primers.

Capítol 8

Equacions diofantines

La segona part del curs es dedica a fer un estudi, d'una banda, d'algunes equacions diofantines, i de l'altra, d'alguns mètodes locals i d'alguns mètodes analítics importants en Teoria algebraica de Nombres. L'objectiu d'aquest capítol és fer-ne una introducció. Concretament, per a aquesta part del curs utilitzarem com a fil conductor l'estudi de l'equació de Fermat i la classificació de les formes quadràtiques racionals. Aquest capítol conté motivacions per a aquest estudi.

8.1 Còniques racionals

Per a començar de manera planera, podem preguntar-nos pel conjunt dels punts racionals d'una cònica projectiva, i ens situarem en el cas d'un cos de característica diferent de 2.

Exercici 8.1.1. Sigui K un cos qualsevol de característica diferent de 2. Aleshores tota forma quadràtica $q(Y_1, Y_2, \ldots, Y_n)$ de coeficients en K és diagonalitzable; és a dir, existeixen $a_1, a_2, \ldots, a_n \in K$ i un canvi lineal de les indeterminades (invertible), també de coeficients en K, de manera que la forma quadràtica q es pot escriure en la forma $a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$.

En particular, tota cònica projectiva C definida sobre K té un model donat per una equació $aX^2 + bY^2 + cZ^2 = 0$, de coeficients $a, b, c \in K$. El problema que ens interessa és fer la descripció del conjunt $C(K)$ format per tots els punts $P := (x, y, z)$ de coordenades projectives $x, y, z \in K$ tals que $ax^2 + by^2 + cz^2 = 0$.

Notem que, per exemple, la cònica donada per l'equació $X^2 + Y^2 + Z^2 = 0$ no té punts racionals (ni tampoc punts reals); en aquest cas, tenim que $C(\mathbb{R}) = C(\mathbb{Q}) = \varnothing$. Així, un primer problema que seria bo de tractar és esbrinar si el conjunt $C(K)$ és no buit.

Definició 8.1.2. Una cònica C s'anomena (absolutament) irreductible quan una forma quadràtica $aX^2 + bY^2 + cZ^2$ que la defineix no és el producte de dues formes lineals de coeficients en K^a, una clausura algebraica de K.

Exercici 8.1.3. En particular, això equival a dir que els coeficients a, b, c són tots tres no nuls. I això equival a dir que cap forma quadràtica que defineix C no descompon en producte de dues formes lineals de coeficients en K^a.

Considerem, doncs, una cònica irreductible, C, definida per una forma quadràtica $aX^2+bY^2+cZ^2$ de coeficients a, b, c en el cos K, i suposem que $P_0 := (x_0, y_0, z_0) \in C(K)$ és un punt K-racional de la cònica C. Sigui r una recta K-racional que no passi per P_0; equivalentment, r és definida per una forma lineal en X, Y, Z de coeficients en K, algun d'ells no nul.

Si ara considerem un punt qualsevol $P \in C(K)$, la recta que uneix P_0 amb P és una recta K-racional, ja que és definida per una equació de coeficients en K; per tant, la intersecció d'aquesta recta amb la recta r és un punt K-racional del pla projectiu. Recíprocament, donat un punt K-racional de r, la recta que uneix aquest punt amb P_0 és una recta K-racional, de manera que la seva intersecció amb la cònica C consta de dos punts K-racionals; en efecte, la intersecció de la recta amb la cònica és una parella de punts del pla projectiu; com que un d'ells és el punt P_0, que és K-racional, i com que la cònica és K-racional, l'altre punt ha de tenir coordenades en K. Dit d'una altra manera, hem provat el resultat següent:

Proposició 8.1.4. *Sigui C una cònica irreductible definida sobre un cos K de característica diferent de 2 i tal que $C(K)$ sigui no buit. Aleshores, existeix una bijecció entre el conjunt $C(K)$ dels punts K-racionals de C i el conjunt dels punts K-racionals d'una recta arbitrària definida sobre K.* □

Definició 8.1.5. S'anomena terna pitagòrica una terna (a, b, c) de nomtres enters per als quals se satisfà l'equació pitagòrica, $X^2 + Y^2 = Z^2$; o sigui, l'equació de Fermat per a exponent $n = 2$. Notem que les ternes pitagòriques tals que $a, b, c > 0$ corresponen a (les longituds de) els costats dels triangles rectangles de costats racionals.

El resultat següent proporciona una parametrització usual de les ternes pitagòriques (cf., per exemple, [Tra 1998]).

Exercici 8.1.6. Sigui C la cònica definida per $X^2 + Y^2 - Z^2 = 0$ sobre $\mathbb{Q}$. En prendre com a punt P_0 el punt $P_0 := (1, 0, 1)$ i com a recta r la recta $X = 0$, s'obté que els punts racionals de C són els punts (x, y, z) i els (y, x, z) del pla projectiu que tenen coordenades enteres de la forma $x = \lambda(u^2 - v^2)$, $y = 2\lambda uv$, $z = \lambda(u^2 + v^2)$, tals que $\lambda \in \mathbb{Z}$, $\lambda \neq 0$, i u, v són enters primers entre si.

Així, doncs, el problema de la descripció del conjunt $C(K)$ del punts K-racionals de la cònica (irreductible) C queda reduït a estudiar en quines condicions el conjunt $C(K)$ és no buit. I disposem d'una bona descripció de la solució en el cas en què el cos K és el cos $\mathbb{Q}$ dels nombres racionals. Dit d'una altra manera, ens plantegem el problema següent.

Problema 8.1.7. Donada una cònica C definida per una equació $aX^2 + bY^2 + cZ^2 = 0$ amb $a, b, c \in \mathbb{Q}$, no nuls, determinar una condició necessària i suficient perquè el conjunt $C(\mathbb{Q})$ sigui no buit.

Per a començar, podem suposar que els coeficients a, b, c són enters primers entre si. En efecte, si multipliquem els coeficients a, b, c de l'equació per un nombre no nul, el conjunt de les solucions de l'equació no varia; per tant, si multipliquem per un denominador comú dels coeficients podem suposar que aquests són enters; un cop els tenim enters, si els dividim pel seu màxim divisor comú obtindrem coeficients primers entre si; és a dir, podem suposar que $\mathrm{mcd}(a, b, c) = 1$.

D'altra banda, podem suposar que els coeficients són lliures de quadrats. En efecte, suposem que $a = d^2a'$, amb a' lliure de quadrats. Si canviem X per X/d, (que és un canvi lineal de les indeterminades), i anàlogament amb els altres dos coeficients, la cònica es pot descriure per una nova equació de la forma $aX^2 + bY^2 + cZ^2 = 0$, amb $a, b, c \in \mathbb{Z}$, no nuls, lliures de quadrats i primers entre si. Una reducció més es resumeix en el resultat següent.

Lema 8.1.8. *Sigui C una cònica absolutament irreductible definida sobre $\mathbb{Q}$. Aleshores, C és descrita per una equació de la forma $aX^2 + bY^2 + cZ^2 = 0$, on a, b, c són enters no nuls, lliures de quadrats, i coprimers dos a dos. Si, a més a més, el conjunt $C(\mathbb{Q})$ és no buit, aleshores a, b, c no són tots del mateix signe.*

Demostració: Cal veure que podem suposar que els coeficients són coprimers dos a dos. Per a això, suposem que d és el màxim divisor comú de a i b; aleshores, podem canviar el coeficient a per a/d, b per b/d, i c per dc, i les indeterminades X per dX, Y per dY, i Z per Z/d, de manera que la nova equació té els coeficients a i b primers entre si; repetint el procediment amb les parelles a, c i b, c, obtenim el resultat que desitjàvem.

Per a la segona part, és clar que si tots els coeficients són del mateix signe els podem suposar positius i si $(x, y, z) \in \mathbb{P}^2(\mathbb{Q})$, aleshores $ax^2 + by^2 + cz^2 > 0$, ja que no pot ser $x = y = z = 0$; però això implica que $C(\mathbb{Q})$ és el conjunt buit. □

Necessitarem, encara, una altra forma equivalent de l'equació; concretament, encara podem multiplicar tots els coeficients per $-c$ i després treure quadrats, de manera que podem suposar que l'equació és de la forma $aX^2 + bY^2 - Z^2 = 0$, amb a, b enters lliures de quadrats, però no necessàriament primers entre si. En aquestes condicions, és clar que tot punt racional de C també és un punt real, de manera que perquè $C(\mathbb{Q})$ sigui no buit cal que els dos coeficients a, b no siguin negatius alhora.

8.2 El teorema de Legendre

L'objectiu d'aquesta secció és demostrar el resultat següent.

Teorema 8.2.1 (Legendre)**.** *Sigui C una cònica plana definida sobre $\mathbb{Q}$, donada per una equació $aX^2 + bY^2 + cZ^2 = 0$ on a, b, c són enters no nuls, lliures de quadrats, no tots tres del mateix signe, i coprimers dos a dos. Condició necessària i suficient perquè el conjunt $C(\mathbb{Q})$ dels punts racionals de C sigui no buit és que $-ab$ sigui un residu quadràtic mòdul c, $-bc$ un residu quadràtic mòdul a, i $-ca$ un residu quadràtic mòdul b.*

Demostració: La demostració de la necessitat de la condició és senzilla. En efecte, suposem que $P \in C(\mathbb{Q})$; podem elegir coordenades homogènies de P, (x, y, z), que siguin enters primers entre si; és a dir, tals que $\mathrm{mcd}(x, y, z) = 1$. Aleshores, se satisfà la congruència $-abx^2 \equiv (by)^2 \pmod{c}$. Si p és un nombre primer que dividís alhora c i x, també dividiria by^2, de manera que dividiria y, ja que $\mathrm{mcd}(b, c) = 1$; per tant, p^2 dividiria $ax^2 + by^2 = -cz^2$ i, com que c és lliure de quadrats, p hauria de dividir z; és a dir, p dividiria x, y, z, contra la suposició que $\mathrm{mcd}(x, y, z) = 1$. Això diu que $\mathrm{mcd}(c, x) = 1$ i, per tant, que x és invertible mòdul c; en conseqüència, $-ab \equiv (by/x)^2 \pmod{c}$ i $-ab$ és un quadrat mòdul c. nàlogament, també $-bc$ és un quadrat mòdul a i $-ca$ és un quadrat mòdul b.

Per a veure la suficiència de les condicions, utilitzarem alguns resultats intermedis.

Lema 8.2.2. *Siguin $A, b, c \in \mathbb{Z}$ tals que* $\mathrm{mcd}(b,c) = 1$*, i A és un quadrat mòdul b i mòdul c. Aleshores, A és un quadrat mòdul bc.*

Demostració: La demostració és una aplicació immediata del teorema xinès del residu: les congruències $z^2 \equiv A \pmod{b}$ i $z^2 \equiv A \pmod{b}$ tenen solució, de manera que també en té la congruència $z^2 \equiv A \pmod{bc}$. □

Lema 8.2.3. *Siguin K un cos qualsevol i a, b elements no nuls de K. Aleshores, les tres condicions següents són equivalents:*

(a) *L'equació $aX^2 + bY^2 - Z^2 = 0$ té una solució no trivial;*

(b) *$a \in \mathrm{N}(K(\sqrt{b})^*)$;*

(c) *$b \in \mathrm{N}(K(\sqrt{a})^*)$,*

on $\mathrm{N}(L^*)$ designa el grup dels elements de K que són norma d'un element no nul de L.

Demostració: Sigui $\alpha \in K(\sqrt{b})^*$ i suposem que $[K(\sqrt{b}) : K] = 2$. Aleshores, podem escriure α en la forma $\alpha = z + y\sqrt{b}$ amb $y, z \in K$, de manera que $\mathrm{N}(\alpha) = z^2 - by^2$. Si tenim una solució no trivial (x, y, z) de l'equació $aX^2 + bY^2 - Z^2 = 0$, se satisfà que $x \neq 0$, ja que si fos $x = 0$ seria $b = (z/y)^2$ i $[K(\sqrt{b}) : K] = 1$; per tant, obtenim que $a = \mathrm{N}(\alpha/x) = (z/x)^2 - b(y/x)^2 \in \mathrm{N}(K(\sqrt{b})^*)$. I recíprocament: si $a = \mathrm{N}(z + y\sqrt{b})$, és $a = z^2 - by^2$ i $(1, y, z)$ és una solució no trivial de l'equació $aX^2 + bY^2 - Z^2 = 0$. D'altra banda, si $[K(\sqrt{b}) : K] = 1$, aleshores b és el quadrat d'un element no nul de K; però en aquest cas tot element de K és norma i l'equació $aX^2 + bY^2 - Z^2 = 0$ té la solució no trivial $(0, 1, \sqrt{b})$. L'equivalència amb l'altra propietat es fa anàlogament, en intercanviar els papers de a i b. □

Per a provar la suficiència de les condicions del teorema de Legendre és suficient demostrar que l'equació $-acX^2 - bcY^2 - Z^2 = 0$ té solucions enteres $(x, y, z) \neq (0, 0, 0)$. La hipòtesi que $-ac$ és un quadrat mòdul b, afegit al fet trivial que $-ac$ és un quadrat mòdul c i al fet que $\mathrm{mcd}(b, c) = 1$, fa que $-ac$ sigui un quadrat mòdul bc. Anàlogament, $-bc$ també és un quadrat mòdul ac. Per tant, el teorema de Legendre quedarà provat si demostrem la proposició següent.

Proposició 8.2.4. *Siguin a, b enters no nuls, lliures de quadrats, no tots dos negatius, i tals que a és un quadrat mòdul b, b és un quadrat mòdul a, i $-ab/d^2$ és un quadrat mòdul d, on $d := \mathrm{mcd}(a, b)$. Aleshores, l'equació $aX^2 + bY^2 - Z^2 = 0$ té solucions enteres $(x, y, z) \neq (0, 0, 0)$.*

Demostració: Podem fer inducció sobre $m := |a| + |b|$; és clar que sempre $m \geq 2$. Si $m = 2$, aleshores $|a| = |b| = 1$ i, com que a i b no són tots dos negatius, les possibilitats de l'equació són

$$\begin{cases} X^2 + Y^2 - Z^2 = 0, & \\ X^2 - Y^2 - Z^2 = 0, & \text{que tenen solucions} \\ -X^2 + Y^2 - Z^2 = 0, & \end{cases} \qquad \begin{matrix} (1,0,1), \\ (1,0,1), \\ (0,1,1), \end{matrix}$$

enteres no trivials.

Suposem, doncs, que $m > 2$. Per la simetria de l'equació, podem suposar que $|a| \leq |b|$, de manera que $|b| \geq 2$. Si $a = 1$, obtenim una solució no trivial $(1, 0, 1)$ de l'equació; si no, com que a és un quadrat mòdul b, podem trobar enters t, b' tals que $t^2 = a + bb'$; com que a és lliure de quadrats, és $b' \neq 0$ i, a més a més, podem elegir t de manera que $2|t| \leq |b|$. Clarament, $bb' = t^2 - a = \mathrm{N}(t - \sqrt{a}) \in \mathrm{N}(\mathbb{Q}(\sqrt{a})^*)$ i, per tant, b és norma de $\mathbb{Q}(\sqrt{a})^*$ si, i només si, ho és b'. Dit d'una altra manera, l'equació $aX^2 + bY^2 - Z^2 = 0$ té solucions no trivials si, i només si, en té l'equació $aX^2 + b'Y^2 - Z^2 = 0$. Ara bé, $|b'| = \dfrac{|t^2 - a|}{|b|} \leq \dfrac{t^2 + |a|}{|b|} \leq \dfrac{(|b|/2)^2 + |a|}{|b|} \leq \dfrac{|b|}{4} + 1 < |b|$, ja que $|b| \geq 2$. Si escrivim $b' = u^2 b''$ amb b'' lliure de quadrats, encara obtenim la desigualtat $|b''| \leq |b'| < |b|$, de manera que $|a| + |b''| < |a| + |b| = m$; per hipòtesi d'inducció, només cal comprovar que els nous coeficients a, b'' satisfan les hipòtesis de la proposició. És a dir, cal comprovar que, si escrivim $d'' := \mathrm{mcd}(a, b'')$, aleshores a, b'' són enters lliures de quadrats, cosa que és clara, no tots dos negatius, i tals que a és un quadrat mòdul b'', b'' és un quadrat mòdul a, i $-ab''/(d'')^2$ és un quadrat mòdul d''.

De la igualtat $t^2 - a = bb''u^2$ es dedueix immediatament, d'una banda, que a és un quadrat mòdul b'' i, de l'altra, que si a és negatiu, aleshores b i b'' tenen el mateix signe; d'on, per hipòtesi, $b, b'' > 0$. Veiem, ara, que b'' és un quadrat mòdul a. Si p és un nombre primer que dividís alhora a i u, de la mateixa igualtat $t^2 - a = bb''u^2$ obtindríem que p^2 dividiria a; però a és lliure de quadrats. Per tant, $\mathrm{mcd}(a, u) = 1$ i podem escriure $bb'' \equiv (t/u)^2 \pmod{a}$; en particular, bb'' és també un quadrat mòdul a/d i, com que b ho és i $\mathrm{mcd}(b, a/d) = 1$, també b'' és un quadrat mòdul a/d. D'altra banda, com que d divideix a i b, de la igualtat $-abb''u^2 = -at^2 + a^2$ resulta que d^2 divideix at^2 i, com que a és lliure de quadrats, d divideix t; posem $t = dt'$ amb $t' \in \mathbb{Z}$. Obtenim la nova igualtat

$$-\frac{ab}{d^2} b''u^2 = -at'^2 + \left(\frac{a}{d}\right)^2,$$

d'on

$$-\frac{ab}{d^2} b''u^2 \equiv \left(\frac{a}{d}\right)^2 \pmod{d}.$$

Com que $\mathrm{mcd}(a, u) = 1$, també $\mathrm{mcd}(d, u) = 1$ i com que, per hipòtesi, $-ab/d^2$ és un quadrat mòdul d, resulta que b'' és un quadrat mòdul d. Finalment, com que a és lliure de quadrats, és $\mathrm{mcd}(d, a/d) = 1$ i, com que b'' és un quadrat mòdul a/d i mòdul d, també b'' és un quadrat mòdul a.

Només resta veure que $-ab''/(d'')^2$ és un quadrat mòdul d''. Anàlogament, de la igualtat $-abb''u^2 = -at^2 + a^2$, podem escriure $t = t''d''$ amb $t'' \in \mathbb{Z}$. Obtenim la igualtat

$$-\frac{ab''}{d''^2} bu^2 = -at''^2 + \left(\frac{a}{d''}\right)^2,$$

d'on

$$-\frac{ab''}{d''^2} bu^2 \equiv \left(\frac{a}{d''}\right)^2 \pmod{d''}.$$

Com que $\mathrm{mcd}(a, u) = 1$, també $\mathrm{mcd}(d'', u) = 1$ i podem escriure

$$-\frac{ab''}{d''^2} b \equiv \left(\frac{a}{d''u}\right)^2 \pmod{d''}.$$

Però si p és un primer que dividís alhora b i d'', de la igualtat $-abb''u^2 = -at''^2 d''^2 + a^2$ resulta que p^3 dividiria a^2, de manera que a no seria lliure de quadrats. Això ens permet dir que $\mathrm{mcd}(b, d'') = 1$ i, aleshores, $-ab''/d''^2$ és un quadrat mòdul d'', ja que b ho és perquè ho és mòdul a i a és un múltiple de d''. Això acaba la demostració. □

8.3 L'equació de Fermat per a exponent 3

En aquesta secció es tracta de provar que l'equació

$$X^3 + Y^3 = Z^3$$

no té solucions enteres no trivials; és a dir, tals que $XYZ \neq 0$.

Per a això, utilitzarem el mètode anomenat del descens així com el coneixement que tenim de l'aritmètica de l'anell dels enters del cos ciclotòmic de les arrels cúbiques de la unitat. De fet, provarem un resultat més general. Concretament, provarem el teorema següent.

Teorema 8.3.1. *Siguin ω una arrel cúbica primitiva de la unitat i $u \in \mathbb{Z}[\omega]$ un element invertible. Aleshores, no existeixen elements $x, y, z \in \mathbb{Z}[\omega]$ tals que $xyz \neq 0$ i $x^3+y^3 = uz^3$.*

Demostració: Farem la demostració del teorema en diverses etapes. Posem $\mathfrak{p}$ l'únic ideal primer de $\mathbb{Z}[\omega]$ que ramifica sobre $\mathbb{Z}$; això és, $\mathfrak{p}$ és l'ideal principal generat per l'element $1 - \omega$. En primer lloc, veiem que no hi ha solucions tals que $xyz \in \mathfrak{p}$ (primer cas).

Però, abans, observem que si $x \in \mathbb{Z}[\omega]$ i si $x - 1 \in \mathfrak{p}$, aleshores $x^3 - 1 \in \mathfrak{p}^4$. En efecte, si escrivim $x - 1 = t(1 - \omega)$ amb $t \in \mathbb{Z}[\omega]$, podem escriure la igualtat $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2) = t(1-\omega)(1+t)(1-\omega)(1+t+\omega)(1-\omega) = t(1+t)(1+t+\omega)(1-\omega)^3$. Com que $\mathbb{Z}[\omega]/\mathfrak{p} \cong \mathbb{Z}/3\mathbb{Z}$, algun dels elements $t, t+1, t+2$ és de l'ideal $\mathfrak{p}$; si $t, t+1 \notin \mathfrak{p}$, aleshores $t + 2 \in \mathfrak{p}$, de manera que $t + 1 + \omega = t + 2 - (1 - \omega) \in \mathfrak{p}$; per tant, obtenim que $x^3 - 1 = t(1 + t)(1 + t + \omega)(1 - \omega)^3 \in \mathfrak{p}^4$, com hem afirmat.

Provem ara el primer cas. Si suposem que tenim una solució x, y, z tal que $xyz \notin \mathfrak{p}$, aleshores ha de ser $x^3, y^3, z^3 \equiv \pm 1 \pmod{\mathfrak{p}^4}$, de manera que obtenim una igualtat

$$\pm 1 \pm 1 \equiv \pm u \pmod{\mathfrak{p}^4};$$

equivalentment, $u \equiv -2, 0, 2 \pmod{\mathfrak{p}^4}$. Però això no és veritat per a cap de les unitats de $\mathbb{Z}[\omega]$. En efecte, les unitats de $\mathbb{Z}[\omega]$ són els nombres $\pm 1, \pm\omega, \pm\omega^2$ i tots ells són ± 1 mòdul $\mathfrak{p}$; a més a més, $\omega - 2 = (\omega - 1) - 1 \notin \mathfrak{p}$, i $\omega + 2 = (\omega - 1) + 3 \notin \mathfrak{p}^2$, de manera que ni $\omega - 2$ ni $\omega + 2$ no pertanyen a $\mathfrak{p}^4$. Anàlogament, tampoc $\omega^2 - 2, \omega^2 + 2$ no pertanyen a $\mathfrak{p}^4$.

Seguidament, suposem que existeix una solució x, y, z tal que $z \in \mathfrak{p}$ i $\mathrm{mcd}(x, y) = 1$ (segon cas); això darrer té sentit ja que l'anell $\mathbb{Z}[\omega]$ és un anell principal. En aquesta situació, se satisfà que $z \in \mathfrak{p}^2$.

En efecte, de la igualtat $x^3 + y^3 = uz^3$ i dels fets que $z \in \mathfrak{p}$ i $\mathrm{mcd}(x, y) = 1$, resulta que $xy \notin \mathfrak{p}$. Igual que abans, obtenim una congruència

$$\pm 1 \pm 1 \equiv uz^3 \pmod{\mathfrak{p}^4}.$$

Com que $\pm 2 \notin \mathfrak{p}$ i $uz^3 \in \mathfrak{p}$, ha de ser $uz^3 \in \mathfrak{p}^4$, de manera que $z \in \mathfrak{p}^2$.

Seguidament anem a fer el pas de descens.

Lema 8.3.2. *Siguin $x, y, z, u \in \mathbb{Z}[\omega]$, i suposem que u és invertible, que $x^3 + y^3 = uz^3$, que $xy \notin \mathfrak{p}$, que $\mathrm{mcd}(x, y) = 1$, i que $z \in \mathfrak{p}^k - \mathfrak{p}^{k+1}$, per a algun $k \geq 2$. Aleshores, existeixen $x_1, y_1, z_1, u_1 \in \mathbb{Z}[\omega]$ que satisfan les mateixes condicions que els x, y, z, u, però $z_1 \in \mathfrak{p}^{k-1} - \mathfrak{p}^k$.*

DEMOSTRACIÓ: Podem escriure la igualtat $x^3+y^3=uz^3$ en la forma més convenient

$$(x+y)(x+\omega y)(x+\omega^2 y)=uz^3.$$

Com que $uz^3\in\mathfrak{p}^6$, algun dels elements $x+y$, $x+\omega y$, $x+\omega^2 y$, pertany a $\mathfrak{p}^2$. Si convé, podem canviar y per ωy o per $\omega^2 y$, de manera que puguem assegurar que $x+y\in\mathfrak{p}^2$. Però, aleshores, $x+\omega y$, $x+\omega^2 y\in\mathfrak{p}-\mathfrak{p}^2$, ja que $x+\omega y=x+y-(1-\omega)y$, i també $x+\omega^2 y=x+y-(1-\omega^2)y$. Si posem $k\geq 2$ l'exponent més gran tal que $z\in\mathfrak{p}^k$, aleshores, l'exponent més gran v tal que $x+y\in\mathfrak{p}^v$ és determinat per la igualtat $v+2=3k$. Ara, $\mathrm{mcd}(x+y,x+\omega y)=\mathrm{mcd}(x+y,x+\omega^2 y)=1-\omega$, ja que $\mathrm{mcd}(x,y)=1$. Per tant, podem factoritzar $x+y$, $x+\omega y$, $x+\omega^2 y$ en la forma

$$\begin{cases} x+y=w_1\alpha_1^3(1-\omega)^v, & \alpha_1\notin\mathfrak{p},\\ x+\omega y=w_2\alpha_2^3(1-\omega), & \alpha_2\notin\mathfrak{p},\\ x+\omega^2 y=w_3\alpha_3^3(1-\omega), & \alpha_3\notin\mathfrak{p},\end{cases}$$

on w_1,w_2,w_3 són unitats de $\mathbb{Z}[\omega]$; i se satisfà que, si $i\neq j$, aleshores $\mathrm{mcd}(\alpha_i,\alpha_j)=1$. Si ara tenim en compte que $1+\omega+\omega^2=0$, obtenim que

$$0=(x+y)+\omega(x+\omega y)+\omega^2(x+\omega^2 y)=w_1\alpha_1^3(1-\omega)^v+\omega w_2\alpha_2^3(1-\omega)+\omega^2 w_3\alpha_3^3(1-\omega).$$

I si dividim per $1-\omega$, obtenim la nova igualtat

$$0=w_1z_1^3+w_2\omega x_1^3+w_3\omega^2 y_1^3,$$

on escrivim $z_1:=\alpha_1(1-\omega)^{k-1}$, $x_1:=\alpha_2$, i $y_1:=\alpha_3$. I en dividir per $w_2\omega$, obtenim una igualtat

$$x_1^3+\varepsilon_1 y_1^3=\varepsilon_2 z_1^3,$$

en la qual ε_i són unitats de $\mathbb{Z}[\omega]$. Si mirem aquesta darrera equació mòdul $\mathfrak{p}^2$ i tenim en compte que $z_1\in\mathfrak{p}^3$ observarem que $\pm1\pm\varepsilon_1\in\mathfrak{p}^2$; però això implica, com abans, que $\varepsilon=\pm1$. D'aquesta manera, i si convé, canviant y_1 de signe, obtenim la igualtat

$$x_1^3+y_1^3=u_1z_1^3,$$

on $u_1:=\varepsilon_2$; com que la potència exacta de $\mathfrak{p}$ que conté z_1 és exactament $k-1$, hem acabat. □

Amb aquest resultat la demostració s'acaba fàcilment. En efecte, si tinguéssim una solució x,y,z tal que $xyz\neq0$, podem suposar que algun dels elements x,y,z no pertany a l'ideal principal $\mathfrak{p}$; si $x,y\notin\mathfrak{p}$, el lema anterior proporciona una contradicció; si $x\in\mathfrak{p}$ però $yz\notin\mathfrak{p}$, aleshores seria $u\equiv\pm1\pmod{\mathfrak{p}^2}$; però això implica que $u=\pm1$, ja que $\omega+1,\omega^2+1\notin\mathfrak{p}$ i $\omega-1,\omega^2-1\notin\mathfrak{p}^2$. En conseqüència, podem reescriure la solució en la forma $(\pm z)^3+(-y)^3=x^3$, amb $yz\notin\mathfrak{p}$, i $x\in\mathfrak{p}$. Ara, podem aplicar el pas de descens i arribem a contradicció. □

8.4 L'equació de Fermat per a exponent 4

Un dels mètodes que va usar Fermat en les seves recerques aritmètiques es coneix avui com el mètode del descens, o mètode del descens de Fermat, i ja l'hem fet servir per a la demostració del cas $n=3$ de l'equació de Fermat.

El mètode consisteix a fer una demostració per reducció a l'absurd, basada en la construcció d'una successió estrictament decreixent de nombres naturals. Usarem aquest mètode per a provar el cas $n = 4$ de l'equació de Fermat (cf. [Tra 1998]).

Proposició 8.4.1. *L'equació diofantina* $X^4+Y^4 = Z^2$ *no admet solucions enteres* (x, y, z) *tals que* $xyz \neq 0$.

Demostració: Suposem que (x, y, z) és una solució entera de l'equació $X^4+Y^4 = Z^2$, tal que $xyz \neq 0$. Si convé, canviem els signes, de manera que podem suposar que $x > 0$, $y > 0$, i $z > 0$. A més a més, si existeixen solucions, podem suposar que z és el menor nombre natural no nul per al qual existeixen nombres enters x, y tals que $x^4+y^4 = z^2$. Si és aquest el cas, se satisfà, a més a més, que $\mathrm{mcd}(x, y) = \mathrm{mcd}(x, z) = \mathrm{mcd}(y, z) = \mathrm{mcd}(x, y, z) = 1$. En efecte, si $d > 1$ és un divisor comú de x i de y, aleshores d^2 és un divisor de z; dividim x i y per d i z per d^2, i obtenim una nova solució positiva (x', y', z') tal que $0 < z' < z$. Anàlogament, si p és un divisor primer comú de x i de z (respectivament, de y i de z), aleshores p també divideix y (respectivament, p també divideix x) i p^2 divideix z, de manera que podem simplificar un factor p de x i de y i p^2 de z i obtenir una altra solució positiva amb un valor positiu i menor de la variable z, contràriament a l'elecció de la solució (x, y, z) com una de les que fan que z sigui el m¡nim possible entre els nombres enters estrictament positius.

Ara, observem que els nombres x^2, y^2 i z formen una terna pitagòrica primitiva i positiva, i podem suposar que y és parell (si convé, intercanviem els papers de x i de y); per tant, existeixen nombres enters $u > v > 0$ tals que $\mathrm{mcd}(u, v) = 1$, que $u \not\equiv v \pmod 2$, i que $x^2 = u^2 - v^2$, $y^2 = 2uv$, i $z = u^2 + v^2$ (cf. l'exercici **8.1.6**).

D'aquesta manera, obtenim que $u^2 = x^2 + v^2$, amb $\mathrm{mcd}(u, v) = 1$, i els tres nombres u, v, x són positius; és a dir, (x, v, u) també és una terna pitagòrica positiva i primitiva amb x senar i, en conseqüència, v és parell i u és senar. Això implica que existeixen nombres enters $a > b > 0$, amb $\mathrm{mcd}(a, b) = 1$ i $a \not\equiv b \pmod 2$, i tals que $x = a^2 - b^2$, $v = 2ab$ i $u = a^2 + b^2$. Ara, de la igualtat $y^2 = 2uv = 4uab$ i del fet que u, a, b són primers entre si dos a dos, obtenim que u, a, i b són quadrats. Ara bé, de la condició $z = u^2+v^2 > u^2 > u > \sqrt{u}$, veiem que se satisfà la igualtat $\sqrt{u}^2 = \sqrt{a}^4 + \sqrt{b}^4$, de manera que obtenim una solució entera de l'equació $X^4 + Y^4 = Z^2$ amb un valor menor de z. Aquesta contradicció acaba la prova del resultat. □

Corol·lari 8.4.2. *L'equació* $X^4 + Y^4 = Z^4$ *no té solucions enteres amb* $XYZ \neq 0$. □

8.5 El primer cas de l'equació de Fermat per a exponents regulars

La conjectura de Fermat, problema que encara era obert en la primera versió d'aquest curs, i que va ésser tancat per A. Wiles (cf. [Wi 1995]), consisteix a demostrar que donat un enter $n \geq 3$, l'equació

$$X^n + Y^n = Z^n$$

no té solucions enteres tals que $XYZ \neq 0$.

Hem provat aquesta conjectura per als casos $n = 3$ i $n = 4$; i és senzill demostrar que si la conjectura de Fermat se satisfà per a tot exponent primer senar $p \geq 5$, aleshores se

satisfà per a tot exponent $n \geq 3$. A més a més, donada una possible solució (x, y, z) amb $xyz \neq 0$, podem suposar que els nombres enters x, y, z són primers dos a dos.

Definició 8.5.1. S'anomena "primer cas del teorema de Fermat" l'enunciat següent:

Sigui $p \geq 5$ un nombre primer. Aleshores, no existeixen enters x, y, z, no nuls, no divisibles per p, primers dos a dos, i tals que $x^p + y^p = z^p$.

Per contra, si algun dels enters x, y, z és divisible per p, aleshores es pot suposar, canviant si convé algun signe, que p divideix z; i, en conseqüència, p no divideix ni x ni y. Aquest és el que se sol anomenar el "segon cas".

En aquesta secció es tracta de provar el primer cas del teorema de Fermat per a tot primer regular $p \geq 5$.

Definició 8.5.2. Siguin p un nombre primer senar i ζ una arrel primitiva p-èsima de la unitat. Es diu que p és un primer regular quan p no divideix h_p, el nombre de classes d'ideals de l'anell dels enters del cos ciclotòmic $\mathbb{Q}(\zeta)$ de les arrels p-èsimes de la unitat.

Amb aquesta definició, l'enunciat precís del resultat que volem provar és el següent.

Teorema 8.5.3 (Kummer)**.** *Sigui p un primer regular. Aleshores, l'equació*

$$X^p + Y^p = Z^p$$

no té solucions enteres (x, y, z) amb x, y, z no nuls, primers dos a dos, i tals que p no divideix el producte xyz.

Abans de procedir a la seva demostració convé establir, però, alguns resultats. Comencem per un resultat de Kummer relatiu a unitats del cos ciclotòmic $K := \mathbb{Q}(\zeta)$, on ζ és una arrel primitiva p-èsima de la unitat.

Lema 8.5.4 (Kummer)**.** *Siguin $K^+ := \mathbb{Q}(\zeta+\zeta^{-1})$ el subcòs real maximal de K, $A := \mathbb{Z}[\zeta]$ l'anell dels enters de K, i A^+ l'anell dels enters de K^+. Aleshores, tota unitat de A és el producte d'una unitat de A^+ per una arrel p-èsima de la unitat.*

Demostració: Considerem K com a subcòs de $\mathbb{C}$ i suposem que u és un element invertible de A. Com que la conjugació complexa és un automorfisme de A, el nombre complex $v := u/\overline{u}$, on $\overline{u}$ designa el complex conjugat de u, és un nombre complex de mòdul 1; a més a més, com que el grup de Galois $\mathrm{Gal}\,(K|\mathbb{Q})$ és commutatiu, per a tot automorfisme σ de K l'element $\sigma(v)$ també és un nombre complex de mòdul 1. D'altra banda, com que u és invertible, també $\overline{u}$ és un element invertible de A, de manera que $v \in A$. Així, l'enter algebraic v té tots els seus conjugats de mòdul 1; això ens permet assegurar que v és una arrel de la unitat; com que les úniques arrels de la unitat de K són les arrels $2p$-èsimes, v és una arrel $2p$-èsima de la unitat i, en conseqüència, de la forma $\pm\zeta^k$, amb k enter; i com que l'ordre p de ζ és senar, podem suposar que $k = 2r$ és un enter parell. Es tracta de veure que $v = \zeta^k$; és a dir, que val el signe positiu. Per a veure això, podem escriure u en la forma

$$u = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2},$$

amb $a_i \in \mathbb{Z}$; aleshores, $u \equiv \overline{u} \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{(1-\zeta)}$, l'únic ideal primer de A que divideix p. Si fos $v = -\zeta^k$, aleshores obtindríem la congruència $\overline{u} \equiv -\overline{u} \pmod{(1-\zeta)}$; com que $2 \notin (1-\zeta)A$, això contradiria el fet que u és unitat.

Per tant, $u = \zeta^{2r}\overline{u}$; si posem $u^+ := \zeta^{-r}u$, aleshores és $\overline{u^+} = \zeta^r\overline{u} = u^+$, de manera que $u^+ \in A \cap \mathbb{R} = A^+$. Així, u és el producte d'una arrel de la unitat, ζ^r, per una unitat u^+ de A^+, i això acaba la demostració. □

Lema 8.5.5 (Kummer)**.** *Siguin p un nombre primer senar, ζ una arrel primitiva p-èsima de la unitat, i $A := \mathbb{Z}[\zeta]$ l'anell dels enters del cos ciclotòmic $\mathbb{Q}(\zeta)$. Suposem que x, y, z són enters no nuls, no divisibles per p, coprimers dos a dos, i tals que $x^p + y^p = z^p$. Aleshores, per a tota parella (i, j) d'enters diferents mòdul p els ideals principals $(x+\zeta^i y)$ i $(x + \zeta^j y)$ de l'anell A són primers entre si.*

Demostració: Posem $\mathfrak{p} := (1 - \zeta)$, l'únic ideal primer de A que divideix p, i suposem que $\mathfrak{q} \subseteq A$ és un ideal primer de A que divideix alhora els ideals $(x + \zeta^i y)$ i $(x + \zeta^j y)$. Aleshores, $\mathfrak{q}$ divideix l'ideal $((\zeta^i-\zeta^j)y)$, de manera que $\mathfrak{q}$ divideix yA o bé $\mathfrak{q}$ divideix l'ideal $(\zeta^i-\zeta^j) = (1-\zeta) = \mathfrak{p}$, ja que $i \not\equiv j \pmod p$. Anàlogament, com que $(x+\zeta^i y) = (y+\zeta^{-i}x)$ i $(x + \zeta^j y) = (y + \zeta^{-j}x)$, $\mathfrak{q}$ divideix xA o bé $\mathfrak{q}$ divideix $\mathfrak{p}$. Com que els enters x, y són primers entre si, els ideals xA, yA també són primers entre si en A; això implica que $\mathfrak{q} = \mathfrak{p}$. En conseqüència, de la congruència $x+y \equiv x+\zeta^i y \pmod{\mathfrak{p}}$ i del fet que $x+y \in \mathbb{Z}$ s'obté que $x+y$ és divisible pel primer de $\mathbb{Z}$ que $\mathfrak{p}$ divideix; és a dir, p divideix $x+y$. Ara, de la igualtat $x^p + y^p = z^p$ i del fet que $x + y$ divideix $x^p + y^p$ es dedueix que p divideix z, contra la hipòtesi. Per tant, els ideals $(x + \zeta^i y)$, $(x + \zeta^j y)$ són primers entre si. □

Anem a procedir, ara, a la demostració del teorema. Com que el cas $p = 3$ ja ha estat provat, i no només el primer cas, podem suposar que $p \geq 5$. Suposem, doncs, que $p \geq 5$ és un primer regular i que x, y, z són enters no divisibles per p, primers dos a dos, i tals que $x^p + y^p = z^p$.

Si suposem que $x \equiv y \equiv -z \pmod p$, aleshores obtenim que $z^p = x^p + y^p \equiv -2z^p$, de manera que p divideix $3z$, absurd; per tant, dos dels tres nombres $x, y, -z$ no són congrus mòdul p; intercanviant, si convé, $-z$ amb x o y, podem suposar que $x \not\equiv y \pmod p$. Aquesta hipòtesi serà important en el que segueix.

De la igualtat $x^p + y^p = z^p$, obtenim, en A, la igualtat

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

per tant, la igualtat d'ideals de A

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

Ara bé, com que els ideals $(x+\zeta^i y)$ són primers entre si, cadascun d'aquests ideals és una potència p-èsima; és a dir, existeixen ideals $\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_{p-1}$ de A tals que $(x + \zeta^i y) = \mathfrak{a}_i^p$, $0 \leq i \leq p - 1$.

Ara utilitzarem la hipòtesi que el primer p és regular. Per a tot índex i l'ideal $\mathfrak{a}_i^p$ és principal; és a dir, $\mathfrak{a}_i$ és un element d'ordre divisor de p en el grup de classes d'ideals de A; com que p no divideix l'ordre d'aquest grup, $\mathfrak{a}_i$ ha de ser un ideal principal. Per tant, podem trobar un element $\alpha_i \in A$ tal que $\mathfrak{a}_i = \alpha_i A$; i aleshores, obtenim la igualtat $(x+\zeta^i y) = (\alpha_i^p)$; dit d'una altra manera, existeix una unitat $\varepsilon_i \in A^*$ tal que $x+\zeta^i y = \varepsilon_i \alpha_i^p$. Fixem-nos en l'índex $i = 1$: com que tota unitat de A és el producte d'una unitat real per

una arrel p-èsima de la unitat, podem escriure una igualtat de la forma $x + \zeta y = \zeta^r u \alpha^p$, amb $u \in A^+$, invertible, $\alpha \in A$, i r enter.

Ara convé observar el fet que, donat un element $\alpha \in A$, arbitrari, existeix un enter $a \in \mathbb{Z}$ tal que $\alpha^p - a \in pA$; en efecte, si escrivim $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, amb $a_i \in \mathbb{Z}$, i després elevem a la potència p-èsima, obtenim que $\alpha^p - \sum_{i=0}^{p-2} a_i^p \in pA$, ja que $\zeta^p = 1$. A més a més, si $\overline{\alpha}$ és el complex conjugat de α, també $\overline{\alpha}^p - a \in pA$, ja que $\overline{\alpha} = \sum_{i=0}^{p-2} a_i \zeta^{-i}$.

D'aquesta manera, obtenim congruències de la forma

$$\begin{aligned} x + \zeta y = \zeta^r u \alpha^p &\equiv \zeta^r u a \pmod{pA} \\ x + \zeta^{-1} y = \zeta^{-r} u \overline{\alpha}^p &\equiv \zeta^{-r} u a \pmod{pA}, \end{aligned}$$

amb $a \in \mathbb{Z}$, ja que $u \in A^+$. Si multipliquem la primera per ζ^{-r} i la segona per ζ^r, obtenim la congruència $\zeta^{-r}(x + \zeta y) \equiv ua \equiv \zeta^r(x + \zeta^{-1} y) \pmod{pA}$, que es pot escriure, després de multiplicar per ζ^r, en la forma $x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \in pA$. Es tracta de veure que aquesta condició duu a contradicció.

Per a això, notem que tot subconjunt de $p-1$ elements del conjunt $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ és una $\mathbb{Z}$-base de l'anell dels enters A de $\mathbb{Q}(\zeta)$. Per tant, si un element de pA és combinació lineal de coeficients enters de $p-1$ d'aquests elements, aleshores tots els coeficients són divisibles per p en $\mathbb{Z}$.

Si apliquem aquesta observació al nostre cas, com que $p \geq 5$ i com que x, y són enters no divisibles per p, dues de les arrels de la unitat $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ han de coincidir. Distingim casos: com que $\zeta \neq 1$, queden les possibilitats $\zeta^{2r} = 1$, $\zeta^{2r-1} = 1$, $\zeta^{2r-2} = 1$.

Primer cas: $\zeta^{2r} = 1$. Aleshores, $y(\zeta - \zeta^{-1}) \in pA$, absurd.

Segon cas: $\zeta^{2r-1} = 1$. En aquest cas, $(x - y)(1 - \zeta) \in pA = \mathfrak{p}^{p-1}$; per tant, $x - y \in \mathfrak{p}^{p-2}$; com que $x - y \in \mathbb{Z}$, ha de ser $x - y \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, contra la hipòtesi que $x \not\equiv y \pmod{p}$.

Tercer cas: $\zeta^{2r-2} = 1$. Aleshores, $x(1 - \zeta^2) \in pA$, de manera que $x \in \mathfrak{p}^{p-3} \cap \mathbb{Z} = p\mathbb{Z}$, contra la hipòtesi que p no divideix xyz.

Això acaba la demostració del primer cas del teorema de Fermat per a primers regulars $p \geq 5$. $\square$

Capítol 9

Anàlisi p-àdica

Per a fer anàlisi, molt sovint és més còmode situar-se en el cos $\mathbb{C}$ que en el cos $\mathbb{R}$. Això és conseqüència del fet que encara que $\mathbb{R}$ és complet, no és algebraicament tancat; en canvi, $\mathbb{C}$, a més a més de ser complet, és algebraicament tancat.

En aquesta segona part del curs, ens interessarà fer anàlisi no només real; sinó, a més a més, anàlisi p-àdica. Cal, doncs, introduir aquesta anàlisi. Després de construir els cossos dels nombres p-àdics, i de provar que són complets, resultarà que no són algebraicament tancats; i, aleshores, podrem considerar la seva clausura algebraica. Però, ai las!, aquesta clausura algebraica no és un cos complet. I ara, un cop considerem la seva compleció, en resulta un cos complet i també algebraicament tancat. I és en aquest cos on serà còmode estudiar funcions i fer anàlisi.

En la primera part del curs, doncs, s'ha evitat parlar dels nombres p-àdics, enters o racionals, d'anells de valoració discreta, d'anells complets, de valoracions, o de complecions de cossos valorats; L'estudi d'aquests objectes i d'aquestes nocions és el que ens ocuparà en aquest capítol.

9.1 Valoracions

Aquesta secció es dedica a la introducció i l'estudi bàsic de les nocions de valoració i d'anell de valoració per a un cos arbitrari.

Definició 9.1.1. Siguin K un cos i Γ un grup abelià totalment ordenat per una relació que denotem per $\leq$. Una aplicació $v : K^* \longrightarrow \Gamma$ s'anomena una valoració de K en Γ quan per a tota parella d'elements $x, y \in K^*$ tals que $x + y \neq 0$ se satisfan les propietats següents:

(a) $v(xy) = v(x) + v(y)$; i

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

Sovint convé pensar l'aplicació estesa a tot el cos K escrivint $v(0) := +\infty$; aquesta extensió és compatible amb els axiomes (a), (b) i les regles habituals de treball amb un element $+\infty$: per a tot element $\gamma \in \Gamma$,

$$+\infty + (+\infty) = +\infty, \qquad \gamma + (+\infty) = +\infty, \qquad +\infty \geq \gamma.$$

La imatge de l'aplicació v és un subgrup totalment ordenat de Γ; s'anomena el grup de valors de la valoració v. A fi de posar de manifest el grup de valors en la definició, s'acostuma a demanar que l'aplicació v sigui exhaustiva; en aquest cas, es diu que v és una valoració de K de grup de valors Γ.

Exemple 9.1.2. Donat un cos qualsevol, K, la valoració trivial és la valoració v definida per $v(x) = 0$, per a tot element $x \neq 0$ de K i $v(0) = +\infty$.

Proposició 9.1.3. *Siguin K un cos i $v : K \longrightarrow \Gamma \cup \{+\infty\}$ una valoració qualsevol de K. El conjunt $A_v := \{x \in K : v(x) \geq 0\}$ és un subanell de K, local, i amb ideal maximal $\mathfrak{P}_v := \{x \in K : v(x) > 0\}$; a més a més, K és el cos de fraccions de A_v.*

Demostració: És clar que A_v és un anell i que $\mathfrak{P}_v$ és un ideal de A_v. Per a veure que A_v és local i que $\mathfrak{P}_v$ és el seu ideal maximal és suficient veure que el complementari $A_v - \mathfrak{P}_v$, el conjunt dels elements $x \in A_v$ tals que $v(x) = 0$, és exactament el grup multiplicatiu dels elements invertibles de A_v. Ara bé, si $u \in A_v$ és un element invertible, aleshores se satisfà la igualtat $v(1) = v(u) + v(u^{-1})$; però $v(1) = v(1) + v(1)$, de manera que $v(1) = 0$ i, com que $v(u), v(u^{-1}) \geq 0$ per hipòtesi, ha de ser $v(u) = v(u^{-1}) = 0$. Recíprocament, si $u \in K$ és tal que $v(u) = 0$, aleshores, de $0 = v(1) = v(u) + v(u^{-1})$ és $v(u^{-1}) = 0$, de manera que $u^{-1} \in A_v$ i u és invertible en A_v. Finalment, suposem que $x \in K$ i $x \notin A_v$; això ens permet dir que $v(x) < 0$, de manera que $v(x^{-1}) > 0$ i, en conseqüència, $x^{-1} \in A_v$; aleshores, $x = \dfrac{1}{x^{-1}}$ pertany al cos de fraccions de A_v. $\square$

Definició 9.1.4. L'anell A_v s'anomena l'anell de la valoració. L'ideal $\mathfrak{P}_v \subseteq A_v$ s'anomena l'ideal de la valoració.

La caracterització següent dels anells de valoració serà útil.

Proposició 9.1.5. *Sigui A un domini d'integritat. Condició necessària i suficient perquè A sigui un anell de valoració és que per a tot element no nul x del cos de fraccions K de A sigui $x \in A$ o bé $x^{-1} \in A$.*

Demostració: Si A és l'anell de valoració associat a una valoració v del seu cos de fraccions, de la igualtat $v(x) + v(x^{-1}) = v(1) = 0$ es dedueix que $x \in A$ o $x^{-1} \in A$, ja que alguna de les dues valoracions és no negativa.

Recíprocament, suposem que A satisfà la propietat de l'enunciat i considerem la projecció natural $v : K^* \longrightarrow K^*/A^*$, on A^* designa el grup dels elements invertibles de A. Clarament se satisfà la propietat multiplicativa $v(xy) = v(x)v(y)$, per a $x, y \in K^*$. D'altra banda, podem definir en el quocient $\Gamma := K^*/A^*$ una estructura de grup totalment ordenat per la fórmula $v(x) \leq v(y) \iff yx^{-1} \in A$. En efecte, la definició no depèn dels representants elegits, ja que dos representants d'un mateix element del quocient coincideixen mòdul el producte per un element invertible de A; a més a més, la relació és trivialment reflexiva i transitiva; també és antisimètrica, ja que de $yx^{-1}, xy^{-1} \in A$ es dedueix que yx^{-1} és invertible en A i, per tant, $v(y) = v(x)$; i, finalment, donats elements $x, y \in K^*$, és $xy^{-1} \in A$ o bé $yx^{-1} = (xy^{-1})^{-1} \in A$, de manera que $v(y) \leq v(x)$ o bé $v(x) \leq v(y)$. Per tant, $\leq$ és una relació d'ordre total en Γ. Resta veure que la relació $\leq$ és compatible amb l'estructura de grup de Γ i que l'aplicació v satisfà el segon axioma de valoració. La primera d'aquestes dues propietats és trivial, ja que $(yz)(xz)^{-1} = yx^{-1}$, de manera que $v(x) \leq v(y)$ equival a $v(xz) \leq v(yz)$. Finalment, si suposem que $x, y, x + y \in K^*$ i que

$v(x) \leq v(y)$, cal veure que $v(x+y) \geq v(x) = \min(v(x), v(y))$; però dir que $v(x) \leq v(y)$ és dir que $yx^{-1} \in A$, de manera que $(x+y)x^{-1} = 1 + yx^{-1} \in A$ i, per tant, $v(x) \leq v(x+y)$, com volíem veure. □

Definició 9.1.6. Una valoració v s'anomena real quan el grup de valors és isomorf, com a grup ordenat, a un subgrup del grup additiu dels nombres reals; s'anomena discreta quan el grup de valors és un grup isomorf, com a grup ordenat, al grup additiu $\mathbb{Z}$. Si v és una valoració discreta es diu que A_v és un anell de valoració discreta.

Exemple 9.1.7. Siguin A un anell de Dedekind, K el seu cos de fraccions i $\mathfrak{p} \subseteq A$ un ideal primer no nul. Donat un element no nul $x \in K$ l'ideal fraccionari xA admet una descomposició única com a producte d'ideals primers; sigui $v_{\mathfrak{p}}(x)$ l'exponent amb què apareix l'ideal $\mathfrak{p}$ en aquesta descomposició. D'aquesta manera es defineix una valoració $v_{\mathfrak{p}}$ de K que té grup de valors el grup additiu $\mathbb{Z}$ dels nombres enters. És, per tant, una valoració discreta; s'anomena la valoració $\mathfrak{p}$-àdica de K.

En particular, per a cada nombre primer p disposem d'una valoració de $\mathbb{Q}$; la valoració p-àdica. Anàlogament, si K és un cos de nombres i $\mathfrak{p}$ és un ideal primer no nul del seu anell d'enters, disposem en K de la valoració $\mathfrak{p}$-àdica. Són valoracions discretes.

Ens interessa, doncs, estudiar els anells de valoració discreta.

Proposició 9.1.8. *Sigui A l'anell de valoració associat a una valoració discreta del seu cos de fraccions, $v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$. Aleshores, A és un domini local principal.*

Demostració: Només cal veure que A és principal. Però si $\mathfrak{a} \subseteq A$ és un ideal no nul qualsevol, podem elegir un element no nul $a \in \mathfrak{a}$ de valoració mínima, ja que el conjunt dels valors dels elements de A és un subconjunt de $\mathbb{N} \cup \{+\infty\}$; aleshores, per a tot element $b \in \mathfrak{a}$, ba^{-1} és un element de valoració no negativa de K, de manera que $ba^{-1} \in A$; per tant, $b = a(ba^{-1}) \in aA$; és a dir, $\mathfrak{a} = aA$. □

Corol·lari 9.1.9. *Els anells de valoració discreta són anells de Dedekind locals.*

Demostració: En efecte, tot anell principal és un anell de Dedekind. □

Proposició 9.1.10. *Recíprocament, siguin A un anell de Dedekind local, $\mathfrak{p}$ el seu ideal maximal, i v la valoració $\mathfrak{p}$-àdica del seu cos de fraccions, definida més amunt. Aleshores, $A = A_v$; és a dir, A és un anell de valoració discreta.*

Demostració: Siguin K el cos de fraccions de A i $x \in K$ un element no nul qualsevol. Com que els únics ideals fraccionaris no nuls de A són les potències de $\mathfrak{p}$, dir que $x \in A$ equival a dir que l'ideal fraccionari xA és enter; és a dir, que xA és una potència no negativa de $\mathfrak{p}$; i això és el mateix que dir que $v(x) \geq 0$ o, equivalentment, que $x \in A_v$. □

9.2 Valor absoluts

Una eina que ja s'ha demostrat útil en la primera part del curs és la noció de valor absolut; per exemple, per a tota la part de geometria dels nombres.

En efecte, en aquell context, només hem utilitzat el valor absolut usual de $\mathbb{R}$ i de $\mathbb{C}$, el fet que $\mathbb{R}$ i $\mathbb{C}$ són complets per a la topologia definida pel seu valor absolut, i hem utilitzat eines de l'anàlisi matemàtica sobre $\mathbb{R}$ i sobre $\mathbb{C}$.

Ara convé fer-ne un estudi més sistemàtic i estendre les nocions a fi de poder fer anàlisi p-àdica.

Definició 9.2.1. Sigui K un cos. Una aplicació $|\ | : K \longrightarrow \mathbb{R}$ s'anomena un valor absolut de K si per a tota parella d'elements $x, y \in K$ se satisfan les propietas següents:

(a) $|x| \geq 0$;

(b) $|x| = 0 \Longleftrightarrow x = 0$;

(c) $|xy| = |x||y|$; i

(d) (Desigualtat triangular) $|x + y| \leq |x| + |y|$.

Si, a més a més, se satisfà la propietat, més forta que (d),

(d') (Desigualtat ultramètrica) $|x + y| \leq \max(|x|, |y|)$,
es diu que el valor absolut és no arquimedià o ultramètric; en cas contrari, el valor absolut s'anomena arquimedià o no ultramètric.

Observació 9.2.2. Com que $|1| = |1 \cdot 1| = |1||1|$ i $1 \neq 0$, és $|1| \neq 0$, de manera que $|1| = 1$.

Exemple 9.2.3. El valor absolut trivial es defineix en qualsevol cos K per les fórmules $|0| = 0$ i $|x| = 1$ per a tot $x \neq 0$. És un valor absolut ultramètric.

Exemple 9.2.4. Si $K \subseteq \mathbb{C}$ és un subcòs qualsevol, la restricció a K del valor absolut de $\mathbb{C}$ és un valor absolut arquimedià de K.

En particular, si K és un cos de nombres i $\sigma : K \longrightarrow \mathbb{C}$ és una immersió complexa de K, obtenim un valor absolut arquimedià de K per la fórmula $|x|_\sigma := |\sigma(x)|$. Si designem com és habitual el nombre complex conjugat d'un nombre complex α amb el símbol $\overline{\alpha}$, podem escriure $|x|_\sigma^2 = \sigma(x)\overline{\sigma(x)}$; en particular, si $\overline{\sigma}$ és la immersió complexa conjugada de σ, se satisfà la igualtat de valors absoluts $|\ |_\sigma = |\ |_{\overline{\sigma}}$.

El resultat següent és un criteri per a decidir quan un valor absolut és o no arquimedià.

Lema 9.2.5. *Condició necessària i suficient perquè un valor absolut d'un cos K sigui no arquimedià és que el conjunt format pels valors absoluts $|n|$, $n \in \mathbb{Z}$, sigui fitat.*

Demostració: En efecte, si $|\ |$ és un valor absolut no arquimedià d'un cos K, aleshores, per a tot enter n, se satisfà $|n| = |1 + \cdots + 1| \leq |1|$, de manera que $|1|$ és la fita desitjada.

Recíprocament, per a tot enter $k \geq 1$, i per a tota parella d'elements $x, y \in K$, la fórmula del binomi i la desigualtat triangular ens permeten escriure que

$$|x + y|^k \leq \sum_{j=0}^{k} \left| \binom{k}{j} \right| |x|^j |y|^{k-j}.$$

Ara, $|x|^j|y|^{k-j} \leq \max(|x|,|y|)^k$; com que els nombres combinatoris són enters, obtenim una desigualtat

$$|x+y|^k \leq C(k+1)\max(|x|,|y|)^k,$$

on C és una fita dels valors absoluts dels enters; aquesta desigualtat la podem escriure en la forma

$$|x+y| \leq C^{1/k}(k+1)^{1/k}\max(|x|,|y|);$$

com que la desigualtat és vàlida per a tot enter $k \geq 1$, podem passar al límit i, com que $\lim C^{1/k}(k+1)^{1/k} = 1$, obtenim la desigualtat que volíem

$$|x+y| \leq \max(|x|,|y|). \ \square$$

Una manera natural d'obtenir valors absoluts en un cos és a partir de valoracions reals. Siguin K un cos i $v : K^* \longrightarrow \mathbb{R} \cup \{+\infty\}$ una valoració real de K. Per a tot nombre real $c > 1$ podem considerar l'aplicació $|\ |_v : K \longrightarrow \mathbb{R}$ definida per $|x|_v := c^{-v(x)}$. Aleshores, $|\ |_v$ és un valor absolut del cos K. S'anomena un valor absolut associat a la valoració v. Clarament, l'anell de la valoració A_v coincideix amb el conjunt dels elements $x \in K$ tals que $|x|_v \leq 1$ i l'ideal de la valoració amb el conjunt dels elements $x \in K$ tals que $|x|_v < 1$.

Exemple 9.2.6. Si considerem el cos $\mathbb{Q}$ dels nombres racionals, disposem, doncs, d'una gran quantitat de valors absoluts: d'una banda, el valor absolut usual $|x| := \max(x,-x)$, que denotarem sovint per $|x|_\infty$; de l'altra, d'una família doblement infinita de valors absoluts $|\ |_p$, associats a cada nombre primer p i a cada nombre real $c > 1$: els valors absoluts $|x|_p := c^{-v_p(x)}$ associats a la valoració p-àdica v_p de $\mathbb{Q}$.

Anàlogament, si K és un cos extensió finita de $\mathbb{Q}$, disposem de tots els valors absoluts $\mathfrak{p}$-àdics, associats als ideals primers no nuls, $\mathfrak{p}$, de l'anell dels enters de K, i dels valors absoluts arquimedians, $|\ |_\sigma$, associats a les diferents immersions complexes, σ, de K.

Ens proposem veure que aquests són, essencialment, tots els valors absoluts dels cossos de nombres. Caldrà, però, treballar una mica. En particular, cal donar un significat precís a l'adverbi **essencialment**.

Lema 9.2.7. *Siguin $|\ |$ un valor absolut d'un cos K i r un nombre real, $0 < r < 1$. Aleshores, l'aplicació definida en K per l'assignació $x \mapsto |x|^r$ també és un valor absolut de K.*

Demostració: Fixat un nombre real positiu x, considerem la funció g definida per a tot nombre real positiu r per la fórmula $g(r) := (1+x^r)^{1/r}$. La derivada d'aquesta funció admet l'expressió

$$r^2 g'(r) = (1+x^r)^{\frac{1-r}{r}}\left(x^r \log x^r - (1+x^r)\log(1+x^r)\right).$$

D'altra banda, la funció h definida per la fórmula $h(x) := x\log x$, per a tot nombre real $x > 1$, és estrictament creixent; i per a tota parella de nombres reals positius x, r se satisfà la desigualtat $x^r \log x^r - (1+x^r)\log(1+x^r) < 0$. En conseqüència, per a tot nombre real positiu x, la derivada de g és estrictament negativa en tot punt r i la funció g és decreixent. Per tant, per a tot nombre real positiu x i tot nombre real r tal que $0 < r < 1$ se satisfà la desigualtat $(1+x^r)^{1/r} > (1+x)$; o equivalentment, $(1+x^r) > (1+x)^r$.

Siguin, ara, $\beta, \gamma \in K$, $\beta, \gamma \neq 0$, i posem $b := |\beta|, c := |\gamma|$. Si fem $x := c/b$, substituïm a la desigualtat anterior, i multipliquem per b^r, obtenim la desigualtat $b^r + c^r > (b+c)^r$; és

a dir, $|\beta+\gamma|^r \leq (|\beta|+|\gamma|)^r < |\beta|^r + |\gamma|^r$. Això és suficient per a demostrar la desigualtat triangular per a la funció $|\ |^r$. Les altres tres propietats de valor absolut són immediates. □

Aquest resultat suggereix la definició següent.

Definició 9.2.8. Dos valors absoluts d'un mateix cos K, $|\ |_1$, $|\ |_2$, s'anomenen equivalents quan per a tot element $x \in K$ les condicions $|x|_1 < 1$ i $|x|_2 < 1$ són equivalents.

En particular, per a tot nombre real positiu $r \leq 1$, els valors absoluts $|\ |$ i $|\ |^r$ són equivalents.

Exercici 9.2.9. L'únic valor absolut equivalent al valor absolut trivial és el trivial.

Exemple 9.2.10. Siguin p un nombre primer i c_1, c_2 nombres reals $c_1, c_2 > 1$; aleshores, els valors absoluts p-àdics definits per a tot nombre racional x per les fórmules $c_i^{-v_p(x)}$, $i = 1, 2$, són equivalents.

Proposició 9.2.11. *Siguin $|\ |_1$, $|\ |_2$, dos valors absoluts equivalents i no trivials d'un cos K. Aleshores, existeix un nombre real $r > 0$ tal que per a tot $x \in K$ és $|x|_2 = |x|_1^r$*

Demostració: Com que els valors absoluts són no trivials, podem trobar un element $x_0 \in K$ tal que $|x_0|_1 > 1$. Sigui r el nombre real definit per la igualtat $|x_0|_2 = |x_0|_1^r$; com que $|x_0|_2 > 1$, ja que $|\ |_2$ és equivalent a $|\ |_1$, obtenim que $r > 0$. Es tracta de veure que per a tot element $x \in K$ se satisfà la igualtat $|x|_2 = |x|_1^r$. Sigui, doncs, $x \in K$ un element no nul; podem escriure $|x|_1 = |x_0|_1^s$ per a un cert nombre real s i elegir dues successions de nombres enters, $\{m_i\}_i$, $\{n_i\}_i$, amb $n_i > 0$, tals que $s = \lim m_i/n_i$ i $m_i/n_i > s$ per a tot índex i. Aleshores, podem escriure que $|x|_1 = |x_0|_1^s < |x_0|_1^{m_i/n_i}$, ja que $|x_0|_1 > 1$; d'aquí, en elevar a n_i, es dedueix que $|x^{n_i}/x_0^{m_i}|_1 < 1$. Com que tots dos valors absoluts són equivalents, obtenim la desigualtat $|x^{n_i}/x_0^{m_i}|_2 < 1$, que implica la relació $|x|_2 < |x_0|_2^{m_i/n_i}$; i, en passar al límit, tenim que $|x|_2 \leq |x_0|_2^s$.

Si repetim l'argument amb successions $\{m_i\}_i$, $\{n_i\}_i$, amb $n_i > 0$, tals que $s = \lim m_i/n_i$ però $m_i/n_i < s$ per a tot índex i, obtenim la desigualtat contrària $|x|_2 \geq |x_0|_2^s$; per tant, la igualtat $|x|_2 = |x_0|_2^s$. En conseqüència, $|x|_2 = |x_0|_2^s = |x_0|_1^{rs} = |x|_1^r$, per a tot element no nul $x \in K$, com volíem demostrar. □

Observem que tot valor absolut $|\ |$ d'un cos K ens permet definir una distància en K per la fórmula $d(x, y) := |y - x|$; en conseqüència, una topologia en K compatible amb l'estructura de cos. És a dir, K té una estructura de cos topològic associada de manera natural a cada valor absolut. La proposició anterior ens ensenya que dos valors absoluts són equivalents quan defineixen la mateixa topologia. En efecte, els subconjunts de K formats pels elements x tals que $|x| < \varepsilon$ formen una base d'entorns oberts de zero; i la proposició anterior ens permet assegurar que aquesta base d'entorns ho és tant per a un valor absolut com per a l'altre.

9.3 Valors absoluts de Q. Fórmula del producte

En aquesta secció es tracta de determinar tots els valors absoluts no equivalents de $\mathbb{Q}$. Recordem que disposem del valor absolut trivial, del valor absolut arquimedià usual, $|x|_\infty := \max(x, -x)$, i, per a tot nombre natural primer p, d'un valor absolut no arquimedià que podem definir, llevat d'equivalència, per la fórmula $|x|_p := p^{-v_p(x)}$.

Lema 9.3.1. *Els valors absoluts* $|\ |_\infty$, $|\ |_p$, *p primer, són no equivalents dos a dos.*

Demostració: Com que $|\ |_\infty$ és arquimedià i $|\ |_p$ és no arquimedià per a tot nombre primer p, només cal veure que si $p \neq \ell$ són nombres primers diferents, aleshores, $|\ |_p$ i $|\ |_\ell$ són no equivalents. Però això és clar, ja que $|p|_p = 1/p < 1$ i, en canvi, $|p|_\ell = 1 \geq 1$. □

Teorema 9.3.2. *Tot valor absolut arquimedià de* $\mathbb{Q}$ *és equivalent a* $|\ |_\infty$. *Tot valor absolut no trivial i no arquimedià de* $\mathbb{Q}$ *és equivalent a un dels valors absoluts p-àdics* $|\ |_p$, *p primer.*

Demostració: Sigui $|\ |$ un valor absolut no trivial de $\mathbb{Q}$. Donats $m, n \in \mathbb{Z}$, $m, n > 1$, podem escriure m en base n; és a dir, si r és el nombre natural tal que $n^r \leq m < n^{r+1}$, aleshores existeixen nombres enters $a_i \in \{0, 1, \ldots, n-1\}$, $0 \leq i \leq r$, $a_r \neq 0$, únics tals que

$$m = \sum_{i=0}^{r} a_i n^i.$$

En aquesta situació, la desigualtat triangular ens permet escriure que

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq \sum_{i=0}^{r} |a_i| \max(1, |n|)^i \leq \sum_{i=0}^{r} |a_i| \max(1, |n|)^r$$

i també que $|a_i| = |1 + \cdots + 1| \leq a_i|1| < n|1| = n$, ja que $|1| = 1$; per tant,

$$|m| \leq \left(1 + \frac{\log m}{\log n}\right) n \max(1, |n|)^{\log m/\log n},$$

ja que hi ha $r + 1$ sumands i se satisfà la desigualtat $r \leq \log m/\log n$. En canviar m per m^k per a qualsevol enter $k > 0$, i elevar a $1/k$, obtenim la desigualtat

$$|m| \leq \left(1 + k\frac{\log m}{\log n}\right)^{1/k} n^{1/k} \max(1, |n|)^{\log m/\log n}$$

i, en prendre límit,

$$|m| \leq \max(1, |n|)^{\log m/\log n}, \tag{9.3.1}$$

per a tota parella de nombres enters $m, n > 1$. Ara distingirem dos casos.

Primer cas: per a tot nombre enter $n > 1$ és $|n| > 1$.

La desigualtat (9.3.1) es pot llegir en la forma $|m|^{1/\log m} \leq |n|^{1/\log n}$. En intercanviar n i m, obtenim la desigualtat contrària i, per tant, el nombre $c := |m|^{1/\log m}$ no depèn de m. Així, se satisfà la igualtat $|n| = c^{\log n}$ per a tot nombre natural $n > 0$. En conseqüència, per a tot nombre racional positiu n/m és $|n/m| = c^{log(n/m)}$. Si escrivim $c = e^a$ per a un cert nombre real positiu a, obtenim la igualtat $|x| = |x|_\infty^a$, la potència a-èsima del valor absolut usual de x, per a tot nombre racional x, de manera que el valor absolut $|\ |$ és equivalent a $|\ |_\infty$.

Segon cas: existeix un nombre enter $n > 1$ tal que $|n| \leq 1$.

En aquest cas, $\max(1, |n|) = 1$ i de la desigualtat (9.3.1) obtenim que $|m| \leq 1$ per a tot nombre enter positiu m. En particular, el valor absolut és no arquimedià. El conjunt $A := \{x \in \mathbb{Q} : |x| \leq 1\}$ és un anell local, amb ideal maximal $\mathfrak{P} := \{x \in \mathbb{Q} : |x| < 1\}$, i conté $\mathbb{Z}$. Sigui $p\mathbb{Z} := \mathfrak{P} \cap \mathbb{Z}$; és un ideal primer no nul de $\mathbb{Z}$, ja que si per a tot nombre

primer p se satisfés la igualtat $|p| = 1$, aleshores seria $|x| = 1$ per a tot nombre racional no nul x i el valor absolut seria trivial. Per tant, p és un nombre primer. Si $m \in \mathbb{Z} - p\mathbb{Z}$, aleshores $m \notin \mathfrak{P}$ i $|m| = 1$, de manera que $\left|\frac{m}{n}p^r\right| = |p^r| = |p|^r$, sempre que $r \in \mathbb{Z}$ i $m, n \in \mathbb{Z} - p\mathbb{Z}$; i això ens permet assegurar que $|\ |$ és equivalent al valor absolut p-àdic $|\ |_p$. $\square$

Observació 9.3.3. Sigui $\mathbb{P}(\mathbb{Q})$ el conjunt format per ∞ i tots els nombres primers $\ell > 1$. Convé normalitzar els valors absoluts de $\mathbb{Q}$ de la manera següent:

$$|x|_\infty := \max(x, -x),$$
$$|p|_p := 1/p.$$

D'aquesta manera, $|p|_\infty = p$, $|p|_p = 1/p$, i $|p|_\ell = 1$, per a tota parella de nombres primers $\ell \neq p$, de forma que per a tot nombre primer p se satisfà la fórmula $\prod_{\ell \in \mathbb{P}(\mathbb{Q})} |p|_\ell = 1$. Per multiplicativitat, obtenim el resultat següent.

Teorema 9.3.4 (Fórmula del producte)**.** *Sigui $x \in \mathbb{Q}$, $x \neq 0$. Aleshores, el conjunt dels elements $\ell \in \mathbb{P}(\mathbb{Q})$ tals que $|x|_\ell \neq 1$ és finit i se satisfà la igualtat*

$$\prod_{\ell \in \mathbb{P}(\mathbb{Q})} |x|_\ell = 1. \ \square$$

9.4 Complecions

Per a procedir a demostrar un resultat anàleg per a tot cos de nombres K és convenient disposar de les complecions dels cossos dotats d'un valor absolut. Ja hem fet notar més amunt que si K és un cos amb un valor absolut $|\ |$, aleshores K és també un espai mètric amb la distància definida per la fórmula $d(x, y) := |y - x|$. En particular, tenen sentit les definicions de successió de Cauchy i de successió convergent d'elements de K respecte de la distància definida pel valor absolut.

Recordem que es diu ue una successió $\{a_n\}_{n \geq 0}$ d'elements $a_n \in K$ és de Cauchy quan per a tot $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, existeix un nombre natural n_0 tal que per a tota parella de nombres naturals $m \geq n \geq n_0$ se satisfà la desigualtat $|a_m - a_n| < \varepsilon$; i es diu que és convergent de límit $a \in K$, quan per a tot $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, existeix un nombre natural n_0 tal que per a tot nombre natural $n \geq n_0$ se satisfà la desigualtat $|a_n - a| < \varepsilon$.

És immediat comprovar que tota successió convergent és de Cauchy, que tota successió de Cauchy és fitada (en el sentit que existeix una constant $C \in \mathbb{R}$ tal que per a tot $n \geq 0$ és $|a_n| < C$), així com les altres propietats usuals de les successions de Cauchy d'elements d'un espai mètric.

Definició 9.4.1. Un cos K dotat d'un valor absolut $|\ |$ es diu que és complet quan tota successió de Cauchy d'elements de K és convergent a un element de K.

El primer objectiu d'aquesta secció és recordar el resultat següent.

Proposició 9.4.2. *Sigui K un cos dotat d'un valor absolut $|\ |$. Existeixen un cos $\widehat{K}$ i un valor absolut $|\ |$ en $\widehat{K}$ tals que:*

(a) $\widehat{K}$ *és un cos complet per al valor absolut* $|\ |$*;*

(b) $\widehat{K}$ *conté* K *com a subcòs i la restricció a* K *del valor absolut de* $\widehat{K}$ *és el valor absolut de partida de* K*;*

(c) K *és dens en* $\widehat{K}$*; i*

(d) *si* $(\widehat{K}_1, |\ |_1)$ *i* $(\widehat{K}_2, |\ |_2)$ *són cossos qualssevol per als quals se satisfan* (a) (b)*, i* (c)*, aleshores existeix un únic isomorfisme de cossos* $\varphi : \widehat{K}_1 \to \widehat{K}_2$ *que és la identitat sobre* K *i que és compatible amb les estructures d'espai mètric; és a dir, tal que* $|\varphi(x)|_2 = |x|_1$*.*

Demostració: Considerem l'anell $\mathcal{C}(K)$ de les successions de Cauchy d'elements de K; l'ideal $\mathcal{I}_0(K)$ format per les successions que tenen límit zero és un ideal maximal d'aquest anell i podem identificar K amb un subcòs de $\mathcal{C}(K)$ si enviem cada element $x \in K$ a la successió constant de valor x. L'anell quocient $\widehat{K} := \mathcal{C}(K)/\mathcal{I}_0(K)$ és, doncs, un cos que conté de manera natural K com a subcòs.

Si $\{a_n\}_n, \{b_n\}_n$ són dos elements de $\mathcal{C}(K)$ que difereixen en un element de $\mathcal{I}_0(K)$, aleshores, els límits $\lim |a_n|$ i $\lim |b_n|$ existeixen i coincideixen en $\mathbb{R}$, de manera que podem definir un valor absolut en $\widehat{K}$ per la fórmula $|\{a_n\}_n| := \lim |a_n|$. Això defineix un valor absolut en $\widehat{K}$ que estén el de K i que satisfà les propietats requerides. Els detalls de la demostració es deixen com a exercici: només cal copiar el que es fa per a veure el resultat en el cas de $\mathbb{Q}$ i $\mathbb{R}$ amb el valor absolut usual. Més detalls es poden trobar, per exemple, en [B-S 66], [Ja 73], [La 70], o [Ri 72]. □

Observació 9.4.3. Notem que la demostració pressuposa que ja s'ha construït el cos dels nombres reals com a cos compleció de $\mathbb{Q}$ per al valor absolut usual. En efecte, ja la definició que hem donat de valor absolut com a aplicació en $\mathbb{R}$ pressuposa que coneixem $\mathbb{R}$. De fet, inicialment caldria definir el valor absolut arquimedià de $\mathbb{Q}$ com a aplicació en $\mathbb{Q}$, i, un cop construït $\mathbb{R}$, estendre la definició de valor absolut al cas general. i acabar la construcció de $\mathbb{R}$ de manera molt semblant a com hem fet. No ens hi entretindrem.

Observació 9.4.4. De fet, es demostra un resultat una mica més general que (d): si $(K_1, |\ |_1)$, $(K_2, |\ |_2)$ són dos cossos amb valors absoluts i $\sigma : K_1 \to K_2$ és un morfisme tal que per a tot element $x \in K_1$ és $|\sigma(x)|_2 = |x|_1$, i si $(\widehat{K}_1, |\ |_1)$ i $(\widehat{K}_2, |\ |_2)$ són cossos amb valors absoluts per als quals se satisfan (a), (b) i (c) per a $(K_1, |\ |_1)$ i $(K_2, |\ |_2)$, respectivament, aleshores existeix una extensió única $\widehat{\sigma} : \widehat{K}_1 \to \widehat{K}_2$ de σ, tal que per a tot element $x \in \widehat{K}_1$ és $|\widehat{\sigma}(x)|_2 = |x|_1$.

Definició 9.4.5. Una parella $(\widehat{K}, |\ |)$ que satisfà les condicions de la proposició s'anomena una compleció de $(K, |\ |)$. Acabem de veure que és única llevat d'un únic isomorfisme de cossos que respecta el valor absolut; és a dir, llevat d'una única isometria de cossos.

L'objectiu més immediat és provar el teorema d'Ostrowski, que ens proporciona tots els cossos complets respecte d'un valor absolut arquimedià. Abans, però, convé establir un resultat previ.

Lema 9.4.6. *Sigui* $|\ |$ *un valor absolut de* $\mathbb{C}$ *que estén el valor absolut usual de* $\mathbb{R}$*. Aleshores, per a tota parella de nombres reals* a, b *se satisfà la igualtat* $|a + bi|^2 = a^2 + b^2$*; és a dir,* $|\ |$ *és el valor absolut usual de* $\mathbb{C}$*.*

DEMOSTRACIÓ: Escrivim $||a+bi|| := (a^2+b^2)^{1/2}$, $a,b \in \mathbb{R}$, el valor absolut usual de $\mathbb{C}$. Com que per a tota parella de nombres reals a,b se satisfà la desigualtat $(|a|-|b|)^2 \geq 0$, és $2|a||b| \leq |a|^2+|b|^2 = a^2+b^2$, de manera que obtenim la desigualtat $(|a|+|b|)^2 \leq 2(a^2+b^2)$ i, en conseqüència, $|a+bi| \leq |a|+|b||i| = |a|+|b| \leq \sqrt{2}(a^2+b^2)^{1/2} = \sqrt{2}||a+bi||$, ja que $|i|=1$ perquè i és una arrel de la unitat. Això ens permet assegurar que la funció $f(\alpha) := |\alpha|/||\alpha||$, definida en $\mathbb{C}-\{0\}$, és fitada per $\sqrt{2}$. Si per a algun nombre complex no nul α fos $f(\alpha)>1$, com que f és una funció multiplicativa, obtindríem la contradicció que $+\infty = \lim f(\alpha^n) \leq \sqrt{2}$; per tant, $f(\alpha) \leq 1$ per a tot $\alpha \in \mathbb{C}-\{0\}$. En canviar α per α^{-1}, obtindríem que $f(\alpha) \geq 1$ per a tot $\alpha \in \mathbb{C}-\{0\}$, de manera que $f(\alpha)=1$, com volíem demostrar. □

Teorema 9.4.7 (Ostrowski)**.** *Sigui K un cos complet respecte d'un valor absolut arquimedià, $|\ |$. Aleshores, K és isomorf al cos $\mathbb{R}$ o bé al cos $\mathbb{C}$ i el valor absolut $|\ |$ és equivalent al valor absolut usual.*

DEMOSTRACIÓ: Com que el valor absolut és arquimedià el cos K ha de ser de característica zero, ja que en cas contrari els valors absoluts dels nombres $n1$, $n \in \mathbb{Z}$, serien en nombre finit i, en conseqüència, el conjunt $\{|n| : n \in \mathbb{Z}\}$ seria fitat. Doncs, la restricció del valor absolut a $\mathbb{Q}$ és un valor absolut arquimedià i, per tant, equivalent al valor absolut usual de $\mathbb{Q}$. Així, podem canviar el valor absolut de K per un d'equivalent, elevant a una potència, per tal que la seva restricció a $\mathbb{Q}$ sigui el valor absolut usual; i això no canvia el resultat que volem provar.

Ara, com que K és complet i conté $\mathbb{Q}$, conté la compleció de $\mathbb{Q}$ respecte del valor absolut usual de $\mathbb{Q}$; és a dir, el cos K conté $\mathbb{R}$ com a cos i la restricció del valor absolut de K a $\mathbb{R}$ coincideix amb el valor absolut usual de $\mathbb{R}$. El següent pas de la demostració consisteix a veure que podem suposar que K conté $\mathbb{C}$ com a cos i que la restricció a $\mathbb{C}$ del valor absolut de K és el valor absolut usual de $\mathbb{C}$.

Si K no conté un element i tal que $i^2=-1$, canviem K per $K(i)$ i considerem el valor absolut de $K(i)$ definit per la fórmula $|a+bi|^2 := |a|^2+|b|^2$, $a,b \in K$; efectivament, aquesta definició proporciona un valor absolut en $K(i)$ que estén el de K i tal que $K(i)$ és complet respecte d'aquest valor absolut. Com que K conté $\mathbb{R}$, obtenim que $K(i)$ conté $\mathbb{C}$ i, en virtut del lema anterior, la restricció del valor absolut de $K(i)$ a $\mathbb{C}$ és el valor absolut usual de $\mathbb{C}$. Si demostrem que $K(i)=\mathbb{C}$ haurem acabat, ja que K és un subcòs de $K(i)=\mathbb{C}$ que conté $\mathbb{R}$, de manera que $K=\mathbb{C}$ o bé $K=\mathbb{R}$, que és el que volem demostrar.

En resum, podem suposar que $\mathbb{C} \subseteq K$ i cal veure que $K=\mathbb{C}$. Suposem que $\mathbb{C} \subsetneq K$ i considerem un element $z \in K$ tal que $z \notin \mathbb{C}$. Es tracta d'arribar a contradicció.

Sigui $m := \inf\{|z-\alpha| : \alpha \in \mathbb{C}\}$. Es tracta de provar, en primer lloc, que existeix un nombre complex α_0 tal que $m=|z-\alpha_0|$; però això és senzill: donat un nombre real positiu ε, el conjunt dels nombres complexos α per als quals $|z-\alpha| \leq m+\varepsilon$ està inclòs en la bola tancada de radi $m+\varepsilon+|z|$ i centre a l'origen; la funció $f(\alpha) := |z-\alpha|$, definida en aquest compacte, és una funció real i contínua de manera que pren el seu mínim en un cert punt α_0 del disc; i això implica que $m=|z-\alpha_0|$ per a un cert element $\alpha_0 \in \mathbb{C}$.

En particular, podem canviar z per $z-\alpha_0$ de manera que obtenim un element $z \in K-\mathbb{C}$ tal que $|z| \leq |z-\alpha|$ per a tot $\alpha \in \mathbb{C}$. Observem que $|z|>0$, ja que $z \notin \mathbb{C}$. Ara es tracta de provar que per a tot nombre complex β tal que $|\beta|<|z|$ és $|z-\beta|=|z|$. Per a això, sigui $n \in \mathbb{N}$ i sigui ζ una arrel primitiva n-èsima de la unitat en $\mathbb{C}$. A partir de la igualtat

$z^n-\beta^n=(z-\beta)(z-\zeta\beta)\cdots(z-\zeta^{n-1}\beta)$, tenim que $|z-\beta||z-\zeta\beta|\cdots|z-\zeta^{n-1}\beta|\leq|z|^n+|\beta|^n$; com que $\zeta^i\beta\in\mathbb{C}$, per a cada un dels factors se satisfà la desigualtat $|z-\zeta^i\beta|\geq|z|$ i obtenim la desigualtat $|z|^{n-1}|z-\beta|\leq|z|^n+|\beta|^n=|z|^n\left(1+\dfrac{|\beta|^n}{|z|^n}\right)$, de manera que $|z-\beta|\leq|z|\left(1+\dfrac{|\beta|^n}{|z|^n}\right)$. Com que això se satisfà per a tot nombre natural n, podem prendre límit i obtenim la desigualtat $|z-\beta|\leq|z|$ per a tot nombre complex β tal que $|\beta|<|z|$. I per l'elecció de z, és $|z-\beta|=|z|$ per a tot nombre complex β tal que $|\beta|<|z|$.

En resum, hem provat que si $\mathbb{C}\subsetneq K$, aleshores podem trobar un element $z\in K-\mathbb{C}$ per al qual se satisfan les dues condicions següents:

(a) per a tot $\beta\in\mathbb{C}$ és $|z|\leq|z-\beta|$; i,

(b) per a tot $\beta\in\mathbb{C}$ tal que $|\beta|<|z|$ és $|z-\beta|=|z|$.

Com que $z\notin\mathbb{C}$, la propietat (a) ens permet assegurar que $|z|>0$ i podem considerar qualsevol nombre complex β_0 tal que $|\beta_0|<|z|$. L'element $z_1:=z-\beta_0$ no pertany a $\mathbb{C}$ i satisfà les mateixes condicions (a) i (b) que z, ja que la segona propietat es dedueix de la primera, com hem vist més amunt. En conseqüència, se satisfan les condicions $z_2:=z_1-\beta_0=z-2\beta_0\notin\mathbb{C}$, $|z_2|=|z|$ i $|z_2|\leq|z_2-\beta|$ per a tot nombre complex β; per inducció, per a tot enter $k\geq1$ obtenim que $z_k:=z-k\beta_0\notin\mathbb{C}$, $|z_k|=|z|$ i $|z_k|\leq|z_k-\beta|$ per a tot nombre complex $\beta\in\mathbb{C}$.

Ara bé, tot nombre complex α es pot escriure en la forma $k\beta_0$ per a algun nombre natural $k\geq0$ i algun nombre complex β_0 tal que $|\beta_0|<|z|$; en conseqüència, $|z-\alpha|=|z|$ per a tot nombre complex α. I això és contradictori. En efecte, si això fos així, per a tota parella de nombres complexos α,β obtindríem una desigualtat de la forma

$$|\alpha-\beta|\leq|\alpha-z|+|z-\beta|=2|z|;$$

però si prenem $\alpha=3|z|$ i $\beta=0$, aleshores $|\alpha-\beta|=|\,3|z|\,|=3|z|>2|z|$, ja que $z\neq0$ i $|\,3|z|\,|=3|z|$ perquè $3|z|$ és real positiu i, en conseqüència, el seu valor absolut és l'usual.

La contradicció és conseqüència de la suposició que $\mathbb{C}\subsetneq K$, de manera que $K=\mathbb{C}$, que és allò que volíem provar. □

9.5 Cossos complets no arquimedians

El teorema d'Ostrowski caracteritza els cossos complets respecte d'un valor absolut arquimedià. Però aquests no són els únics cossos complets que ens interessen. Entre els cossos complets respecte de la topologia definida per un valor absolut n'hi ha una classe especialment important des del punt de vista de l'Aritmètica: les complecions dels cossos de nombres respecte dels valors absoluts $\mathfrak{p}$-àdics per als ideals primers no nuls $\mathfrak{p}$ dels seus anells d'enters. En aquesta secció es tracta d'estudiar-los. Per a això ens situarem en un cas una mica més general.

Proposició 9.5.1. *Siguin K un cos, v una valoració real de K i $\widehat{K}$ la compleció de K respecte d'un valor absolut associat a la valoració v. Aleshores, existeix una única valoració $\widehat{v}:\widehat{K}\longrightarrow\mathbb{R}\cup\{+\infty\}$ que estén la valoració v i tal que el valor absolut de $\widehat{K}$ com a cos compleció de K és associat a aquesta valoració. A més a més, el grup de valors de $\widehat{v}$ coincideix amb el grup de valors de v.*

DEMOSTRACIÓ: Si convé, podem canviar el valor absolut de K per un d'equivalent i, així, podem suposar que és definit per la fórmula $|x| = e^{-v(x)}$, per a tot element $x \in K$; equivalentment, podem pensar que la valoració de K és definida per la fórmula $v(x) = -\log|x|$. Aquesta observació ens servirà per a definir una valoració real de $\widehat{K}$. En efecte, donat $\alpha \in \widehat{K}$, posem $\widehat{v}(\alpha) := -\log|\alpha|$; aquesta fórmula defineix una aplicació $\widehat{v} : \widehat{K} \longrightarrow \mathbb{R} \cup \{+\infty\}$ que estén la valoració v i, com que el valor absolut de K és no arquimedià, el mateix succeeix amb el valor absolut de $\widehat{K}$, de manera que per a $\widehat{v}$ se safisfan les propietats formals de valoració. Resta veure que el grup de valors de $\widehat{v}$ coincideix amb el grup de valors, Γ, de v.

Per a això, donat $\alpha \in \widehat{K}$, $\alpha \neq 0$, existeix una successió $\{a_n\}_n$ d'elements $a_n \in K$ tal que $\alpha = \lim a_n$, de manera que $|\alpha| = \lim|a_n| \neq 0$, per definició del valor absolut de $\widehat{K}$. En particular, $\{|a_n|\}_n$ és una successió convergent de nombres reals no negatius; per tant, admet una parcial monòtona. En canviar, doncs, la successió $\{a_n\}_n$ per una parcial adequada, podem suposar que $\{|a_n|\}_n$ és monòtona. I com que $\widehat{v}(\alpha) \in \Gamma$ equival a $\widehat{v}(\alpha^{-1}) \in \Gamma$, canviem, si convé, α per α^{-1}, i podem suposar que $\{|a_n|\}_n$ és decreixent. Veiem que la successió $\{|a_n|\}_n$ és constant d'un lloc endavant. Si no fos així, prenem una parcial de la successió $\{a_n\}_n$ de manera que podem suposar que la successió $\{|a_n|\}_n$ és estrictament decreixent; és a dir, que per a tot nombre natural n és $|a_{n+1}| < |a_n|$. En aquestes condicions, com que el valor absolut de K és no arquimedià, per a tot nombre natural n se satisfà la igualtat $|a_n - a_{n+1}| = |a_n|$. Ara bé, la successió $\{a_n\}_n$ és de Cauchy i, per tant, $\lim|a_{n+1} - a_n| = 0$; és a dir, $|\alpha| = \lim|a_n| = 0$. Però això contradiu el fet que $\alpha \neq 0$. En conseqüència, la successió $\{|a_n|\}_n$ és constant d'un lloc endavant, de manera que el seu límit és aquesta constant; és a dir, existeix $n \in \mathbb{N}$ tal que $|\alpha| = |a_n|$ o, equivalentment, $\widehat{v}(\alpha) = v(a_n) \in \Gamma$ i ja hem acabat. □

Observació 9.5.2. Hem provat que tot element no nul de $\widehat{K}$ es pot escriure com a límit d'una successió de Cauchy d'elements de K tal que el valor absolut dels seus termes és constant. En particular, les unitats de l'anell $\widehat{A}$ són els límits de successions de Cauchy d'elements de K de valor absolut 1.

Corol·lari 9.5.3. *Si la valoració v és discreta, aleshores la valoració $\widehat{v}$ és discreta.* □

En el cas dels valors absoluts associats a valoracions discretes podem dir encara més.

Proposició 9.5.4. *Siguin A un anell de valoració discreta, $\mathfrak{p} = \pi A$ el seu ideal maximal, K el seu cos de fraccions i $\widehat{K}$ la compleció de K respecte del valor absolut $\mathfrak{p}$-àdic. Siguin $\widehat{A} := \{x \in \widehat{K} : |x| \leq 1\}$ i $\widehat{\mathfrak{p}} := \{x \in \widehat{K} : |x| < 1\}$. Aleshores,*

(a) *$\widehat{A}$ és un anell de valoració discreta amb ideal maximal $\widehat{\mathfrak{p}}$;*

(b) *per a tot nombre enter no negatiu n se satisfà la igualtat d'ideals $\widehat{\mathfrak{p}}^n = \pi^n \widehat{A}$;*

(c) *per a tot nombre enter $n \geq 1$ hi ha un isomorfisme natural $A/\mathfrak{p}^n \cong \widehat{A}/\widehat{\mathfrak{p}}^n$; i*

(d) *$\widehat{A}$ és el límit projectiu del sistema $A/\mathfrak{p}^n$, és a dir, la compleció de A respecte de la seva topologia $\mathfrak{p}$-àdica.*

DEMOSTRACIÓ: La propietat (a) és immediata a partir de la proposició anterior, ja que $\widehat{A}$ és l'anell de la valoració $\widehat{v}$ extensió de la valoració $\mathfrak{p}$-àdica de K i $\widehat{\mathfrak{p}}$ el seu ideal maximal.

Per a veure (b) només cal observar que $\widehat{v}(\pi^n) = v(\pi^n)$, de manera que π^n genera la potència n-èsima de l'ideal maximal $\widehat{\mathfrak{p}}$ de $\widehat{A}$.

Veiem (c). Donat un element $\alpha \in \widehat{A} - \widehat{\mathfrak{p}}$ podem elegir una successió d'elements $a_n \in A_{\mathfrak{p}}$ de límit α i de valor absolut $|a_n| = 1$. D'un lloc endavant, per als elements a_n se satisfan relacions de la forma $a_{n+1} - a_n \in \pi A$, ja que la successió $\{a_n\}_n$ és de Cauchy i, per tant, d'un lloc endavant, $|a_{n+1} - a_n|$ és tan petit com vulguem. Això ens permet assegurar que podem escriure la successió $\{a_n\}_n$ com la suma d'una successió constant formada per un element de A de valor absolut 1 i una successió de Cauchy d'elements de $\mathfrak{p}$; per tant, l'aplicació natural $A/\mathfrak{p} \longrightarrow \widehat{A}/\widehat{\mathfrak{p}}$, que s'obté en factoritzar l'aplicació

$$A \longrightarrow \widehat{A} \longrightarrow \widehat{A}/\widehat{\mathfrak{p}},$$

és exhaustiva. Com que $\mathfrak{p}$ és, clarament, el nucli d'aquesta última aplicació, obtenim un isomorfisme $A/\mathfrak{p} \cong \widehat{A}/\widehat{\mathfrak{p}}$. Això demostra el cas $n = 1$.

Per al cas $n > 1$, podem multiplicar la igualtat $\widehat{A} = A + \widehat{\mathfrak{p}}$ per π; obtenim la igualtat $\widehat{\mathfrak{p}} = \pi\widehat{A} = \pi A + \pi\widehat{\mathfrak{p}} = \pi A + \widehat{\mathfrak{p}}^2$; en substituir en l'anterior i tenir en compte que $A + \pi A = A$ obtenim la igualtat $\widehat{A} = A + \widehat{\mathfrak{p}}^2$. I, recursivament, per a tot nombre natural $n \geq 1$ obtenim la igualtat $\widehat{A} = A + \widehat{\mathfrak{p}}^n$. A més a més, en tenir en compte les valoracions dels elements, $\widehat{\mathfrak{p}}^n \cap A = \mathfrak{p}^n$, de manera que el morfisme $A/\mathfrak{p}^n \longrightarrow \widehat{A}/\widehat{\mathfrak{p}}^n$ és un isomosfisme.

Resta demostrar (d). L'anell $\widehat{A}$ és un subanell topològic tancat de $\widehat{K}$, que és un anell (cos) topològic complet; per tant, és un anell complet; de fet, com que A és un subanell dens de $\widehat{A}$, $\widehat{A}$ és la compleció de A respecte de la topologia $\mathfrak{p}$-àdica i, en conseqüència, és el límit projectiu dels anells quocient $A/\mathfrak{p}^n$. □

Observació 9.5.5. En el cas dels anells d'enters dels cossos de nombres, o més generalment, en el cas que el cos residual de A és un cos finit, els anells residuals $A/\mathfrak{p}^n$ són anells finits; per tant, són anells topològics discrets, compactes i Hausdorff. En conseqüència, l'anell $\widehat{A}$ és un anell topològic compacte i Hausdorff per a la topologia $\mathfrak{p}$-àdica.

Per a acabar aquesta primera descripció dels cossos complets respecte d'un valor absolut associat a una valoració discreta, el resultat següent ens proporciona una manera de representar els seus elements. En efecte, considerem un sistema de representants $R \subseteq A$ del cos residual $A/\mathfrak{p}$.

Proposició 9.5.6. *Si la valoració és discreta, tot element no nul $x \in \widehat{K}$ es pot escriure de manera única com la suma d'una sèrie de Laurent*

$$x = \sum_{n \geq n_0} a_n \pi^n,$$

on n_0 és un nombre enter no necessàriament positiu, $a_n \in R$, i $a_{n_0} \neq 0$.

Demostració: L'anell $\widehat{A}$ és el límit projectiu dels anells quocient $A/\mathfrak{p}^n$; per tant, si n_0 denota la valoració $\mathfrak{p}$-àdica de x, l'element $\pi^{-n_0}x \in \widehat{A}$ es pot escriure com una successió coherent $(b_0, b_0 + b_1\pi, \ldots, b_0 + b_1\pi + \cdots + b_n\pi^n, \ldots)$ d'elements de $A/\pi^n A$, i els elements b_n es poden elegir en un sistema de representants de $A/\mathfrak{p}$. Dit d'una altra manera, $\pi^{-n_0}x$ és el límit de la successió de sumes parcials de la sèrie, evidentment convergent, $b_0 + b_1\pi + \cdots + b_n\pi^n + \ldots$; només cal escriure $a_n := b_{n+n_0}$. □

Definició 9.5.7. Siguin K un cos de nombres i $\mathfrak{p}$ un ideal primer de l'anell dels enters de K. Escriurem $K_{\mathfrak{p}}$ per denotar el cos compleció de K respecte del valor absolut discret associat a la valoració $\mathfrak{p}$-àdica. En particular, $\mathbb{Q}_p$ denota el cos dels nombres racionals p-àdics; és a dir, la compleció de $\mathbb{Q}$ per a la valoració p-àdica. De la mateixa manera, $\mathbb{Z}_p$ designa l'anell dels enters de $\mathbb{Q}_p$; és a dir, l'anell de la valoració p-àdica de $\mathbb{Q}_p$ o, si es vol, la compleció de l'anell $\mathbb{Z}$ per a la topologia p-àdica.

9.6 Extensions finites de cossos complets no arquimedians

L'objectiu d'aquesta secció és l'estudi de les extensions del valor absolut d'un cos complet no arquimedià a un cos extensió finita.

Sigui, doncs, K un cos complet respecte de la topologia definida per un valor absolut no arquimedià, que denotarem per $|\ |$. Ens interessa parlar d'espais vectorials normats.

Definició 9.6.1. Sigui E un K-espai vectorial de dimensió finita, n. Una norma en E (respecte del valor absolut de K) és una aplicació $||\ ||: E \longrightarrow \mathbb{R}$ per a la qual se satisfan les propietats següents:

(a) $||x|| \geq 0$;

(b) $||x|| = 0 \Longleftrightarrow x = 0$;

(c) $||\lambda x|| = |\lambda|\,||x||$; i

(d) $||x + y|| \leq ||x|| + ||y||$,

per a qualsevol elecció d'elements $x, y \in E$ i $\lambda \in K$.

En particular, l'aplicació $d : E \times E \longrightarrow \mathbb{R}$ definida per la igualtat $d(x, y) := ||y - x||$ és una distància en E, invariant per translació, de manera que E és un K-espai vectorial topològic.

Definició 9.6.2. Dues normes $||\ ||_1, ||\ ||_2$ de E s'anomenen equivalents quan existeixen constants reals positives C_1, C_2 tals que per a tot element $x \in E$ se satisfan les desigualtats $C_1||x||_1 \leq ||x||_2 \leq C_2||x||_1$. Això és equivalent a dir que totes dues normes defineixen distàncies equivalents.

Proposició 9.6.3. *Sigui E un K-espai vectorial de dimensió finita, posem n. Totes les normes de E sobre K són equivalents; en particular, totes són equivalents a la norma del suprem: elegida una K-base $\{e_1, \ldots, e_n\}$ de E, posem* $\left|\left|\sum_{i=1}^{n} x_i e_i\right|\right| := \max\{|x_1|, \ldots, |x_n|\}$.

Demostració: Exercici. □

Corol·lari 9.6.4. *Sigui $L|K$ una extensió finita de cossos, tal que K és complet respecte de la topologia definida per un valor absolut no arquimedià. Aleshores, existeix un únic valor absolut de L, llevat d'equivalència, que estén el valor absolut de K.*

Demostració: Exercici. □

9.7 Valors absoluts arquimedians d'un cos de nombres

L'objectiu d'aquesta secció és la determinació d'un sistema de representants, mòdul equivalència, del conjunt de tots els valors absoluts arquimedians d'un cos de nombres K.

Sigui, doncs, K un cos de nombres. Si pensem K com a cos abstracte, i si denotem per $n := [K : \mathbb{Q}]$ el seu grau absolut, com que l'extensió $K|\mathbb{Q}$ és separable i $\mathbb{C}$ és un cos algebraicament tancat que conté $\mathbb{Q}$, hi ha exactament n maneres diferents d'incloure K en $\mathbb{C}$. D'aquestes, n'hi ha unes quantes, diem r_1, que tenen imatge dins $\mathbb{R}$; s'anomenen les immersions reals de K; les altres $n-r_1$ són sempre en nombre parell i es poden agrupar en r_2 parelles, cada parella formada per una immersió σ i la immersió complexa conjugada de σ, $c \circ \sigma$, on $c : \mathbb{C} \longrightarrow \mathbb{C}$ denota la conjugació complexa; s'anomenen les immersions imaginàries de K. Amb aquesta definició de r_1 i r_2, podem escriure la igualtat $n = r_1+2r_2$; a partir d'ara, indicarem les immersions de K en $\mathbb{C}$ de la manera següent: $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ denotaran les immersions reals, $\sigma_{r_1+1}, \sigma_{r_1+2}, \ldots, \sigma_{r_1+r_2}$, un sistema de representants de les parelles d'immersions no reals $(\sigma, c \circ \sigma)$, i $\sigma_{r_1+r_2+j} = c \circ \sigma_{r_1+j}$, per a $1 \leq j \leq r_2$, les altres immersions imaginàries (cf. la secció **4.3**).

Cada una de les immersions $\sigma : K \longrightarrow \mathbb{C}$ dóna lloc a un valor absolut arquimedià de K, $|\ |_\sigma$, de la manera següent: per a tot element $x \in K$, es defineix $|x|_\sigma := |\sigma(x)|$, on $|z| := (z\overline{z})^{1/2}$ denota el valor absolut usual del nombre complex z. La comprovació dels axiomes de valor absolut és immediata. Com que, per a tot nombre complex z és $|z| = |\overline{z}|$, una immersió σ i la immersió complexa conjugada de σ, $c \circ \sigma$, defineixen el mateix valor absolut. Es tracta de provar el resultat següent.

Proposició 9.7.1. *Sigui K un cos de nombres. Per a cada nombre i, $1 \leq i \leq r_1 + r_2$, denotem per $|\ |_i := |\ |_{\sigma_i}$, el valor absolut de K definit per la immersió σ_i. Aleshores, per a $i \neq j$ els valors absoluts $|\ |_i$ i $|\ |_j$ no són equivalents i tot valor absolut arquimedià de K és equivalent a un dels valors absoluts $|\ |_i$.*

Demostració: Sigui $|\ |$ un valor absolut arquimedià de K. La restricció a $\mathbb{Q}$ d'aquest valor absolut és un valor absolut arquimedià de $\mathbb{Q}$; per tant, equivalent al valor absolut usual. Canviant-lo, si convé, per una potència, podem suposar que $|\ |$ és una extensió a K del valor absolut usual de $\mathbb{Q}$. En virtut del teorema d'Ostrowski, la compleció de K respecte d'aquest valor absolut és un cos isomorf a $\mathbb{R}$ o bé a $\mathbb{C}$. És a dir, si $\widehat{K}$ designa aquesta compleció, hi ha un isomorfisme de cossos $\sigma : \widehat{K} \longrightarrow \sigma(\widehat{K}) \subseteq \mathbb{C}$ que respecta el valor absolut; és a dir, tal que per a tot element $x \in \widehat{K}$ és $|x|^2 = \sigma(x)\overline{\sigma(x)}$. Com que K és subcòs de la seva compleció, la restricció a K de σ és una immersió complexa de K i se satisfà la igualtat $|x| = |x|_\sigma$ per a tot element $x \in K$. Resta demostrar que els valors absoluts $|\ |_i$, $1 \leq i \leq r_1 + r_2$, són no equivalents.

La demostració d'aquest resultat està inclosa en la demostració del teorema de Dirichlet d'estructura del grup de les unitats de l'anell dels enters d'un cos de nombres (cf. el teorema **4.6.1**). En efecte, allà es prova que existeixen unitats $u_1, \ldots, u_r$, on $r := r_1 + r_2$, tals que $|\sigma_i(u_j)| \leq 1$ si $i \neq j$ i $|\sigma_i(u_i)| > 1$, per a $1 \leq i, j \leq r_1 + r_2$. Per tant, els valors absoluts de K definits per aquestes immersions són no equivalents. □

Observació 9.7.2. De fet, per a aquesta darrera part, es prova un resultat que implica aquest que s'acaba d'enunciar; es deixa com a exercici la comprovació dels detalls de la implicació.

Més generalment, suposem que K és un cos amb un valor absolut arquimedià $|\ |$; canviant-lo, si convé, per un valor absolut equivalent, podem suposar que la restricció a $\mathbb{Q}$ del valor absolut $|\ |$ és el valor absolut usual de $\mathbb{Q}$. En virtut del teorema d'Ostrowski, la compleció de K respecte d'aquest valor absolut ha de ser un cos isomorf, com a cos amb un valor absolut, al cos $\mathbb{R}$ o bé al cos $\mathbb{C}$. Per tant, i com que K és subcòs de la seva compleció, podem suposar que K és un subcòs de $\mathbb{C}$ i que el valor absolut $|\ |$ de K és la restricció del valor absolut usual de $\mathbb{C}$.

Sigui $L|K$ una extensió finita i denotem per n el seu grau; com que K és de característica zero i $\mathbb{C}$ és un cos algebraicament tancat que conté K, hi ha exactament n maneres diferents d'incloure L en $\mathbb{C}$. Cada una de les n K-immersions $\sigma : L \longrightarrow \mathbb{C}$ ens permet definir un valor absolut arquimedià de L que estén el valor absolut $|\ |$ de K; això es pot fer per la fórmula $|x|_\sigma := |\sigma(x)|$. I el cos L no té cap altre valor absolut arquimedià que estengui el valor absolut $|\ |$ de K que els definits d'aquesta manera. En efecte, si $||\ ||$ és un valor absolut de L que estén $|\ |$, hi ha un isomorfisme $\sigma : \widehat{L} \longrightarrow \sigma(\widehat{L}) \subseteq \mathbb{C}$ de la compleció de L respecte del valor absolut $||\ ||$ de manera que per a tot element $x \in \widehat{L}$ és $||x|| = |\sigma(x)|$, on $|\ |$ designa, aquí, el valor absolut usual de $\mathbb{C}$. La restricció de σ al cos L ens proporciona una K-immersió de L en $\mathbb{C}$ i el valor absolut de L, com a restricció que és del de $\widehat{L}$, és donat per la fórmula $||x|| = |\sigma(x)|$, per a tot element $x \in L$.

En resum, hem demostrat el resultat següent.

Proposició 9.7.3. *Siguin K un cos, $|\ |$ un valor absolut arquimedià de K, i $L|K$ una extensió finita. Aleshores, existeix una immersió de K en $\mathbb{C}$ i tot valor absolut $||\ ||$ de L que estén el de K és donat per una fórmula $||x|| = |\sigma(x)|$, per a tot $x \in L$, on $|\ |$ denota una extensió a $\mathbb{C}$ fixa del valor absolut de K i σ una qualsevol de les K-immersions de L en $\mathbb{C}$.* $\square$

9.8 Extensió de valors absoluts discrets

Siguin K un cos de nombres i $|\ |$ un valor absolut de K. La restricció a $\mathbb{Q}$ de $|\ |$ és equivalent a un dels valors absoluts de $\mathbb{Q}$; per tant, o bé és el trivial, o bé és l'usual, o bé és un valor absolut p-àdic per a un cert nombre primer p. Dit d'una altra manera, el valor absolut de K és l'extensió d'algun dels valors absoluts de $\mathbb{Q}$. Ja hem estudiat el cas dels valors absoluts arquimedians; ara es tracta d'estudiar els altres. Comencem pel valor absolut trivial.

Proposició 9.8.1. *Sigui $L|K$ una extensió algebraica qualsevol de cossos. L'únic valor absolut de L que estén el valor absolut trivial de K és el trivial.*

Demostració: Cal veure que per a tot element no nul $x \in L$ és $|x| = 1$. Si $x^n \in K$ per a algun enter $n > 0$, de la igualtat $|x|^n = |x^n| = 1$ es dedueix que $|x| = 1$; per tant, podem suposar que $x^n \notin K$ per a cap natural $n \geq 1$. En aquest cas, però, x satisfà una equació de la forma $x^n = g(x)$ per a algun polinomi $g \in K[T]$ de grau menor que n. Suposem que $|x| \neq 1$. La desigualtat triangular ens permet escriure $|x|^n \leq |a_0| + |a_1||x| + \cdots + |a_{n-1}||x|^{n-1} \leq 1 + |x| + |x|^2 + \cdots + |x|^{n-1} = \dfrac{|x|^n - 1}{|x| - 1}$. Si $|x| > 1$, obtenim la desigualtat $|x|^n(|x| - 1) \leq |x|^n - 1$, d'on deduïm que $|x|^n(|x| - 2) \leq -1 < 0$ i, per tant, $|x| < 2$. Com que, per a tot enter $k \geq 1$ se satisfà la desigualtat $|x^k| = |x|^k > 1$,

repetint l'argument obtenim que $|x|^k < 2$; en conseqüència, i per pas al límit, ha de ser $|x| \leq 1$; això contradiu el fet que $|x| > 1$. Si $|x| < 1$, canviem x per x^{-1} i arribem a la mateixa contradicció. Per tant, ha de ser $|x| = 1$, com volíem demostrar. □

En conseqüència, si K és un cos de nombres i $|\ |$ és un valor absolut no trivial i no arquimedià de K, aleshores $|\ |$ és l'extensió d'un dels valors absoluts p-àdics de $\mathbb{Q}$. Per tant, ens cal estudiar l'extensió dels valors absoluts discrets a cossos extensió finita.

Suposem, doncs, que A és un anell de valoració discreta, $\mathfrak{p}$ el seu ideal maximal, i K el seu cos de fraccions, i siguin $L|K$ una extensió finita i B la clausura entera de A en L. Podem descriure fàcilment algunes extensions del valor absolut $\mathfrak{p}$-àdic de K a L.

Per a començar, observem que B és un anell de Dedekind, de manera que podem escriure $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ la descomposició de l'ideal $\mathfrak{p}$ en B. Els anells localitzats de B en els ideals $\mathfrak{P}_i$ són anells de valoració discreta que dominen A, i la valoració $\mathfrak{P}_i$-àdica de L, normalitzada de manera que el grup de valors sigui $\frac{1}{e_i}\mathbb{Z}$, és una extensió de la valoració $\mathfrak{p}$-àdica de K. Per tant, per a cada ideal primer de B que divideix $\mathfrak{p}$ obtenim un valor absolut en L que estén el valor absolut $\mathfrak{p}$-àdic de K. Es tracta de veure que, llevat d'equivalència, aquests són els únics valors absoluts de L que estenen el valor absolut $\mathfrak{p}$-àdic de K. Concretament, se satisfà el resultat següent.

Proposició 9.8.2. *Sigui $L|K$ una extensió finita de cossos i suposem que K és el cos de fraccions d'un anell de valoració discreta A amb ideal maximal $\mathfrak{p}$. Aleshores, tot valor absolut de L que estén el valor absolut $\mathfrak{p}$-àdic de K és un dels valors absoluts $\mathfrak{P}_i$-àdics, on $\mathfrak{P}_i$ són tots els ideals maximals de la clausura entera de A en L. A més a més, per a $\mathfrak{P}_i \neq \mathfrak{P}_j$ els valors absoluts $\mathfrak{P}_i$-àdic i $\mathfrak{P}_j$-àdic de L no són equivalents.*

Demostració: Suposem que $|\ |$ és un valor absolut de L que estén el valor absolut $\mathfrak{p}$-àdic de K. Aleshores $|\ |$ és no arquimedià i podem considerar l'anell $A' := \{x \in L : |x| \leq 1\}$, que és un anell de valoració amb ideal maximal $\mathfrak{P}' := \{x \in L : |x| < 1\}$. Clarament, l'anell A' domina l'anell local A, que és l'anell de la valoració $\mathfrak{p}$-àdica de K. En particular, A' conté la clausura entera de A en L; és a dir, A' conté B. En efecte, si $x \in B$ no fos de A', aleshores $x^{-1} \in \mathfrak{P}'$ i a partir d'una relació de dependència entera de x de coeficients en A, obtindríem una igualtat de la forma

$$1 = \sum_{i=0}^{n-1} a_i (x^{-1})^{n-i}, \qquad a_i \in A,$$

de manera que $1 \in \mathfrak{P}'$, contradicció. Si demostrem que A' és el localitzat de B en un dels ideals primers $\mathfrak{P}_i$, obtindrem que A' és l'anell de la valoració $\mathfrak{P}_i$-àdica i, en conseqüència, que el valor absolut de L és equivalent al valor absolut $\mathfrak{P}_i$-àdic. Sigui $\mathfrak{P}_i$ la contracció de $\mathfrak{P}'$ a B. L'anell localitzat de B en $\mathfrak{P}_i$, posem B_i, també és un subanell de A', ja que els elements de B que no estan en $\mathfrak{P}_i$ són invertibles en A'. Això ens permet dir que A' és un anell de valoració que domina l'anell de valoració discreta B_i; Per tant, $A' = B_i$, ja que els anells de valoració discreta són els subanells maximals del seu cos de fraccions; en efecte, si π és un generador de l'ideal maximal de B_i, aleshores $L = B[\pi^{-1}]$, i qualsevol subanell de L que conté estrictament B_i conté π^{-1}.

Per últim, els valors absoluts $\mathfrak{P}_i$-àdics de L són no equivalents dos a dos, ja que valoracions equivalents d'un cos L tenen associat el mateix anell de valoració. □

Corol·lari 9.8.3. *Sigui K un cos de nombres. Els valors absoluts no equivalents de K són el trivial, els valors absoluts arquimedians associats a les r_1 immersions reals de K, els valors absoluts arquimedians associats a les r_2 parelles d'immersions imaginàries de K, i els valors absoluts $\mathfrak{p}$-àdics associats als diferents ideals primers no nuls $\mathfrak{p}$ de l'anell dels enters de K.* □

Convé normalitzar els valors absoluts d'un cos de nombres K de la manera següent. El valor absolut arquimedià donat per una immersió real $\sigma : K \longrightarrow \mathbb{R}$, es normalitza per $|x|_\sigma := |\sigma(x)|$, on $|\ |$ és el valor absolut usual de $\mathbb{R}$, i el valor absolut arquimedià donat per una immersió imaginària $\sigma : K \longrightarrow \mathbb{C}$, es normalitza per $|x|_\sigma := |\sigma(x)|^2$, on $|\ |$ és el valor absolut usual de $\mathbb{C}$, encara que, de fet, $|\ |^2$ no és un valor absolut perquè no satisfà la desigualtat triangular. D'altra banda, el valor absolut no arquimedià associat a un ideal primer no nul $\mathfrak{p}$ de l'anell dels enters de K, es normalitza per $|p|_\mathfrak{p} = p^{-1/ef}$, on $e := e(\mathfrak{p}|p)$ i $f := f(\mathfrak{p}|p)$ són l'índex de ramificació i el grau residual absoluts de l'ideal primer $\mathfrak{p}$ sobre la seva contracció $p\mathbb{Z}$ a $\mathbb{Z}$. Això s'aconsegueix si definim $|\pi|_\mathfrak{p} := p^{-1/f}$, per a un generador π de l'ideal maximal de l'anell de la valoració $\mathfrak{p}$-àdica de K. Amb aquestes normalitzacions se satisfà una fórmula del producte anàloga a la del cas $K = \mathbb{Q}$.

Teorema 9.8.4 (Fórmula del producte)**.** *Sigui $\mathbb{P}(K)$ el conjunt format per tots els valors absoluts de K normalitzats com més amunt. Aleshores, per a tot element no nul $x \in K$ el conjunt dels elements $\mathfrak{p} \in \mathbb{P}(K)$ tals que els valors absoluts $|x|_\mathfrak{p}$ són diferents de 1 és un conjunt finit i se satisfà la igualtat*

$$\prod_{\mathfrak{p}\in\mathbb{P}(K)} |x|_\mathfrak{p} = 1.$$

Demostració: Per a la primera part no hi ha res a provar, ja que la factorització de l'ideal fraccionari principal engendrat per x només conté una quantitat finita d'ideals primers $\mathfrak{p}$ de l'anell d'enters A de K. Per a la segona part, és a dir, per a la fórmula del producte, sigui $\pi_\mathfrak{p}$ un generador de l'ideal primer extensió de $\mathfrak{p}$ a l'anell localitzat de A en $\mathfrak{p}$. Observem, en primer lloc, que podem escriure la igualtat

$$\prod_{\mathfrak{p}\in\mathbb{P}(K)} |x|_\mathfrak{p} = \prod_{p\in\mathbb{P}(\mathbb{Q})} \prod_{\mathfrak{p}|p} |x|_\mathfrak{p},$$

on la divisibilitat d'elements de $\mathbb{P}(\mathbb{Q})$ per elements de $\mathbb{P}(K)$ cal entendre-la com a extensió de valors absoluts. Fixem-nos en els valors absoluts arquimedians de K i de $\mathbb{Q}$. Se satisfà la igualtat

$$\prod_{\sigma|\infty} |x|_\sigma = \prod_{\sigma \text{ real}} |\sigma(x)| \prod_{\sigma \text{ imaginària}} |\sigma(x)|^2 = \prod_{\sigma \text{ real}} |\sigma(x)| \prod_{\sigma \text{ imaginària}} |\sigma(x)||\overline{\sigma(x)}| = |\mathrm{N}(x)|_\infty,$$

on N denota la norma de l'extensió $K|\mathbb{Q}$ i $|\ |_\infty$ el valor absolut usual en $\mathbb{C}$. A més a més, per a tot ideal primer $\mathfrak{p}$ de l'anell d'enters de K se satisfà la igualtat $|x|_\mathfrak{p} = |\pi_\mathfrak{p}^{v_\mathfrak{p}(x)}|_\mathfrak{p}$, de manera que $|x|_\mathfrak{p} = |\pi_\mathfrak{p}|_\mathfrak{p}^{v_\mathfrak{p}(x)} = p^{-f(\mathfrak{p}|p)v_\mathfrak{p}(x)} = |p^{f(\mathfrak{p}|p)}|_p^{v_\mathfrak{p}(x)} = |\mathrm{N}(\mathfrak{p})|_p^{v_\mathfrak{p}(x)}$. D'altra banda, si prescindim del signe, la norma de x es pot escriure en la forma

$$\mathrm{N}(x) = \mathrm{N}\left(\prod_{p \text{ primer}} \prod_{\mathfrak{p}|p} \mathfrak{p}^{v_\mathfrak{p}(x)}\right) = \prod_{p \text{ primer}} \prod_{\mathfrak{p}|p} \mathrm{N}(\mathfrak{p})^{v_\mathfrak{p}(x)};$$

però el valor absolut p-àdic del producte $\prod_{\mathfrak{p}|\ell} \mathrm{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}$ quan $\ell \neq p$ és 1, ja que aquest producte només és divisible per potències de ℓ. Per tant, $|\mathrm{N}(x)|_p = \left|\prod_{\mathfrak{p}|p} \mathrm{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}\right|_p$. Això ens permet escriure, finalment, la cadena d'igualtats

$$\prod_{p \text{ primer}} \prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}} = \prod_{p \text{ primer}} \prod_{\mathfrak{p}|p} |\mathrm{N}(\mathfrak{p})|_p^{v_{\mathfrak{p}}(x)} = \prod_{p \text{ primer}} \left|\prod_{\mathfrak{p}|p} \mathrm{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}\right|_p = \prod_{p \text{ primer}} |\mathrm{N}(x)|_p .$$

En conseqüència, si afegim el producte per als valors absoluts arquimedians i tenim en compte la fórmula del producte per a $\mathbb{Q}$, i que $\mathrm{N}(x) \in \mathbb{Q}$, obtenim la fórmula desitjada. □

9.9 Ramificació i compleció

Siguin $L|K$ una extensió de cossos de nombres, $B|A$ l'extensió corresponent dels seus anells d'enters, $\mathfrak{P}$ un ideal primer no nul de B, i escrivim $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Hem definit anteriorment l'índex de ramificació $e(\mathfrak{P}|\mathfrak{p})$ i el grau residual $f(\mathfrak{P}|\mathfrak{p})$, i hem vist que aquests invariants es poden calcular a partir de la localització dels anells en l'ideal $\mathfrak{p}$. És a dir, que els invariants de ramificació es poden calcular localment.

D'altra banda, acabem d'aprendre a considerar les complecions dels cossos de nombres en els ideals primers no nuls dels seus anells d'enters. En particular, hem après a construir cossos $L_{\mathfrak{P}}$, compleció de L respecte del valor absolut $\mathfrak{P}$-àdic de L i $K_{\mathfrak{p}}$, compleció de K respecte del valor absolut $\mathfrak{p}$-àdic de K. A més a més, els cossos $L_{\mathfrak{P}}$ i $K_{\mathfrak{p}}$, són els cossos de fraccions de les complecions dels anells de valoració discreta localitzats de B en $\mathfrak{P}$ i de A en $\mathfrak{p}$, respectivament. Ens podem preguntar si hi ha alguna relació natural, i quina, entre els nombres de ramificació dels ideals $\mathfrak{P}$ i $\mathfrak{p}$ i les complecions dels anells.

Lema 9.9.1. *Existeix una única immersió de $K_{\mathfrak{p}}$ en $L_{\mathfrak{P}}$, de manera que $L_{\mathfrak{P}}$ és un cos extensió de $K_{\mathfrak{p}}$. A més a més, l'extensió $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ és una extensió finita.*

Demostració: Comencem per adonar-nos del fet que $L_{\mathfrak{P}}$ és un cos complet que conté K, ja que conté L, i que la restricció a K del valor absolut de $L_{\mathfrak{P}}$ és el valor absolut de K; per tant, $L_{\mathfrak{P}}$ conté la compleció de K respecte del seu valor absolut; és a dir, $L_{\mathfrak{P}}$ conté $K_{\mathfrak{p}}$.

D'altra banda, podem considerar $\alpha \in L$ un element primitiu de l'extensió $L|K$. Aleshores, obtenim la cadena d'inclusions de cossos $K_{\mathfrak{p}} \subseteq K_{\mathfrak{p}}(\alpha) \subseteq L_{\mathfrak{P}}$; i $K_{\mathfrak{p}}(\alpha)$ és un $K_{\mathfrak{p}}$-espai vectorial de dimensió finita menor o igual que el grau de l'extensió $L|K$ generat per les potències de α. Per tant, $K_{\mathfrak{p}}(\alpha)$, amb la restricció del valor absolut de $L_{\mathfrak{P}}$, és un $K_{\mathfrak{p}}$-espai vectorial normat de dimensió finita; en particular, $K_{\mathfrak{p}}(\alpha)$ és complet per a la topologia definida pel valor absolut de $L_{\mathfrak{P}}$. Ara bé, tot espai mètric complet és tancat, de manera que $K_{\mathfrak{p}}(\alpha)$ és un tancat que conté L, i que està inclòs en $L_{\mathfrak{P}}$; com que $L_{\mathfrak{P}}$ és la compleció de L, L és dens en $L_{\mathfrak{P}}$, de manera que $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\alpha)$; en conseqüència, l'extensió $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ és finita de grau menor o igual que el grau de l'extensió $L|K$. □

Observació 9.9.2. No cal pensar, però, que el grau és el mateix per a tots els valors absoluts $\mathfrak{P}$-àdics per als primers $\mathfrak{P}$ que divideixen $\mathfrak{p}$. De fet, això depèn de com descompon el polinomi $\mathrm{Irr}(\alpha, K)(X)$ en el cos $K_\mathfrak{p}$ i de quin factor prenem com a $\mathrm{Irr}(\alpha, K_\mathfrak{p})(X)$.

En particular, l'anell $\widehat{B}_\mathfrak{P}$, compleció de B en $\mathfrak{P}$, és un anell de valoració discreta complet que domina $\widehat{A}_\mathfrak{p}$; no només això, sinó que $\widehat{B}_\mathfrak{P}$ és la clausura entera de $\widehat{A}_\mathfrak{p}$ en $L_\mathfrak{P}$. Per a veure-ho, només cal demostrar que hi ha una única extensió a $L_\mathfrak{P}$ del valor absolut $\mathfrak{p}$-àdic de $K_\mathfrak{p}$. En efecte, ara disposem d'una extensió finita de cossos de fraccions d'anells de valoració discreta de manera que l'anell de $L_\mathfrak{P}$ domina l'anell de $K_\mathfrak{p}$; en particular, la clausura entera de $\widehat{A}_\mathfrak{p}$ en $L_\mathfrak{P}$ és un subanell de $\widehat{B}_\mathfrak{P}$, i aquest darrer anell n'és un localitzat. Però l'únic ideal primer de la clausura entera que divideix $\widehat{\mathfrak{p}}$ és l'ideal $\widehat{\mathfrak{p}}$, ja que per ser $K_\mathfrak{p}$ complet, hi ha una única extensió del seu valor absolut; per tant, la clausura entera és un anell local i, en conseqüència, coincideix amb el seu localitzat $\widehat{B}_\mathfrak{P}$.

D'altra banda, ja hem vist que els cossos residuals es conserven per compleció; en particular, el grau residual es conserva per compleció; és a dir, $f(\mathfrak{P}|\mathfrak{p}) = f(\widehat{\mathfrak{P}}|\widehat{\mathfrak{p}})$. A més a més, hem vist que la valoració $\mathfrak{P}$-àdica de L, normalitzada de manera que el grup de valors sigui $\frac{1}{e}\mathbb{Z}$, on $e := e(\mathfrak{P}|\mathfrak{p})$, és l'extensió a L de la valoració $\mathfrak{p}$-àdica de K, normalitzada de manera que el seu grup de valors és $\mathbb{Z}$; per tant, l'índex de ramificació es pot veure com l'índex del grup de valors de la valoració $\mathfrak{p}$-àdica en el grup de valors de la valoració $\mathfrak{P}$-àdica; o equivalentment, com l'índex del grup de valors del valor absolut $\mathfrak{p}$-àdic en el grup de valors del valor absolut $\mathfrak{P}$-àdic; com que aquests grups no canvien per compleció, obtenim que l'índex de ramificació es pot calcular com l'índex de ramificació en els anells compleció.

D'altra banda, en el cas dels cossos complets també se satisfà la fórmula $\sum_{i=1}^{g} e_i f_i = n$, ja que les extensions residuals coincideixen. Per tant, i com que ara només hi ha un ideal primer que divideix l'ideal primer de l'anell base, obtenim la fórmula $[L_\mathfrak{P} : K_\mathfrak{p}] = e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p})$.

Proposició 9.9.3. *Si l'extensió $L|K$ és de Galois de grup de Galois G, aleshores l'extensió $L_\mathfrak{P}|K_\mathfrak{p}$ també és de Galois i el grup de Galois és el grup de descomposició $G_{-1}(\mathfrak{P}|\mathfrak{p})$.*

Demostració: Sigui $\sigma \in G_{-1} := G_{-1}(\mathfrak{P}|\mathfrak{p})$. Com que $L_\mathfrak{P}$ és la compleció de L en $\mathfrak{P}$, σ s'estén per continuïtat a un automorfisme de $L_\mathfrak{P}$, de manera única. A més a més, la seva restricció a $K_\mathfrak{p}$ és la identitat, ja que és l'extensió a $K_\mathfrak{p}$ de la identitat de K. Dit d'una altra manera, tot element de G_{-1} dóna lloc a un element de $\mathrm{Gal}\,(L_\mathfrak{P}|K_\mathfrak{p})$; i dos elements diferents de G_{-1} donen lloc a elements diferents del grup de Galois, ja que actuen diferent en $L \subseteq L_\mathfrak{P}$. Però acabem de veure que el grau de l'extensió $L_\mathfrak{P}|K_\mathfrak{p}$ és exactament el producte $e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p})$, que és l'ordre del grup de descomposisió G_{-1}; per tant, $G_{-1}(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}\,(L_\mathfrak{P}|K_\mathfrak{p})$, com volíem demostrar. □

Observació 9.9.4. No és cert, en general, que tot element de G s'estengui per continuïtat a un automorfisme de $L_\mathfrak{P}$; de fet, s'estén per continuïtat a un isomorfisme de $L_\mathfrak{P}$ en $L_{\sigma(\mathfrak{P})}$, ja que la topologia $\mathfrak{P}$-àdica es transforma en la $\sigma(\mathfrak{P})$-àdica.

Corol·lari 9.9.5. *En la mateixa situació de la proposició anterior, els grups de ramificació superior coincideixen amb els de l'extensió $B|A$.*

DEMOSTRACIÓ: Només cal tenir en compte que els anells quocient $B_{\mathfrak{P}}/\mathfrak{P}^n$ es conserven per compleció i aplicar la definició. □

Ens interessa, ara, mirar-nos més de prop les complecions dels cossos de nombres en els ideals primers dels seus anells d'enters. Per a això és còmode disposar del resultat següent, que es pot entendre com una versió del Lema de Hensel.

Proposició 9.9.6 (Lema d'aixecament d'idempotents)**.** *Siguin A un anell de valoració discreta, K el seu cos de fraccions, i $\mathfrak{p} = \pi A$ el seu ideal maximal, i suposem que K és complet per a la topologia $\mathfrak{p}$-àdica. Sigui B una A-àlgebra (anell commutatiu) completa per a la topologia $\mathfrak{p}$-àdica; és a dir, suposem que per a tota successió $\{a_n\}_n$ d'elements de B tal que per a tot nombre natural n sigui $a_{n+1} - a_n \in \pi^n B$, existeix un element $a \in B$ de manera que $a - a_n \in \pi^n B$, també per a tot nombre natural n. Suposem que $e_1 \in B/\pi B$ és un element idempotent. Aleshores, existeix un element idempotent $E_1 \in B$ tal que $e_1 = E_1 + \pi B$. Si $e_1, e_2 \in B/\pi B$ són idempotents ortogonals, aleshores existeixen idempotents ortogonals $E_1, E_2 \in B$ tals que $e_i = E_i + \pi B$.*

DEMOSTRACIÓ: Observem la identitat polinòmica següent, vàlida a tot anell B, no necessàriament commutatiu, i per a tot nombre natural n:

$$1 = \big(X + (1-X)\big)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} X^{2n-i}(1-X)^i;$$

i considerem el polinomi de coeficients enters

$$f_n(X) := \sum_{i=0}^{n} \binom{2n}{i} X^{2n-i}(1-X)^i$$

(atenció al límit superior del sumatori!). Se satisfan les congruències

$$\begin{aligned} f_n(X) &\equiv 0 \pmod{X^n}, \\ f_n(X) &\equiv 1 \pmod{(1-X)^n}, \end{aligned}$$

de manera que, també,

$$\begin{aligned} f_{n+1}(X) &\equiv 0 \equiv f_n(X) \pmod{X^n}, \\ f_{n+1}(X) &\equiv 1 \equiv f_n(X) \pmod{(1-X)^n}; \end{aligned}$$

i, per tant,

$$f_{n+1}(X) \equiv f_n(X) \pmod{X^n(1-X)^n}. \tag{9.9.1}$$

D'altra banda,

$$\begin{aligned} f_n(X) &\equiv 0 \equiv f_n(X)^2 \pmod{X^n}, \\ f_n(X) &\equiv 1 \equiv f_n(X)^2 \pmod{(1-X)^n}, \end{aligned}$$

d'on es dedueix que

$$f_n(X) \equiv f_n(X)^2 \pmod{X^n(1-X)^n}. \tag{9.9.2}$$

Apliquem aquestes identitats al nostre problema. Donat l'idempotent $e_1 \in B/\pi B$, considerem un element qualsevol $b \in B$ tal que $e_1 = b + \pi B$. Com que $e_1 = e_1^2$, se satisfà que $b(1-b) = b - b^2 \in \pi B$ i, en elevar a n, que $b^n(1-b)^n \in \pi^n B$. La propietat (9.9.1) ens permet assegurar que la successió d'elements de B, $\{f_n(b)\}_n$, és de Cauchy i,

en conseqüència, convergent en B. Sigui $E_1 \in B$ un límit d'aquesta successió; aleshores, la propietat (9.9.2) ens permet assegurar que l'element E_1 és un idempotent de B; i com que $f_n(X) \equiv f_1(X) \equiv X \pmod{X(1-X)}$, també $f_n(b) \equiv b \pmod{\pi B}$, de manera que $e_1 = E_1 + \pi B$.

Per a la segona part, considerem els idempotents e_1, e_2, e_1+e_2 de $B/\pi B$; podem trobar un idempotent $E \in B$ tal que $E + \pi B = e_1 + e_2$ i elegir un element qualsevol $a \in B$ de manera que $a+\pi B = e_1$; sigui $b := EaE$. Aleshores, $b+\pi B = (e_1+e_2)e_1(e_1+e_2) = e_1$, per l'ortogonalitat de e_1 i e_2; en conseqüència, $b^2 - b \in \pi B$ i, en repetir l'argument anterior, $E_1 := \lim f_n(b)$ és un idempotent de B tal que $E_1 + \pi B = e_1$. Com que E és idempotent, i per definició de b, obtenim les igualtats $bE = b = Eb$, d'on deduïm que, per a tot nombre natural $n \geq 1$, se satisfan les igualtats $f_n(b)E = f_n(b) = Ef_n(b)$. Per tant, en el límit, $E_1E = E_1 = EE_1$. Sigui $E_2 := E - E_1$; aquesta propietat i el fet que E i E_1 són idempotents, ens permeten assegurar que també ho és E_2, que, a més a més, és ortogonal amb E_1, i se satisfà $E_2 + \pi B = e_2$, com volíem provar. □

Corol·lari 9.9.7 (Lema de Hensel)**.** *Siguin A un anell de valoració discreta, K el seu cos de fraccions, $\mathfrak{p} \subseteq A$ l'ideal maximal, $\overline{K} := A/\mathfrak{p}$ el cos residual, i suposem que K és complet per a la topologia $\mathfrak{p}$-àdica. Sigui $F(X) \in A[X]$ un polinomi mònic i sigui $f(X) = g(X)h(X)$ una factorització de $F(X)$ en $\overline{K}[X]$ amb $g(X), h(X)$ primers entre si. Aleshores, existeixen polinomis $G(X), H(X) \in A[X]$ tals que $g(X), h(X)$ són les reduccions mòdul $\mathfrak{p}$ dels polinomis $G(X), H(X)$, respectivament, i $F(X) = G(X)H(X)$.*

Demostració: Sigui $B := A[X]/(F(X))$; com que F és mònic, B és una A-àlgebra lliure de rang $n := \mathrm{gr}(F(X))$. A més a més, B és una A-àlgebra completa per a la topologia $\mathfrak{p}$-àdica, ja que aquesta topologia coincideix amb la topologia producte de A^n; per tant, podem aplicar la proposició. L'àlgebra $B/\mathfrak{p}B$ es pot calcular en la forma següent:

$$B/\mathfrak{p}B \cong A[X]/(\mathfrak{p}, F(X)) \cong \overline{K}[X]/(f(X)) \cong \overline{K}[X]/(g(X)) \times \overline{K}[X]/(h(X)),$$

i podem considerar els elements idempotents $e_1 := (1,0), e_2 := (0,1)$ que corresponen a aquesta descomposició de $B/\mathfrak{p}B$. Siguin $E_1, E_2 \in B$ idempotents ortogonals de B tals que $E_1+E_2 = 1$; l'existència la garanteix la demostració de la proposició, ja que podem triar E com qualsevol idempotent de B que redueixi a la suma $e_1 + e_2$. Aleshores B, com a anell, és la suma directa $B = BE_1 \oplus BE_2$. Sigui $\alpha \in B$ la imatge de X. El polinomi característic de α en B és $F(X)$, ja que $B = A[X]/(F(X))$; d'altra banda, és el producte dels polinomis característics de α en cada un dels factors BE_i. Aquests polinomis, posem $G'(X), H'(X)$, són mònics i, llevat del producte per una unitat del quocient $B/\mathfrak{p}$, redueixen als polinomis $g(X), h(X)$; per tant, si multipliquem $G'(X)$ per una unitat convenient de A i $H'(X)$ per la seva inversa, obtenim els polinomis $G(X), H(X)$ que volíem. □

Corol·lari 9.9.8. *En la mateixa situació del lema de Hensel, si $F(X)$ té una arrel simple mòdul $\mathfrak{p}$, aleshores té una arrel simple en A.*

Demostració: És suficient prendre $g(X) := X - b$, on b és una arrel simple de $F(X)$ mòdul $\mathfrak{p}$. □

Corol·lari 9.9.9. *Per a tot nombre priner p, el cos dels nombres racionals p-àdics, $\mathbb{Q}_p$, conté les arrels $(p-1)$-èsimes de la unitat.*

Demostració: En efecte, el cos residual és exactament $\mathbb{F}_p$, el cos de les arrels $(p-1)$-èsimes de la unitat. Per tant, el polinomi $X^{p-1}-1 \in \mathbb{Z}_p[X]$ té $p-1$ arrels simples diferents mòdul p. □

9.10 Lema de Krasner

Com que $\mathbb{F}_p$ només conté les arrel $(p-1)$-èsimes de la unitat, el cos $\mathbb{Q}_p$ no pot contenir totes les arrels de la unitat; de fet, només conté les arrels $(p-1)$-èsimes de la unitat, si $p \neq 2$, i les arrels quadrades, $1, -1$, si $p = 2$. En conseqüència, un cos complet respecte d'un valor absolut no arquimedià no ha de ser necessàriament algebraicament tancat. En aquesta secció es tracta d'estudiar la clausura algebraica d'un cos complet respecte d'un valor absolut no arquimedià.

Sigui K un cos complet respecte d'un valor absolut no arquimedià. Ja hem fet notar abans que si $L|K$ és una extensió finita, aleshores hi ha una única extensió a L del valor absolut de K i que L és complet respecte d'aquest valor absolut. Aquest resultat té una conseqüència immediata.

Corol·lari 9.10.1. *Sigui $\overline{K}$ una clausura algebraica fixa de K. Aleshores, existeix una única extensió del valor absolut de K a un valor absolut de $\overline{K}$.*

Demostració: Siguin $L_1|K$, $L_2|K$ subextensions finites de $\overline{K}|K$; la restricció a $L_1 \cap L_2$ dels valors absoluts de L_i extensió del valor absolut de K és la mateixa, en virtut de la unicitat de l'extensió del valor absolut de K a una extensió finita. Per tant, podem definir en $\overline{K}$ un valor absolut prenent com a valor absolut d'un element $x \in \overline{K}$ el valor absolut $|x|$, on $|\ |$ denota l'extensió a $K(x)$ del valor absolut de K. La comprovació dels axiomes de valor absolut és immediata. Per a la unicitat, només cal tenir en compte que aquest valor absolut està determinat pel valor absolut en les subextensions finites, i aquest és únic. □

Corol·lari 9.10.2. *Sigui α un element algebraic sobre K. Per a tota K-immersió σ de $K(\alpha)$ en $\overline{K}$ és $|\sigma(\alpha)| = |\alpha|$. En particular, si $n := [K(\alpha) : K]$, és $|\alpha| = |\mathrm{N}(\alpha)|^{1/n}$, on $|\mathrm{N}(\alpha)|$ és el valor absolut original de K.*

Demostració: Sigui $L|K$ una clausura normal de $K(\alpha)|K$; si σ és un K-automorfisme de L, podem definir un valor absolut en L que estén el valor absolut de K per la fórmula $|x|_\sigma := |\sigma(x)|$, per a tot element $x \in L$; la unicitat del valor absolut de L ens permet assegurar que $|\sigma(\alpha)| = |\alpha|$. Això demostra la primera part i, en conseqüència, de la igualtat

$$|\mathrm{N}(\alpha)| = \prod_\sigma |\sigma(\alpha)|,$$

obtenim la segona. □

En general, donat un cos K i una extensió monògena finita, $K(\alpha)|K$, no hi ha criteris per a obtenir altres elements primitius per a l'extensió $K(\alpha)|K$. El lema de Krasner proporciona un d'aquests criteris en el cas que K és complet respecte d'un valor absolut no arquimedià.

Proposició 9.10.3 (Lema de Krasner)**.** *Siguin $\alpha, \beta \in \overline{K}$ tals que α és separable sobre $K(\beta)$. Suposem que per a tots els conjugats, $\sigma(\alpha) \neq \alpha$, de α sobre K, se satisfà que $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. Aleshores, $\alpha \in K(\beta)$.*

Demostració: Sigui τ una $K(\beta)$-immersió de $K(\alpha, \beta)$ en $\overline{K}$. Per la unicitat de l'extensió del valor absolut de K, se satisfà la igualtat $|\beta - \tau(\alpha)| = |\tau(\beta - \alpha)| = |\beta - \alpha|$; per tant, per a tota K-immersió σ de $K(\alpha)$ en $\overline{K}$, $\sigma \neq \mathrm{id}$, se satisfà la desigualtat $|\beta - \tau(\alpha)| < |\sigma(\alpha) - \alpha|$.

En conseqüència, $|\tau(\alpha)-\alpha| \leq \max(|\tau(\alpha)-\beta|, |\beta-\alpha|) < |\sigma(\alpha)-\alpha|$. Però això ens permet assegurar que $\tau(\alpha) = \alpha$, de manera que τ és la identitat en $K(\alpha, \beta)$. Això és dir que $K(\alpha, \beta) \subseteq K(\beta)$, de manera que $\alpha \in K(\beta)$, com volíem provar. □

Observació 9.10.4. En particular, quan per a $\beta \in K(\alpha)$ se satisfan les desigualtats $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$, aleshores $K(\beta) = K(\alpha)$.

El lema de Krasner admet una formulació més útil a la pràctica. Abans, però, establirem alguns resultats previs. Si $f := a_0 + a_1X + \cdots + a_nX^n \in K[X]$ és un polinomi qualsevol, posarem $|f| := \max(|a_0|, \ldots, |a_n|)$. El resultat següent generlitza el corresponent, ben conegut, del cas complex per al valor absolut arquimedià.

Lema 9.10.5. *Sigui $g := b_0 + b_1X + \cdots + b_nX^n \in K[X]$, amb $b_n \neq 0$, i sigui $\beta \in \overline{K}$ una arrel de g. Aleshores, $|\beta| \leq \max(|b_0b_n^{-1}|, \ldots, |b_{n-1}b_n^{-1}|, 1)$.*

Demostració: Si $\beta = 0$, no hi ha res a provar. Si $|\beta| < 1$, ja hem acabat; en cas contrari, $|\beta^{-1}| < 1$ i podem escriure la igualtat

$$|\beta| = |b_n^{-1}||b_0\beta^{1-n} + b_1\beta^{2-n} + \cdots + b_{n-2}\beta^{-1} + b_{n-1}|,$$

d'on es dedueix que $|\beta| \leq \max(|b_i||b_n|^{-1}|\beta^{i+1-n}| : 0 \leq i \leq n-1)$, d'on la desigualtat que volíem, ja que $|\beta^{-1}| < 1$. □

Observació 9.10.6. En particular, si g és mònic, aleshores $|\beta| \leq |g|$.

Siguin $\alpha_1, \ldots, \alpha_n$ totes les arrels de f, i suposem que f, g són mònics. Suposem que $|f-g| < \varepsilon < 1$; aleshores, $|g| = |f + (g-f)| \leq \max(|f|, \varepsilon) = |f|$, ja que 1 és un coeficient de f i, per tant, $|f| \geq 1$; en virtut del lema, les arrels de g estan fitades per $|f|$. En conseqüència, si β és una arrel de g, les potències $1, \beta, \ldots, \beta^{n-1}$, estan fitades per $|f|^{n-1}$; per tant, $|f(\beta)| = |f(\beta) - g(\beta)| < |f|^{n-1}\varepsilon$. És a dir, si g és a prop de f, el valor de f en una arrel β de g és a prop de zero; per tant, la continuïtat de les funcions polinòmiques ens permet assegurar que β és a prop d'una arrel de f, diem $\alpha := \alpha_1$. En particular, la distància de β a les altres arrels (diferents de α) de f és fitada inferiorment.

Entre els polinomis g tals que $|f-g| < \varepsilon$, sempre n'hi ha de separables, ja que la condició d'inseparabilitat d'un polinomi g és donada per l'anul·lació del resultant de g (cf. [Tra 2020]) i el seu derivat, g', que és una condició polinòmica en els coeficients de g i, per tant, aquest resultant no pot ser idènticament nul en un entorn obert de f. En efecte, podem identificar el conjunt dels polinomis mònics de $K[X]$ i de grau n amb l'espai vectorial normat K^n amb la norma del suprem; aleshores, els polinomis g tals que $|g-f| < \varepsilon$ formen la bola oberta de radi ε d'aquest espai normat, mentre que la condició d'anul·lació del resultant defineix una hipersuperfície en K^n; per tant, un subespai de dimensió estrictament inferior. Cal tenir en compte que K no pot ser finit, ja que l'únic valor absolut possible en un cos finit és el valor absolut trivial perquè està format per arrels de la unitat.

Aquesta propietat ens permet assegurar que si r és la multiplicitat de α com a arrel de f, aleshores hi ha exactament r arrels de g que s'apropen a α i mantenen distància fitada inferiorment amb les altres arrels de f; en efecte, en cas contrari podríem construir una successió de polinomis separables g amb tantes arrels que s'apropen a α com les del polinomi g de partida i de límit f; per pas al límit, α no podria ser de multiplicitat r.

En resum, si g és un polinomi proper a f, el nombre d'arrels de g properes a α coincideix amb la multiplicitat de α com a arrel de f.

Una conseqüència d'això és la següent formulació del lema de Krasner.

Proposició 9.10.7. *Siguin $f(X)$, $g(X) \in K[X]$ polinomis mònics i del mateix grau, i suposem que $f(X)$ és irreductible i separable i que $|f-g|$ és petit. Aleshores, g també és irreductible. A més a més, per a tota arrel α de f en $\overline{K}$ existeix una arrel β de g tal que $K(\beta) = K(\alpha)$.*

Demostració: Com que f és separable, si g és prou a prop de f aleshores g és separable i les seves arrels s'apropen a les de f. Ara, si β és una arrel de g prou a prop de l'arrel α de f, el lema de Krasner ens permet assegurar que $K(\alpha) \subseteq K(\beta)$; com que $[K(\alpha) : K] = n$ i g és mònic de grau n, se satisfà la igualtat i, en conseqüència, g també és irreductible. □

Una aplicació senzilla i, alhora, interessant, és el resultat següent.

Corol·lari 9.10.8. *Sigui L un cos extensió finita de $\mathbb{Q}_p$. Aleshores, existeix un cos de nombres K, inclòs en L, de grau $[K : \mathbb{Q}] = [L : \mathbb{Q}_p]$, i dens en L. En particular, $L = K\mathbb{Q}_p$.*

Demostració: Siguin α un element primitiu de l'extensió $L|\mathbb{Q}_p$ i $f(X) := \mathrm{Irr}(\alpha, \mathbb{Q}_p)(X)$. Qualsevol polinomi g prou proper a f té una arrel β que defineix la mateixa extensió $L|\mathbb{Q}_p$; i per ser $\mathbb{Q}$ dens en $\mathbb{Q}_p$, podem prendre g de coeficients racionals. Aleshores, podem prendre $K := \mathbb{Q}(\beta)$ i, clarament, és $L = \mathbb{Q}_p(\beta) = K\mathbb{Q}_p$. La densitat de K en L es dedueix del fet que la compleció de K en l'ideal contracció al seu anell d'enters de l'ideal primer de L conté K i $\mathbb{Q}_p$, de manera que conté $L = \mathbb{Q}_p(\beta)$; però essent L complet, L ha de contenir aquesta compleció; per tant, L és la compleció de K en un cert ideal del seu anell d'enters, de manera que K és dens en L. □

Observació 9.10.9. En particular, tot cos L extensió finita de $\mathbb{Q}_p$ és la compleció d'un cos de nombres K respecte de la topologia definida per la valoració $\mathfrak{p}$-àdica associada a un ideal primer no nul $\mathfrak{p}$ de l'anell d'enters de K; i com que L conté la compleció de $\mathbb{Q}$ respecte de la topologia p-àdica, aquest ideal primer ha de dividir $p\mathbb{Z}$.

Com a aplicació del lema de Krasner podem establir l'existència, per a cada n donat, de només un nombre finit d'extensions d'un cos $\mathfrak{p}$-àdic de grau n. Per a centrar una mica més la qüestió, observem que els cossos algebraicament tancats no tenen extensions finites no trivials, que els cossos finits tenen exactament una extensió de grau n per a cada enter $n \geq 1$, i que els cossos de nombres tenen un conjunt infinit d'extensions de cada grau $n > 1$. Els cossos extensió finita de $\mathbb{Q}_p$ ocupen un lloc intermedi, des d'aquest punt de vista, entre els cossos finits i els cossos de nombres.

Proposició 9.10.10. *Sigui $K|\mathbb{Q}_p$ una extensió finita. Donat un enter $n > 1$, el conjunt de les extensions de K de grau n incloses en una clausura algebraica fixa de $\mathbb{Q}_p$ és finit.*

Demostració: Si $L|K$ és una extensió finita, i si A i B són els anells dels enters de K, L, respectivament, podem elegir un element primitiu β de $L|K$ tal que $\beta \in B$. A més a més, si $[L : K] = n$, el polinomi irreductible $\mathrm{Irr}(\beta, K)(X)$ pertany a $A[X]$. Podem identificar, però, el conjunt dels polinomis mònics de $A[X]$ de grau n amb l'espai topològic A^n. Ara, el lema de Krasner ens permet obtenir un recobriment obert de A^n assignant a cada punt de A^n un entorn de manera que tots els polinomis de l'entorn defineixin la

mateixa extensió de K; com que A és un anell compacte, aquest recobriment admet un subrecobriment finit, de manera que tota extensió de K de grau n és determinada per un polinomi elegit entre un conjunt finit de possibilitats (per exemple, els centres de les boles obertes determinades pel subrecobriment finit). És a dir, hi ha només un nombre finit d'extensions finites $L|K$ de grau donat n. □

Observació 9.10.11. Notem que, en el cas dels cossos de nombres, els teoremes de finitud són basats en l'estudi de la geometria dels nombres; més concretament, en el teorema de Minkowski (cf. **4.2.4**) que, alhora, es basa en propietats de compacitat. En aquest cas dels cossos $\mathfrak{p}$-àdics, la finitud també es basa en propietats de compacitat.

9.11 El cos $\mathbb{C}_p$

Hem construït un cos compleció de $\mathbb{Q}$ per al valor absolut p-àdic; per tant, ja estem en disposició de fer-hi anàlisi amb prou solvència. Però el cos no és algebraicament tancat. I la clausura algebraica de $\mathbb{Q}_p$ no és pas complet (cf. més avall). Ara ja podem construir l'anàleg del cos $\mathbb{C}$ dels nombres complexos per a la topologia p-àdica. Recordem que busquem construir un cos complet i algebraicament tancat.

Notem, en primer lloc, que $\mathbb{Q}_p$ no és algebraicament tancat. En efecte, les úniques arrels de la unitat de $\mathbb{Q}_p$ d'ordre primer amb p són les arrels $(p-1)$-èsimes de la unitat, en virtut del lema de Hensel; per tant, $\mathbb{Q}_p$ no pot ser algebraicament tancat.

D'altra banda, si considerem una clausura algebraica de $\mathbb{Q}_p$, $\overline{\mathbb{Q}}_p$, i estenem el valor absolut p-àdic a aquest cos de l'única manera que podem fer-ho, obtenim que $\overline{\mathbb{Q}}_p$ no és complet. En efecte, això es dedueix immediatament del resultat següent.

Lema 9.11.1. *Per a tot enter $n \geq 1$ sigui $a_n \in \overline{\mathbb{Q}}_p$ l'element definit de la manera següent:*

$$a_n := \begin{cases} \zeta_n, & \text{si } p \text{ no divideix } n, \\ 1, & \text{si } p \text{ divideix } n, \end{cases}$$

on ζ_n designa una arrel primitiva n-èsima de la unitat en $\overline{\mathbb{Q}}_p$. Aleshores, la sèrie $\sum_{n\geq 1} a_n p^n$ no és convergent en $\overline{\mathbb{Q}}_p$, però, en canvi, satisfà la condició de Cauchy.

Demostració: Com que els coeficients a_n són arrels de la unitat, se satisfà immediatament que $|a_n| = 1$ per a tot $n \geq 1$; per tant, $a_n p^n$ tendeix a zero per al valor absolut p-àdic; és a dir, la successió de sumes parcials de la sèrie satisfà la condició de Cauchy, ja que el valor absolut és no arquimedià. Suposem que la sèrie és convergent en $\overline{\mathbb{Q}}_p$; es tracta d'arribar a contradicció. Sigui α la suma de la sèrie; aleshores, α és algebraic sobre $\mathbb{Q}_p$ i, en conseqüència, existeix un cos K, extensió finita de $\mathbb{Q}_p$, tal que $\alpha \in K$. Anem a veure, per inducció, que K conté tots els coeficients a_n de la sèrie. En efecte, suposem que K conté els coeficients $a_1, \ldots, a_{n-1}$. Si n és divisible per p, aleshores $a_n = 1 \in K$ i ja hem acabat; en cas contrari, podem considerar l'element $\beta \in K$ definit per la igualtat

$$p^n \beta = \alpha - \sum_{m=0}^{n-1} a_m p^m.$$

Clarament, $\beta \equiv a_n = \zeta_n \pmod{p}$. Apliquem el lema de Hensel: el polinomi $X^n - 1$ és separable en una clausura algebraica del cos residual de K, ja que aquest cos residual és una extensió finita de $\mathbb{F}_p$, el cos residual de $\mathbb{Q}_p$; en conseqüència, les arrels n-èsimes de la unitat són totes diferents en $\overline{\mathbb{F}}_p$. D'altra banda, la reducció de β és una arrel de $X^n - 1$ en el cos residual de K; per tant, l'anell de la valoració de K conté una arrel de $X^n - 1$ que coincideix mòdul p amb β; en conseqüència, K conté una arrel primitiva n-èsima de la unitat i, per tant, $a_n \in K$. Però això és contradictori; en efecte, si $a_n \in K$ per a tot enter $n \geq 1$, aleshores K contindria una infinitat d'arrels de la unitat d'ordre no divisible per p; com que aquestes arrels són diferents en $\overline{\mathbb{F}}_p$, el cos residual de K hauria de ser infinit i, en canvi, és una extensió finita de $\mathbb{F}_p$. □

Definició 9.11.2. Denotarem per $\mathbb{C}_p$ la compleció de $\overline{\mathbb{Q}}_p$ respecte del valor absolut p-àdic.

Ara obtenim un cos complet; però, algebraicament tancat? La resposta és afirmativa.

Proposició 9.11.3. *El cos $\mathbb{C}_p$, compleció de $\overline{\mathbb{Q}}_p$ respecte del valor absolut p-àdic, és algebraicament tancat.*

Demostració: Es tracta de veure que tot element algebraic sobre $\mathbb{C}_p$ ja pertany a $\mathbb{C}_p$. Siguin, doncs, α un element algebraic sobre $\mathbb{C}_p$ i $f(X) := \mathrm{Irr}(\alpha, \mathbb{C}_p)(X) \in \mathbb{C}_p[X]$ el polinomi mònic irreductible que té α com a arrel. Com que $\overline{\mathbb{Q}}_p$ és dens en $\mathbb{C}_p$, podem elegir un polinomi $g(X) \in \overline{\mathbb{Q}}_p[X]$ tal que $|f - g|$ sigui tan petit com vulguem. Aleshores, $|g(\alpha)| = |g(\alpha) - f(\alpha)|$ és tan petit com vulguem: en particular, g té una arrel més propera a α que els conjugats de α (diferents de α); si la designem per $\beta \in \overline{\mathbb{Q}}_p$, el lema de Krasner ens permet assegurar que $\alpha \in \mathbb{C}_p(\beta)$; però com que $\beta \in \overline{\mathbb{Q}}_p \subseteq \mathbb{C}_p$, és $\mathbb{C}_p(\beta) = \mathbb{C}_p$, de manera que $\alpha \in \mathbb{C}_p$, com volíem demostrar. □

Així, disposem d'un cos algebraicament tancat i complet per a la topologia p-àdica. De vegades se l'anomena el cos dels nombres complexos p-àdics.

Observació 9.11.4. Si es repassa la construcció de la compleció d'un cos dotat d'un valor absolut i se suposa que aquest cos és numerable o bé té cardinal menor o igual que la potència del continu, hom s'adona que el cos compleció és de cardinal potència del continu. D'altra banda, el pas d'un cos no finit a una clausura algebraica no modifica el cardinal. En conseqüència, el cos $\mathbb{C}_p$ és de cardinal la potència del continu. En particular, és la clausura algebraica d'un cos extensió transcendent pura de $\mathbb{Q}$ amb una base de transcendència de cardinal la potència del continu, igual que $\mathbb{C}$. Per tant, $\mathbb{C}_p$ és isomorf a $\mathbb{C}$ com a cos; però només com a cos!, no com a espai topològic!

Anàlogament, també $\overline{\mathbb{Q}}_p$ és algebraicament tancat i de cardinal la potència del continu; per tant, també! és isomorf a $\mathbb{C}$ i a $\mathbb{C}_p$ com a cos; però no com a espai topològic: en un cas, perquè la topologia no és arquimediana; en l'altre cas, perquè no és complet.

9.12 Funcions p-àdiques

Aquesta secció es dedica a la introducció i l'estudi d'algunes funcions p-àdiques. Concretament, de les funcions exponencial i logarítmica. Començarem per estudiar la funció exponencial.

Definició 9.12.1. Anomenarem exponencial la sèrie de potències

$$\exp(X) := \sum_{n\geq 0} \frac{1}{n!} X^n \in \mathbb{Q}[[X]].$$

Si pensem en $\mathbb{C}$ amb la topologia usual, la sèrie exponencial té radi de convergència $+\infty$, de manera que defineix una funció a tot $\mathbb{C}$. En el cas de $\mathbb{C}_p$ això no és pas d'aquesta manera. De fet, ni tan sols és convergent en la bola unitat. En efecte, notem que $p^{\frac{-1}{p-1}} < 1$ i que se satisfà el resultat següent.

Lema 9.12.2. *El radi de convergència de la sèrie exponencial en $\mathbb{C}_p$ és $p^{\frac{-1}{p-1}}$.*

Demostració: Fixat un nombre natural n, la valoració p-àdica de $n!$ és donada per la fórmula

$$v_p(n!) = \sum_{i\geq 1} \left[\frac{n}{p^i}\right].$$

En efecte, la quantitat de nombres enters entre 1 i n que són divisibles per p^i és exactament la part entera del quocient n/p^i; per tant, el sumand $\left[\frac{n}{p^i}\right]$ afegeix una unitat per a cada un d'aquests nombres enters; però les altres $i-1$ unitats ja han estat afegides en els sumands $\left[\frac{n}{p^j}\right]$ per a $j < i$. Ara, les desigualtats $\left[\frac{n}{p^i}\right] \leq \frac{n}{p^i}$, permeten escriure immediatament que

$$v_p(n!) \leq \sum_{i\geq 1} \frac{n}{p^i} < \frac{n}{p-1}.$$

D'altra banda, per a $p^i \leq n < p^{i+1}$ i per a $1 \leq j \leq i$ podem escriure que $\frac{n}{p^j} - 1 \leq \left[\frac{n}{p^j}\right]$, de manera que, per a tot nombre natural $i \geq 1$, és $\frac{n}{p} + \cdots + \frac{n}{p^i} - i \leq v_p(n!)$; però se satisfà la desigualtat

$$\frac{n}{p} + \cdots + \frac{n}{p^i} - i = \frac{n}{p-1} - \frac{np^{-i}}{p-1} - i > \frac{n-p}{p-1} - \frac{\log n}{\log p},$$

on log indica aquí el logaritme real usual (en qualsevol base). Per tant, obtenim les desigualtats

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

que, en termes de valor absolut p-àdic normalitzat de manera que $|p| = p^{-1}$, podem escriure en la forma $p^{-\frac{1}{p-1}} < |n!|^{1/n} < p^{-\frac{1-\frac{p}{n}}{p-1} + \frac{\log n}{n \log p}}$. En prendre límit, obtenim la igualtat $p^{-\frac{1}{p-1}} = \lim |n!|^{1/n}$, ja que $\lim p^{-\frac{1-\frac{p}{n}}{p-1} + \frac{\log n}{n \log p}} = p^{-\frac{1}{p-1}}$; i la fórmula d'Hadamard per al càlcul del radi de convergència d'una sèrie de potències ens permet assegurar que el radi de convergència de la sèrie $\exp(X)$ en $\mathbb{C}_p$ és $p^{\frac{-1}{p-1}}$. □

En conseqüència, podem definir la funció exponencial p-àdica en el disc obert de radi $p^{\frac{-1}{p-1}}$ de $\mathbb{C}_p$; és una funció que pren valors en $\mathbb{C}_p$ i que satisfà les propietats usuals de l'exponencial

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

sempre que x, y estan en el disc de convergència. En efecte, això es dedueix immediatament del fet que la sèrie exponencial, com a tal sèrie formal, satisfà les dues propietats enunciades.

Observació 9.12.3. En particular, té sentit parlar de $\exp(p)$, si $p \neq 2$ i de $\exp(4)$ quan $p = 2$, però no en té parlar de $\exp(1)$, per exemple. Encara que podríem definir $\exp(1)$ com una arrel p^2-èsima de $\exp(p^2)$, això no donaria una definició unívoca de $\exp(1)$, sinó només mòdul el producte per una arrel primitiva p-èsima de la unitat.

Definició 9.12.4. Anomenarem sèrie logaritme la sèrie de potències

$$\log(1+X) := \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} X^n \in \mathbb{Q}[[X]].$$

Anàlogament, se satisfà la propietat formal

$$\log(1+X) + \log(1+Y) = \log(1+X+Y+XY) = \log((1+X)(1+Y)),$$

així com els fets que $\exp(\log(1+X)) = 1+X$ i $\log(\exp(X)) = X$; aquestes propietats tenen sentit a nivell formal ja que podem substituir les sèries que no tenen terme constant. Recordem que el radi de convergència de la sèrie logaritme en $\mathbb{C}$ és 1. Això succeeix també en el cas de $\mathbb{C}_p$.

Proposició 9.12.5. *El radi de convergència en $\mathbb{C}_p$ de la sèrie logaritme és* 1.

Demostració: Per a tot nombre enter $n \geq 1$ i per a la valoració p-àdica de n se satisfan les desigualtats $0 \leq v_p(n) \leq \dfrac{\log n}{\log p}$, de manera que la fórmula d'Hadamard ens permet concloure com abans. □

En conseqüència, podem definir una funció en el disc obert de $\mathbb{C}_p$ de radi 1 per la fórmula

$$\log_p(1+x) := \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n.$$

Anomenarem a aquesta funció el logaritme p-àdic. Se satisfan les propietats formals del logaritme que hem indicat més amunt, sempre que x, y pertanyin al disc de convergència. De totes maneres, podem estendre el logaritme a una funció definida en tot ${\mathbb{C}_p}^*$. Però, per a això, convé estudiar, prèviament, l'estructura del grup multiplicatiu ${\mathbb{C}_p}^*$.

Proposició 9.12.6. *Siguin W el grup de les arrels de la unitat d'ordre no divisible per p, i $U_1 := \{x \in \mathbb{C}_p : |x-1| < 1\}$, la bola oberta de radi 1 i centre en 1 de $\mathbb{C}_p$. Aleshores, U_1 és un subgrup multiplicatiu de ${\mathbb{C}_p}^*$ i ${\mathbb{C}_p}^*$ admet una descomposició en producte directe de la forma*

$${\mathbb{C}_p}^* = p^{\mathbb{Q}} \times W \times U_1,$$

on $p^{\mathbb{Q}}$ indica un subgrup de ${\mathbb{C}_p}^*$ isomorf al grup additiu dels nombres racionals i format per les potències racionals de p.

Demostració: Cal definir precisament el subgrup $p^{\mathbb{Q}}$. De fet, per a cada nombre racional r, podem prendre el nombre real positiu p^r, que és un nombre algebraic; si ara prenem una immersió de $\overline{\mathbb{Q}}$ en $\mathbb{C}_p$, obtenim un subgrup de ${\mathbb{C}_p}^*$, $p^{\mathbb{Q}}$, ja que en $\mathbb{R} \cap \overline{\mathbb{Q}}$ se satisfan les

igualtats $p^r p^s = p^{r+s}$ per a tota parella de nombres racionals r, s. Observem, però, que el subgrup $p^{\mathbb{Q}}$ no està definit de manera canònica: depèn de la immersió de $\overline{\mathbb{Q}}$ en $\mathbb{C}_p$.

Sigui $\alpha \in {\mathbb{C}_p}^*$. Com que $\overline{\mathbb{Q}}_p$ és dens en $\mathbb{C}_p$, podem prendre $a \in \overline{\mathbb{Q}}_p$ de manera que $|a| = |\alpha|$; com que el grup de valors de la valoració real de $\overline{\mathbb{Q}}_p$ extensió de la valoració p-àdica de $\mathbb{Q}_p$ és exactament $\mathbb{Q}$, el valor absolut de a és una potència racional de p. Dit d'una altra manera, existeix $r \in \mathbb{Q}$ tal que $|\alpha| = p^r$; però, com que $p^r \in \mathbb{C}_p$ té valor absolut p^{-r}, obtenim que $|\alpha p^r| = 1$; és a dir, podem escriure tot element de $\mathbb{C}_p$ com el producte d'un element de $p^{\mathbb{Q}}$ per un element de valor absolut 1 de manera única, ja que p^r és determinat de manera única en $p^{\mathbb{Q}}$ pel valor absolut de α. Resta veure que el subgrup de ${\mathbb{C}_p}^*$ format pels elements de valor absolut 1 és el producte directe de W i U_1.

Sigui, doncs, $\alpha \in {\mathbb{C}_p}^*$ un element de valor absolut 1; igual que abans, podem prendre un element $a \in \overline{\mathbb{Q}}_p$ tal que $|\alpha - a| < 1$, de manera que $|a| = |\alpha| = 1$. En particular, a és un element invertible de l'anell de valoració $\overline{\mathbb{Z}}_p$ de $\overline{\mathbb{Q}}_p$; per tant, a és congru a una arrel de la unitat d'ordre no divisible per p mòdul l'ideal de la valoració, ja que aquest cos residual és, clarament, un subcòs de $\overline{\mathbb{F}}_p$ (de fet és tot $\overline{\mathbb{F}}_p$), per ser la reunió (límit inductiu) dels cossos residuals de les extensions finites de $\mathbb{Q}_p$. És a dir, existeix un element $\omega \in W$ tal que $|a - \omega| < 1$; en conseqüència, també $|\alpha - \omega| < 1$ i, per tant, $|\alpha\omega^{-1} - 1| < 1$. Dit d'una altra manera, podem trobar una arrel de la unitat d'ordre no divisible per p tal que α és el producte d'aquesta arrel de la unitat per un element de U_1; i l'arrel de la unitat està determinada unívocament per la seva reducció mòdul l'ideal de la valoració; per tant, la descomposició és única i el resultat desitjat queda provat. □

Corol·lari 9.12.7. *Existeix una única funció* $\log_p$ *definida en* ${\mathbb{C}_p}^*$ *que satisfà les propietats següents:*

(a) $\log_p(p) = 0$*;*

(b) *per a tota parella d'elements* $\alpha, \beta \in {\mathbb{C}_p}^*$*, és* $\log_p(\alpha\beta) = \log_p(\alpha) + \log_p(\beta)$*; i*

(c) *per a tot element* $\alpha \in \mathbb{C}_p$ *tal que* $|\alpha| < 1$*,* $\log_p(1+\alpha)$ *és donat per la suma de la sèrie de potències* $\log(1+X)$ *en* $X = \alpha$*.*

Demostració: Com que, en subsituir X per 0 a la sèrie, tenim que $\log_p(1) = 0$, la propietat (b) obliga que $\log_p(\omega) = 0$ per a tota arrel de la unitat, ω. Per tant, les condicions (a) i (b) obliguen que el logaritme sigui nul en el subgrup $p^{\mathbb{Q}} \times W$. Així, en tenir en compte l'estructura de ${\mathbb{C}_p}^*$ que acabem de provar, només cal definir $\log_p$ en U_1; però això ja està fet per la sèrie de potències, que determina el valor $\log_p(x) = \log_p(1+(x-1))$ per a $|x-1| < 1$; és a dir, per a $x \in U_1$. □

Tot i que se satisfan les propietats formals $\exp(\log(1+X)) = 1+X$ i $\log(\exp(X)) = X$, no podem afirmar que això sigui així per a les funcions p-àdiques corresponents; de fet, això només succeeix en el disc obert $|x| < p^{\frac{-1}{p-1}}$. Observem que aquest és el domini de convergència de la funció exp. Per a veure aquest fet necessitarem estudiar una mica més les funcions exp i $\log_p$.

Lema 9.12.8. *Si* $|x| < p^{\frac{-1}{p-1}}$*, aleshores* $|\log_p(1+x)| = |x|$*. Si* $|x| = p^{\frac{-1}{p-1}}$*, aleshores* $|\log_p(1+x)| \leq |x|$*.*

Demostració: Per a tot nombre enter $n \geq 1$ se satisfà la desigualtat $|n| \geq 1/n$, ja que $n|n| = np^{-v_p(n)} \in \mathbb{N} - \{0\}$. A més a més, si $1 \leq n < p$, aleshores $|n| = 1$. Per tant, per

a $|x| < p^{\frac{-1}{p-1}}$ és $|x| < 1$ i $\left|\frac{x^n}{n}\right| \begin{cases} = |x|^{n-1}|x| < |x|, & \text{si } 2 \leq n < p, \\ < np^{\frac{1-n}{p-1}}|x| \leq |x|, & \text{si } n \geq p, \end{cases}$ ja que la successió de terme general $np^{\frac{1-n}{p-1}}$ és decreixent per a $n \geq p$ i val 1 per a $n = p$. En conseqüència, i com que el valor absolut és no arquimedià, totes les sumes parcials $\sum_{n=1}^{k} \frac{(-1)^{n+1}}{n} x^n$ són de valor absolut igual a $|x|$, que és el del primer sumand; és a dir, $\log_p(1+x)$ és el límit d'una successió de Cauchy d'elements del tancat definit per la condició $|x'| = |x|$. Com que $\mathbb{C}_p$ és un espai mètric complet, tot subconjunt tancat és complet i el límit de la successió pertany a aquest tancat. Això demostra que $|\log_p(1+x)| = |x|$, en el cas que $|x| < p^{\frac{-1}{p-1}}$.

En el cas que la hipòtesi sigui $|x| \leq p^{\frac{-1}{p-1}}$, les desigualtats estrictes de més amunt es converteixen en $\leq$, de manera que l'argument continua essent vàlid en la bola tancada de radi $|x|$; per tant, obtenim el resultat enunciat. □

Corol·lari 9.12.9. *Per a $|x| < p^{\frac{-1}{p-1}}$ és $\log_p(\exp(x)) = x$ i $\exp(\log_p(1+x)) = 1+x$.*

Demostració: Ja sabem que les igualtats se satisfan a nivell de sèries formals de potències; per tant, només cal comprovar la convergència. Ara, com que per a tot natural n és $v_p(n!) < \frac{n}{p-1}$, la hipòtesi ens permet assegurar que $\left|\frac{x^n}{n!}\right| < 1$ per a tot $n \geq 1$, de manera que

$$\exp(x) - 1 = \sum_{n \geq 1} \frac{1}{n!} x^n$$

convergeix a un element de valor absolut menor estricte que 1. En efecte, la bola oberta de radi 1 és un subgrup topològic additiu obert, de manera que és tancat. En conseqüència, $\exp(x)$ i $\log_p(\exp(x))$ són convergents, de manera que se satisfà la propietat desitjada $\log_p(\exp(x)) = x$.

D'altra banda, el lema anterior ens permet assegurar on la sèrie $\exp(\log_p(1+x))$ és convergent, ja que $|x| < p^{\frac{-1}{p-1}}$ implica que $|\log_p(1+x)| = |x|$; per tant, l'altra igualtat. □

Observació 9.12.10. Sempre que l'exponencial és convergent, se satisfà la igualtat $\log_p(\exp(x)) = x$; però això no és cert per a l'altra igualtat. En efecte, si prenem ζ una arrel p-èsima primitiva de la unitat i fem $x := \zeta - 1$, aleshores $|\zeta - 1| < 1$, de manera que $\log_p(\zeta)$ és convergent; ara bé, $\log_p(\zeta) = 0$, ja que ζ és una arrel de la unitat, de manera que $\exp(\log_p(\zeta)) = \exp(0) = 1$, però $1 \neq \zeta$.

Com a corol·lari del lema, podem obtenir de manera senzilla els zeros de la funció logaritme.

Corol·lari 9.12.11. *Sigui $x \in \mathbb{C}_p{}^*$ qualsevol. Condició necessària i suficient perquè sigui $\log_p(x) = 0$ és que x sigui el producte d'una arrel de la unitat per una potència racional de p.*

Demostració: La suficiència ja està vista en l'extensió de la funció logaritme a tot $\mathbb{C}_p{}^*$. Per a la necessitat, i tenint en compte l'estructura de $\mathbb{C}_p{}^*$, podem suposar que $x = 1 + y$ amb $|y| < 1$. Aleshores, existeix un nombre natural n_0 tal que per a tot nombre natural $n \geq n_0$ és $|y|^{p^n} < p^{\frac{-1}{p-1}}$. Podem escriure la igualtat

$$x^{p^n} - 1 = (1+y)^{p^n} - 1 = \sum_{i=1}^{p^n - 1} \binom{p^n}{i} y^i + y^{p^n};$$

com que tots els coeficients binòmics del sumatori són divisibles per p, i com que $|y| < 1$, tots aquests sumands tenen valor absolut menor o igual que $|py|$; però $|py| < |p| = p^{-1} \leq p^{\frac{-1}{p-1}}$, de manera que, per l'elecció de n, $|x^{p^n} - 1| < p^{\frac{-1}{p-1}}$. Apliquem el lema de més amunt: $|\log_p(x^{p^n})| = |x^{p^n} - 1|$, que és nul per la hipòtesi que $\log_p(x) = 0$; per tant, $x^{p^n} = 1$; és a dir, x és una arrel de la unitat. $\square$

Capítol 10

Formes quadràtiques p-àdiques

Un dels temes habituals d'estudi dels cursos bàsics de geometries lineal o projectiva és el tractament de les còniques i les quàdriques; és a dir, de les formes quadràtiques, sobre els cossos $\mathbb{R}$ o $\mathbb{C}$, de les quals se n'acostuma a fer una classificació. A la pràctica, però, sovint es tenen equacions sobre el cos dels nombres racionals. I una pregunta natural a fer-se en aquest context és: per què no es fa la classificació sobre el cos dels nombres racionals?

Aquest capítol posa les bases per a què, en el següent, poguem fer aquesta classificació. De fet, un dels ingredients principals de la classificació sobre $\mathbb{Q}$ és el teorema de Hasse-Minkowski (cf. **11.3.1**), que permet fer ús de la classificació sobre $\mathbb{R}$ i sobre tots els cossos p-àdics, $\mathbb{Q}_p$, per a obtenir la classificació sobre $\mathbb{Q}$.

Així, doncs, dediquem aquest capítol a la classificació de les formes quadràtiques sobre els cossos p-àdics.

10.1 Espais quadràtics

L'objectiu d'aquesta secció és recordar el concepte i les propietats més elementals de les formes quadràtiques sobre un cos de característica diferent de 2. Siguin, doncs, K un cos de característica diferent de 2, i V un espai vectorial de dimensió finita, n, sobre K.

Definició 10.1.1. Una forma quadràtica en V és una aplicació $q : V \longrightarrow K$ tal que

(a) per a tot element $\lambda \in K$ i tot vector $v \in V$ és $q(\lambda v) = \lambda^2 q(v)$; i

(b) l'aplicació $B : V \times V \longrightarrow K$ definida per $B(v_1, v_2) := q(v_1 + v_2) - q(v_1) - q(v_2)$ és una forma bilineal.

La parella (V, q) s'anomena un espai quadràtic de dimensió n sobre K.

Com que $\text{car}(K) \neq 2$, té sentit considerar l'aplicació bilineal simètrica definida per la fórmula $\beta(v_1, v_2) = v_1 \cdot v_2 := \frac{1}{2} B(v_1, v_2)$. Se satisfà la igualtat $v \cdot v = q(v)$, de manera que hi ha una bijecció entre el conjunt de les formes quadràtiques sobre V i el conjunt de les formes bilineals simètriques sobre V; l'aplicació inversa assigna a cada forma bilineal simètrica β la forma quadràtica $q(v) := \beta(v, v)$. De fet, tant un conjunt com l'altre són espais vectorials de manera natural i aquesta aplicació és un isomorfisme entre aquests espais vectorials.

Definició 10.1.2. Si $(V_1, q_1), (V_2, q_2)$ són dos espais quadràtics de dimensió finita sobre K, un morfisme d'espais quadràtics, o morfisme mètric, de (V_1, q_1) en (V_2, q_2) és una aplicació K-lineal $\varphi : V_1 \longrightarrow V_2$ tal que per a tot vector $v_1 \in V_1$ és $q_2(\varphi(v_1)) = q_1(v_1)$.

En aquest cas, se satisfà la igualtat $\varphi(v_1) \cdot \varphi(v_1') = v_1 \cdot v_1'$, per a tota parella (v_1, v_1') d'elements de V_1.

Definició 10.1.3. Siguin q_1, q_2 formes quadràtiques. Direm que q_1 i q_2 són equivalents, i escriurem $q_1 \sim q_2$, quan els espais quadràtics (V_1, q_1) i (V_2, q_2) són isomorfs; és a dir, quan existeix un isomorfisme $\varphi : V1 \longrightarrow V_2$ tal que $q_2(\varphi(v_1)) = q_1(v_1)$ per a tot element $v_1 \in V_1$.

En particular, la dimensió de l'espai quadràtic (V, q) és un invariant de la classe d'equivalència de la forma quadràtica q.

Definició 10.1.4. Sigui $\{e_1, \ldots, e_n\}$ una K-base arbitrària de V. S'anomena matriu de q en la base $\{e_1, \ldots, e_n\}$ la matriu de la forma bilineal β associada a la forma quadràtica q en aquesta base; és a dir, és la matriu quadrada de n files que té coeficients els elements de K, $a_{i,j} := e_i \cdot e_j$. S'anomena també la matriu de la mètrica.

Donat un vector $x := x_1e_1 + \cdots + x_ne_n$, amb $x_1, \ldots, x_n \in K$, podem escriure

$$q(x) = \sum_{i=1}^{n} a_{i,i}x_i^2 + 2\sum_{i<j} a_{i,j}x_ix_j;$$

o, en forma matricial, $q(x) = (x)^t(a_{i,j})(x)$, on (x) és la matriu columna formada per les coordenades de x en la base $\{e_i\}$ i $(x)^t = (x_1, \ldots, x_n)$ la matriu transposada de la matriu (x). Així, si $\{e_1', \cdots, e_n'\}$ és una altra base i $P \in \mathbf{GL}(n, K)$ és la matriu del canvi de base (és a dir, la matriu dels vectors e_i' expressats en la base $\{e_i\}$), aleshores la matriu de q en aquesta base és la matriu $(a_{i,j}') = P^t(a_{i,j})P$. En particular, el determinant de la matriu $(a_{i,j})$, pensat com a element de K, no és pas un invariant de la forma quadràtica ni de la seva classe d'equivalència; però sí que ho és si el pensem mòdul el quadrat d'un element no nul de K; en efecte, se satisfà la igualtat $\det(a_{i,j}') = \det(a_{i,j}) \det P^2$.

Definició 10.1.5. S'anomena discriminant de q el determinant de la matriu $(a_{i,j})$ pensat com a element de $\{0\} \cup K^*/K^{*2}$. El denotarem per $\mathrm{disc}(q)$. És un invariant de la classe d'equivalència de la forma quadràtica.

La dimensió i el discriminant no són, però, suficients per a descriure les classes d'equivalència de formes quadràtiques. En efecte, les dues formes quadràtiques de K^3, X^2 i $X^2 + Y^2$ tenen discriminant nul, però no són pas equivalents; per exemple, perquè un canvi de base no modifica el rang de la matriu de la mètrica i totes dues matrius tenen rang diferent. Per tant, cal afegir encara més invariants per a determinar completament el conjunt de classes d'equivalència de formes quadràtiques sobre un cos K. Veurem més endavant que aquests tres invariants, dimensió, discriminant i rang, són suficients per a classificar les formes quadràtiques sobre un cos algebraicament tancat. Ara ens interessa aprofundir una mica en l'estudi del rang.

Definició 10.1.6. Sigui (V, q) un espai quadràtic. Dos vectors $v, w \in V$ s'anomenen ortogonals, i s'escriu $v \perp w$, quan $v \cdot w = 0$; un vector s'anomena isòtrop quan és ortogonal

a si mateix; un vector s'anomena totalment isòtrop quan és ortogonal a tot altre vector de V. Un subespai vectorial $W \subseteq V$ s'anomena isòtrop quan tots els seus elements són isòtrops. S'anomena radical de (V, q), o bé nucli de (V, q), el subconjunt de V format pels vectors totalment isòtrops.

En general, donat un subconjunt arbitrari $S \subseteq V$, el conjunt

$$S^{\perp} := \{v \in V : v \perp w, \text{ per a tot } w \in S\}$$

és un subespai vectorial de V que s'anomena l'ortogonal de S; en conseqüència, el radical és l'ortogonal de tot l'espai vectorial V. Donat un subespai vectorial arbitrari $W \subseteq V$, podem considerar el seu dual W^* i l'aplicació lineal $f_W : V \longrightarrow W^*$ que associa a cada element $v \in V$ la forma lineal de W definida per $w \mapsto v \cdot w$; el nucli d'aquesta forma lineal és l'ortogonal de W. El cas particular $W = V$ dóna el radical de (V, q). Si tenim en compte l'expressió matricial de la forma bilineal associada a q, ens adonem de seguida que la matriu de f_V en una base de V i la seva dual en V^* és exactament la mateixa que la matriu de la mètrica; per tant, el rang de la matriu de la mètrica és la codimensió del radical. En particular, condició necessària i suficient perquè el radical de V sigui nul és que $\operatorname{disc}(q) \neq 0$.

Definició 10.1.7. Una forma quadràtica q, i també l'espai quadràtic (V, q), s'anomena no degenerada o no singular quan $\operatorname{disc}(q) \neq 0$.

Observació 10.1.8. En general no és cert que la restricció a un subespai vectorial d'una forma quadràtica no degenerada sigui una forma quadràtica no degenerada. Per exemple, la forma quadràtica de K^2 de matriu

$$S := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

és clarament no degenerada, però la seva restricció al subespai generat pel vector $(1, 1)$ és la forma nul·la.

Observació 10.1.9. D'altra banda, una forma quadràtica no degenerada pot tenir una base formada per vectors isòtrops; per exemple, la forma de K^2 donada per la matriu S de més amunt admet la matriu

$$H := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

en la base $\{(1, 1), \frac{1}{2}(1, -1)\}$.

Definició 10.1.10. Un espai quadràtic s'anomena un pla hiperbòlic quan admet una base formada per dos elements isòtrops e_1, e_2 tals que $e_1 \cdot e_2 \neq 0$.

Observació 10.1.11. En particular, en la base $e_1, \dfrac{1}{(e_1 \cdot e_2)} e_2$, la matriu de la forma quadràtica és la matriu H de més amunt; per tant, un pla hiperbòlic és de dimensió 2, és no degenerat, i té discriminant -1.

Proposició 10.1.12. *Sigui (V, q) un espai quadràtic no degenerat i suposem que V conté un element isòtrop no nul, v. Aleshores, V conté un pla hiperbòlic que conté v.*

DEMOSTRACIÓ: Com que V és no degenerat, existeix un element $x \in V$ tal que $v \cdot x \neq 0$ (en cas contrari, v seria del radical de V). Posem $w := x - \dfrac{(x \cdot x)}{2(v \cdot x)} v$; aleshores, w és isòtrop i $v \cdot w = v \cdot x \neq 0$; per tant, $W := \langle v, w \rangle$ és un pla hiperbòlic que conté v. □

Notació 10.1.13. Una forma quadràtica en un espai de dimensió 1 sempre és de la forma $q(v) = ax^2$, per a un cert element $a \in K$. En efecte, elegida una base de V, si x designa la coordenada de v en aquesta base, podem escriure $q(v) = ax^2$ per a un cert element $a \in K$; i un canvi de base modifica a multiplicant-lo pel quadrat d'un element no nul de K; aquest element a, doncs, està definit mòdul quadrats de K^*; escriurem $q = \langle a \rangle$.

10.2 Diagonalització

En aquesta secció es tracta d'estudiar la reducció de les formes quadràtiques amb els ulls posats en la seva classificació; especialment, en el càlcul del rang. Considerem, doncs, un espai quadràtic (V, q) de dimensió finita, n, sobre un cos K de característica diferent de 2.

Definició 10.2.1. Es diu que una base $\{e_1, e_2, \ldots, e_n\}$ de (V, q) és ortogonal quan se satisfan les igualtats $e_i \cdot e_j = 0$, si $i \neq j$.

Si $\{e_1, e_2, \ldots, e_n\}$ és una base ortogonal de (V, q), aleshores la matriu de la mètrica en aquesta base és una matriu diagonal. Recíprocament, si la matriu de la mètrica en una base és diagonal, aleshores la base és ortogonal. En particular, el nombre de zeros que apareixen a la diagonal és la dimensió del radical, ja que els vectors de la base que corresponen a aquests zeros són vectors totalment isòtrops i en nombre igual a la dimensió del radical, que és la codimensió d'aquesta matriu. Es tracta de veure que sempre existeixen bases ortogonals. Per a això comencem per la definició següent.

Definició 10.2.2. S'anomena suma ortogonal dels dos espais quadràtics (V_1, q_1) i (V_2, q_2) l'espai quadràtic $(V_1 \oplus V_2, q)$ on q és la forma quadràtica definida, per a $v_1 \in V_1$, $v_2 \in V_2$, arbitraris, per la igualtat $q(v_1 + v_2) := q(v_1) + q(v_2)$. Escriurem $V_1 \perp V_2$ per a indicar la suma ortogonal i, anàlogament, $q_1 \perp q_2$.

Si (V, q) és un espai quadràtic i W és un subespai qualsevol, aleshores W és ortogonal al radical de (V, q); per tant, qualsevol suplementari de $\mathrm{rad}(V)$ com a subespai vectorial és ortogonal a $\mathrm{rad}(V)$. En conseqüència, (V, q) descompon en suma ortogonal de $\mathrm{rad}(V)$ i un suplementari qualsevol. A més a més, és clar a partir de la definició que el rang de la suma ortogonal és la suma de rangs, de manera que el rang del suplementari sempre és màxim; és a dir, la restricció de la forma quadràtica q a un suplementari qualsevol de $\mathrm{rad}(V)$ és una forma quadràtica no degenerada. No només això, sinó que dos suplementaris qualssevol de $\mathrm{rad}(V)$ són isomètrics. En efecte, si $V = V_1 \perp \mathrm{rad}(V) = V_2 \perp \mathrm{rad}(V)$, donat $v_1 \in V_1$ podem escriure v_1 de manera única en la forma $v_1 = v_2 + v'$ amb $v_2 \in V_2$ i $v' \in \mathrm{rad}(V)$; aleshores, $q(v_1) = q(v_2)$ i l'assignació $v_1 \mapsto v_2$ defineix una isometria de V_1 en V_2.

Definició 10.2.3. Sigui $a \in K$. Direm que la forma quadràtica q representa a, i escriurem $q \to a$, quan existeix un vector no nul $v \in V$ tal que $q(v) = a$.

Corol·lari 10.2.4. *Siguin q una forma quadràtica i $a \in K^*$ un element no nul de K. Condició necessària i suficient perquè q representi a és que q representi ab^2, per a tot element $b \in K^*$.* □

El pas clau de la diagonalització de formes quadràtiques el proporciona el resultat següent.

Proposició 10.2.5. *Siguin (V, q) un espai quadràtic i $a \in K^*$ un element no nul de K. Condició necessària i suficient perquè q representi a és que q descompongui com a suma ortogonal de la forma quadràtica $\langle a \rangle$ i una certa forma quadràtica q'.*

Demostració: Clarament, la forma quadràtica $\langle a \rangle \perp q'$ representa a; vegem el recíproc. Sigui V_1 un suplementari de $\mathrm{rad}(V)$; aleshores la restricció a V_1 de q, posem q_1, és no degenerada; com que $a \neq 0$, la condició $q \to a$ és equivalent a $q_1 \to a$; per tant, podem suposar que q és no degenerada.

Suposem, doncs, que $q \to a$ i que q és no degenerada. Sigui $v \in V$ tal que $q(v) = a$. Aleshores, la restricció de q a Kv és la forma quadràtica $\langle a \rangle$ i $Kv \cap Kv^\perp = (0)$, ja que v no és un vector isòtrop. A més a més, com que q és no singular, la dimensió de $Kv^\perp$ és la codimensió de Kv, de manera que $Kv + Kv^\perp = V$; i com que Kv és ortogonal a $Kv^\perp$, és $Kv \perp Kv^\perp = V$, de manera que la restricció q' de q a $Kv^\perp$ és la forma que necessitàvem. □

Corol·lari 10.2.6. *Tota espai quadràtic admet una base ortogonal; és a dir, tota forma quadràtica (sobre un cos de característica diferent de 2) és diagonalitzable.*

Demostració: Per inducció sobre el rang de la forma; si $\mathrm{rang}(q) = 1$, el resultat és trivial. Si el suposem cert fins a dimensió $n-1$, podem prendre un element no nul $a \in K$ tal que $q \to a$, de manera que $q = \langle a \rangle \perp q'$, per a una certa forma de rang $\mathrm{rang}(q) - 1$. Per hipòtesi d'inducció, la forma q' és diagonalitzable, i clarament $\langle a \rangle$ ho és. Per tant, la seva suma ortogonal és diagonalitzable, ja que el vector v que representa a és ortogonal al subespai suplementari de $\langle v \rangle$. □

És a dir, si escrivim $\langle a_1, \ldots, a_n \rangle$ per a designar la forma quadràtica suma ortogonal de les formes quadràtiques de rang 1, $\langle a_i \rangle$, tota forma quadràtica q és equivalent a una forma quadràtica del tipus $\langle a_1, \ldots, a_n \rangle$, on els elements $a_i \in K$ poden ser repetits o nuls.

Observació 10.2.7. Hom podria haver demostrat aquest resultat d'una manera molt més senzilla. En efecte, podríem haver ensenyat el mètode de Gauss de completar quadrats per a la reducció d'una forma quadràtica a una suma de quadrats. Hem fet aquesta demostració a fi de posar de manifest fets que ens seran d'utilitat més endavant.

10.3 Teorema de Witt

Acabem de provar que tota forma quadràtica sobre un cos de característica diferent de 2 és equivalent a una forma quadràtica diagonal; és a dir, a una forma quadràtica del tipus $\langle a_1, \ldots, a_n \rangle$. En conseqüència, per a fer la classificació de les formes quadràtiques podem limitar-nos a classificar les formes quadràtiques diagonals. El teorema de simplificació de Witt proporcionarà el pas inductiu per a aquesta classificació.

D'altra banda, ja hem vist que la dimensió i el rang són invariants associats a cada classe d'equivalència de formes quadràtiques; per tant, podem suposar fixats aquests invariants; igualment, si convé, podem suposar fixat el discriminant com a element de $\{0\} \cup K^*/K^{*2}$, ja que el discriminant també és un invariant de la classe d'equivalència.

El fet que dos suplementaris qualssevol del radical siguin isomètrics fa que puguem reduir-nos a classificar espais quadràtics no singulars. En efecte, si (V,q) i (V',q') són espais quadràtics isomètrics, els seus radicals són isomorfs i, en conseqüència, suplementaris de $\mathrm{rad}(V)$ i $\mathrm{rad}(V')$ són isomètrics. El recíproc és clar; si suplementaris dels radicals són isomètrics i els radicals són isomorfs (i.e., tenen la mateixa dimensió), aleshores (V,q) i (V',q') són isomètrics, ja que són suma ortogonal d'espais isomètrics.

Per tant, a partir d'ara suposarem que els espais quadràtics són no singulars. El primer que cal fer és estudiar de quina manera es poden estendre morfismes mètrics de subespais.

Proposició 10.3.1. *Siguin (V,q), (V',q'), espais quadràtics no singulars de dimensió finita, $U \subseteq V$ un subespai vectorial qualsevol, i $\sigma : U \longrightarrow V'$ un morfisme mètric injectiu. Suposem que U és degenerat. Aleshores, existeix un subespai vectorial $\overline{U} \subseteq V$ tal que U és un hiperplà de $\overline{U}$, i existeix un morfisme mètric injectiu $\overline{\sigma} : \overline{U} \longrightarrow V'$ que estén σ.*

Dit d'una altra manera, tot morfisme mètric injectiu d'un subespai singular U de V es pot prolongar a un morfisme mètric injectiu d'un subespai de V que conté U com a hiperplà.

Demostració: Com que U és singular, $\mathrm{rad}(U) \neq (0)$ i podem elegir un element no nul $u_0 \in \mathrm{rad}(U)$ i una forma lineal $\omega : U \longrightarrow K$ tal que $\omega(u_0) = 1$. Ara, com que V és no singular, l'aplicació $V \longrightarrow V^*$ donada per $v \mapsto (u \mapsto v \cdot u)$ és un isomorfisme canònic i, per tant, component amb l'aplicació dual de la inclusió $U \subseteq V$, l'aplicació $V \longrightarrow U^*$ donada per $v \mapsto (u \mapsto v \cdot u)$ és exhaustiva. En conseqüència, existeix un element $v \in V$ tal que $\omega(u) = v \cdot u$ per a tot element $u \in U$. A més a més, canviant si convé v per $v - \dfrac{1}{2}(v \cdot v)u_0$, podem suposar que $v \cdot v = 0$. En particular, com que $\omega(u_0) = 1 \neq 0$ i $u_0 \in \mathrm{rad}(U)$, el vector v no és pas de U, i podem elegir $\overline{U} := U \oplus Kv$; així, obtenim un subespai vectorial de V que conté U com a hiperplà.

Posem, ara, $U' := \sigma(U)$, $u_0' := \sigma(u_0)$, i $\omega' := \omega \circ \sigma^{-1}$. Com que σ és un morfisme mètric injectiu, U' és un subespai singular de V', u_0' és un element de $\mathrm{rad}(U')$, i ω' és una forma lineal de U' tal que $\omega'(u_0') = 1$; repetint la construcció de més amunt, obtenim un subespai vectorial $\overline{U}' \subseteq V'$ que conté $\sigma(U)$ com a hiperplà en la forma $\overline{U}' = U' \oplus Kv'$. Sigui $\overline{\sigma} : \overline{U} \longrightarrow \overline{U}' \subseteq V'$ l'extensió de σ a $\overline{U}$ definida per $\overline{\sigma}(v) := v'$. Aleshores, $\overline{\sigma}$ és un morfisme mètric injectiu de $\overline{U}$ en V' que estén σ, com volíem demostrar. En efecte, només cal comprovar que es respecta la mètrica i sobre U no hi ha res a dir; sobre Kv tampoc, ja que v és un vector isòtrop, igual que v'; i per últim, el producte $u \cdot v$ d'un element $u \in U$ per v és donat per la forma lineal ω, mentre que el producte de $\sigma(u)$ per v' és donat per la forma lineal $\omega' = \omega \circ \sigma^{-1}$. □

Teorema 10.3.2 (Witt)**.** *Siguin (V,q), (V',q'), espais quadràtics no singulars de dimensió finita, $U \subseteq V$ un subespai qualsevol, i $\sigma : U \longrightarrow V'$ un morfisme mètric injectiu. Suposem que (V,q) i (V',q') són isomètrics. Aleshores, existeix una isometria $\overline{\sigma} : V \longrightarrow V'$ que estén σ.*

Demostració: Encara que no podem suposar que $q = q'$, com que (V,q) i (V',q') són isomètrics, podem suposar que $V = V'$. I si apliquem successivament la proposició anterior, i com que V és de dimensió finita, podem suposar que U no és singular. Ara podem fer la prova per inducció sobre la dimensió de U. Si U és de dimensió 1, aleshores qualsevol element no nul $u \in U$ és no isòtrop i un dels dos elements de V, $u \pm \sigma(u)$ és

no isòtrop; en efecte, en cas contrari es tindrien igualtats $2u \cdot u \pm 2u \cdot \sigma(u) = u \cdot u \pm 2u \cdot \sigma(u) + \sigma(u) \cdot \sigma(u) = 0$, ja que σ és una isometria amb la imatge, i en sumar-les i tenir en compte que $\mathrm{car}(K) \neq 2$, obtindríem que u és isòtrop. Posem $\overline{u} := u + \varepsilon\sigma(u)$, $\varepsilon = \pm 1$, un dels $u \pm \sigma(u)$ que no sigui isòtrop i sigui $\overline{U}^{\perp}$ l'ortogonal de $\overline{u}$. Aleshores, $\overline{U}^{\perp}$ és un hiperplà, ja que $\overline{u}$ és no isòtrop, i $V = K\overline{u} \perp \overline{U}^{\perp}$. Siguin σ' l'automorfisme de V que és la identitat sobre $\overline{U}^{\perp}$ i que canvia $\overline{u}$ de signe, i $\overline{\sigma} := -\varepsilon\sigma'$. Aleshores, $\overline{\sigma}$ és una isometria de V i, com que $u - \varepsilon\sigma(u) \in \overline{U}^{\perp}$, se satisfan les igualtats $\sigma'(u - \varepsilon\sigma(u)) = u - \varepsilon\sigma(u)$ i $\sigma'(u + \varepsilon\sigma(u)) = -(u + \varepsilon\sigma(u))$, de manera que, en suman i dividir per 2, $\sigma'(u) = -\varepsilon\sigma(u)$; és a dir, $\overline{\sigma}(u) = \sigma(u)$, i $\overline{\sigma}$ prolonga σ, com volíem demostrar.

Suposem, ara, que U és de dimensió més gran que 1. Podem elegir una descomposició de U com a suma ortogonal de dos subespais no trivials, U_1 i U_2 de U. En particular, U_2 està inclòs en l'ortogonal de U_1. Per hipòtesi d'inducció, la restricció σ_1 de σ a U_1 es prolonga a una isometria σ_1 de V; i si canviem σ per $\sigma_1^{-1} \circ \sigma$, podem suposar que la restricció σ_1 de σ a U_1 és la identitat en U_1. Aleshores, σ aplica U_2 en $U_1^{\perp}$. De nou per hipòtesi d'inducció, la restricció de σ a U_2 es prolonga en un automorfisme σ_2 de $U_1^{\perp}$. Aleshores, podem posar $\overline{\sigma}$ l'automorfisme de V que és la identitat en U_1 i σ_2 en $U_1^{\perp}$: i aleshores, $\overline{\sigma}$ és una isometria que prolonga σ, ja que V és la suma ortogonal de U_1 i $U_1^{\perp}$, per ser U_1 no singular. □

Corol·lari 10.3.3. *Sigui (V, q) un espai quadràtic no singular. Els ortogonals de dos subespais isomètrics de V són isomètrics.*

Demostració: En primer lloc, construïm una prolongació a V d'una isometria entre els dos espais; i després la restringim als ortogonals. □

10.4 Classificació de formes quadràtiques sobre cossos finits

El teorema de Witt ens permet donar una primera descripció de les formes quadràtiques sobre un cos arbitrari de característica diferent de 2. Recordem que hem demostrat més amunt que podem limitar-nos a classificar formes quadràtiques no singulars.

Proposició 10.4.1. *Sigui (V, q) un espai quadràtic no singular de dimensió finita. Existeixen plans hiperbòlics $H_1, \ldots, H_m$ i un subespai quadràtic W de V sense vectors isòtrops no nuls tals que $V = H_1 \perp \cdots \perp H_m \perp W$.*

Demostració: Si V no conté vectors isòtrops no nuls, prenem $W = V$ i $m = 0$ i ja hem acabat. En cas contrari, sigui $v \in V$ un vector isòtrop no nul; podem considerar (cf. la proposició **10.1.12**) un pla hiperbòlic $H_1 = H := \langle v, w \rangle \subseteq V$ i V descompon en suma directa ortogonal de H i $H^{\perp}$, ja que V i H són no singulars. Podem acabar la prova per inducció sobre la dimensió de V; per hipòtesi d'inducció, $H^{\perp}$ és la suma ortogonal de plans hiperbòlics $H_2, \ldots, H_m$ amb un subespai quadràtic W sense vectors isòtrops no nuls; per tant, $V = H_1 \perp \cdots \perp H_m \perp W$ és la descomposició que cercàvem. □

Teorema 10.4.2. *El nombre m de plans hiperbòlics de la proposició anterior no depèn de la descomposició i coincideix amb el màxim de les dimensions dels subespais isòtrops de V.*

DEMOSTRACIÓ: La unicitat de la descomposició és conseqüència del teorema de Witt. En efecte, si tenim dues descomposicions $V = H_1 \perp \cdots \perp H_m \perp W = H'_1 \perp \cdots \perp H'_{m'} \perp W'$ amb H_i, H'_j plans hiperbòlics i W, W' subespais sense vectors isòtrops no nuls, aleshores $m = m'$ i $W \cong W'$. En efecte, com que $H_1 \cong H'_1$, podem estendre aquesta isometria a tot V, de manera que els suplementaris ortogonals són isomorfs; per inducció sobre m, de $H_2 \perp \cdots \perp H_m \perp W \cong H'_2 \perp \cdots \perp H'_{m'} \perp W'$ obtenim $m = m'$ i $W \cong W'$. Per tant, només resta demostrar que m és el màxim de les dimensions dels subespais isòtrops.

Clarament, si prenem una base v_i, w_i de cada H_i de manera que v_i, w_i siguin isòtrops i $v_i \cdot w_i = 1$, els vectors $v_1, \ldots, v_m$ generen un subespai isòtrop de dimensió m, ja que $v_i \perp v_j$ per a tota parella d'índexs i, j. Així, m no supera el màxim de les dimensions dels subespais isòtrops. D'altra banda, suposem que M és un subespai isòtrop i sigui $\{v_1, \ldots, v_k\}$ una base de M; podem elegir un vector no isòtrop $w_1 \in V$ tal que $v_1 \cdot w_1 = 1$, de manera que $H_1 := \langle v_1, w_1 \rangle$ és un pla hiperbòlic. En general no és cert que el vector w_1 sigui ortogonal a tots els $v_2, \ldots, v_k$, però si canviem cada vector v_i pel vector $v_i - (v_i \cdot w_1)v_1$ obtenim una nova base de M de manera que $\langle v_2, \ldots, v_k \rangle$ és ortogonal a H_1. Ara podem considerar la descomposició $V = H_1 \perp H_1^\perp$ i tenir en compte que $\langle v_2, \ldots, v_k \rangle \subseteq H_1^\perp$; per inducció, obtenim en $H_1^\perp$ una descomposició amb un mínim de $k-1$ plans hiperbòlics, de manera que V admet una descomposició en suma ortogonal amb un mínim de k plans hiperbòlics. Per tant, $k \leq m$, i això acaba la prova. □

Observació 10.4.3. Això no és una classificació completa de les formes quadràtiques no degenerades. Però redueix aquesta classificació a la classificació dels espais quadràtics no singulars que no tenen vectors isòtrops no nuls. Per als cossos algebraicament tancats i per als cossos finits, però, podem obtenir fàcilment una classificació completa de les formes quadràtiques sense fer servir el teorema de Witt.

Proposició 10.4.4. *Suposem que K és un cos algebraicament tancat de característica diferent de 2. Aleshores totes les formes quadràtiques no degenerades del mateix rang són equivalents; en particular, equivalents a la forma $\langle 1, \ldots, 1 \rangle$.*

DEMOSTRACIÓ: Sabem que tota forma quadràtica és diagonalitzable; per tant, equivalent a una suma ortogonal de formes quadràtiques de la forma $\langle a_i \rangle$, amb $a_i \in K$; i si la forma és no singular, tots els elements a_i han de ser no nuls. Ara, si K és algebraicament tancat, a_i sempre és un quadrat, de manera que podem dividir el i-èsim element de la base per una arrel quadrada de a_i; això demostra l'equivalència de la forma $\langle a_i \rangle$ amb la forma $\langle 1 \rangle$ i acaba la prova. □

Observació 10.4.5. En aquest cas, el discriminant no aporta res a la classificació, ja que per ser tot element un quadrat, totes les formes quadràtiques no singulars tenen discriminant 1. Dit d'una altra manera, el rang és un sistema complet d'invariants de les classes d'isomorfia de formes quadràtiques no degenerades sobre un cos algebraicament tancat de característica $\neq 2$.

Exercici 10.4.6. Si K és algebraicament tancat, aleshores tot pla hiperbòlic admet una base de manera que la seva matriu en aquesta base és la matriu identitat en dimensió 2.

Per a acabar aquesta secció farem la classificació en el cas en què el cos K és un cos finit de característica diferent de 2. Per a això cal estudiar, en primer lloc, les sumes de quadrats en $K := \mathbb{F}_q$, on q és una potència d'un nombre primer senar p.

Lema 10.4.7. *Siguin $a, b, c \in \mathbb{F}_q^*$ elements no nuls qualssevol. Aleshores, existeixen elements $x, y \in \mathbb{F}_q$ tals que $ax^2 + by^2 = c$. Dit d'una altra manera, tota forma quadràtica de rang 2 sobre un cos finit de característica diferent de 2 representa tot element no nul del cos.*

Demostració: Podem fer una demostració molt elemental d'aquest fet. Per exemple, el conjunt dels quadrats de $\mathbb{F}_q$ és de cardinal $\frac{q+1}{2}$, ja que el morfisme de grups de $\mathbb{F}_q^*$ d'elevar al quadrat té nucli $\{\pm 1\}$ i a més el zero és un quadrat. Per tant, com que a és no nul, el conjunt $A := \{ax^2 : x \in \mathbb{F}_q\}$ també té cardinal $\frac{q+1}{2}$; i, per homotècia i translació, el conjunt $B := \{c - by^2 : y \in \mathbb{F}_q\}$ també té cardinal $\frac{q+1}{2}$. En conseqüència, la intersecció de A amb B no pot ser el conjunt buit. Un punt de la intersecció satisfà la igualtat $ax^2 + by^2 = c$, i la prova és completa, perquè x, y no poden ser nuls simultàniament. □

Exercici 10.4.8. Siguin p un nombre natural primer, $p \equiv 3 \pmod 4$, i $\mathbb{F}_q|\mathbb{F}_p$ una extensió de grau senar (o sigui, $q = p^f$, amb f senar). Llavors, la forma quadràtica $X^2 + Y^2$ no representa zero en $\mathbb{F}_q$.

Corol·lari 10.4.9. *Tota forma quadràtica de rang ≥ 3 sobre $\mathbb{F}_q$ representa tot element de $\mathbb{F}_q$; en particular, representa zero.*

Demostració: Podem suposar que la forma és de rang 3 i escriure-la en una base ortogonal en la forma $aX^2 + bY^2 - cZ^2$ amb $a, b, c \in \mathbb{F}_q^*$. Si $ax^2 + by^2 = c$ és una representació de c per la forma $aX^2 + bY^2$, aleshores, $ax^2 + by^2 - c1^2$ és una representació de zero per la forma $aX^2 + bY^2 - cZ^2$. □

Teorema 10.4.10. *Sigui g un generador del grup multiplicatiu $\mathbb{F}_q^*$. Per a tot enter $n \geq 1$ només hi ha dues classes d'equivalència de formes quadràtiques de rang n: admeten per representants les formes $\langle 1, \ldots, 1\rangle$ i $\langle 1, \ldots, 1, g\rangle$.*

Demostració: Observem, en primer lloc, que g no és un quadrat de $\mathbb{F}_q^*$, ja que és un generador d'aquest grup d'ordre parell. En particular, el discriminant de qualsevol forma quadràtica no singular, mòdul quadrats, és o bé 1 o bé g. La demostració del teorema es fa per inducció sobre el rang. El cas de rang 1 és immediat. D'altra banda, si el rang és més gran que 1, la forma quadràtica representa 1; per tant, admet una descomposició en suma ortogonal de la forma $\langle 1\rangle$ amb una forma quadràtica de rang una unitat inferior i podem aplicar la hipòtesi d'inducció. □

Observació 10.4.11. Així, doncs, una condició necessària i suficient perquè dues formes quadràtiques no degenerades sobre $\mathbb{F}_q$ siguin equivalents és que tinguin el mateix rang i el mateix discriminant.

10.5 Àlgebres de quaternions

Sigui K un cos de característica diferent de 2. L'estudi de les formes quadràtiques sobre K conté, en particular, l'estudi de les formes $aX^2 + bY^2 - Z^2$ i $X^2 - aY^2 - bZ^2 + abT^2$. I aquestes tenen una interpretació interessant en el context d'àlgebres de quaternions.

Definició 10.5.1. Siguin K un cos de característica diferent de 2, i a, b elements no nuls de K. Representem per $\left(\frac{a,b}{K}\right)$ l'espai vectorial de dimensió 4 sobre K amb base $\{e_0, e_1, e_2, e_3\}$, dotat del producte determinat per les regles següents:

(a) el producte és bilineal i té element neutre $e_0 = 1$;

(b) el producte és associatiu i $e_1^2 = a, \quad e_2^2 = b, \quad e_1e_2 = -e_2e_1 = e_3$.

Amb aquesta definició, $\left(\frac{a,b}{K}\right)$ és una K-àlgebra associativa i amb unitat. Es diu que $\left(\frac{a,b}{K}\right)$ és l'àlgebra de quaternions de paràmetres a, b sobre K.

Exercici 10.5.2. La condició (b) de la definició es pot canviar per la condició (b') següent:
$e_1^2 = a, \quad e_2^2 = b, \quad e_3^2 = -ab,$
$e_1e_2 = -e_2e_1 = e_3, \qquad e_2e_3 = -e_3e_2 = -be_1, \qquad e_3e_1 = -e_1e_3 = -ae_2.$

Definició 10.5.3. Donat un quaternió $q = x_0 + x_1e_1 + x_2e_2 + x_3e_3$, x_0, x_1, x_2, $x_3 \in K$, el quaternió $\overline{q} := x_0 - x_1e_1 - x_2e_2 - x_3e_3$ s'anomena el conjugat de q. La norma de q és l'element $\mathrm{N}(q) := q\overline{q} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \in K$. Es poden verificar sense dificultat les propietats següents:

(a) $\overline{q_1 + q_2} = \overline{q}_1 + \overline{q}_2$, (b) $\overline{q_1q_2} = \overline{q}_2\,\overline{q}_1$, i (c) $\mathrm{N}(q_1q_2) = \mathrm{N}(q_1)\mathrm{N}(q_2)$.

Proposició 10.5.4. *Siguin $a, b, c \in K$ elements no nuls qualssevol. Es tenen iomorfismes $\left(\frac{a,b}{K}\right) \cong \left(\frac{b,a}{K}\right) \cong \left(\frac{a,-ab}{K}\right) \cong \left(\frac{a,(1-a)b}{K}\right) \cong \left(\frac{a,bc^2}{K}\right) \cong \left(\frac{ac^2,b}{K}\right)$, l'iomorfisme amb $\left(\frac{a,(1-a)b}{K}\right)$, sempre que $a \neq 1$.*

Demostració: Els isomorfismes de $\left(\frac{a,b}{K}\right)$ amb les altres àlgebres són immediats si tenim en compte els canvis de base següents: a partir de la base $\{e_0, e_1, e_2, e_3\}$ la base $\{e_0, e_2, e_1, -e_3\}$ determina l'isomorfisme amb l'àlgebra $\left(\frac{b,a}{K}\right)$; la base $\{e_0, e_1, e_3, ae_2\}$ amb l'àlgebra $\left(\frac{a,-ab}{K}\right)$; la base $\{e_0, e_1, e_2 + e_3, e_3 + ae_2\}$ amb l'àlgebra $\left(\frac{a,(1-a)b}{K}\right)$; la base $\{e_0, e_1, ce_2, ce_3\}$ amb l'àlgebra $\left(\frac{a,bc^2}{K}\right)$; i la base $\{e_0, ce_1, e_2, ce_3\}$ amb $\left(\frac{ac^2,b}{K}\right)$. □

Proposició 10.5.5. *Per a elements no nuls $a, b \in K$, són equivalents:*

(a) *l'àlgebra $\left(\frac{a,b}{K}\right)$ és un cos (no commutatiu);*

(b) *l'equació $x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = 0$ no té solucions no trivials en K;*

(c) *l'equació $ax^2 + by^2 = z^2$ no té solucions no trivials en K; i*

(d) *l'àlgebra $\left(\frac{a,b}{K}\right)$ no és isomorfa a l'àlgebra $\mathbf{M}(2, K)$ de les matrius quadrades 2×2 de coeficients en K.*

DEMOSTRACIÓ: Si un quaternió $q := x_0 + x_1e_1 + x_2e_2 + x_3e_3$, x_0, x_1, x_2, $x_3 \in K$, té invers q', aleshores és $\mathrm{N}(q)\mathrm{N}(q') = \mathrm{N}(e_0) = 1$, de manera que $\mathrm{N}(q) \neq 0$; recíprocament, si $\mathrm{N}(q) \neq 0$, aleshores $\dfrac{\overline{q}}{\mathrm{N}(q)}$ té sentit i és el quaternió invers de q. Per tant, condició necessària i suficient perquè tot quaternió no nul sigui invertible és que $\mathrm{N}(q) \neq 0$ sempre que $q \neq 0$. Equivalentment, que l'única solució de l'equació $\mathrm{N}(q) = 0$ sigui $q = 0$; però $\mathrm{N}(q) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$, de manera que l'equivalència de (a) amb (b) és clara.

D'altra banda, si l'equació (c) té una solució no trivial i fem $x_0 = z$, $x_1 = x$, $x_2 = y$ i $x_3 = 0$, obtenim immediatament que (b) té una solució no trivial; per tant, (b) implica (c). Recíprocament, suposem que l'equació (c) només té la solució trivial; en particular, b no és el quadrat de cap element de K i, en conseqüència, l'extensió $K(\sqrt{b})|K$ és de grau 2; a més a més, l'equació (b) es pot escriure en la forma $\mathrm{N}_{K(\sqrt{b})|K}(x_0 + x_2\sqrt{b}) = a\mathrm{N}_{K(\sqrt{b})|K}(x_1 + x_3\sqrt{b})$, de manera que condició necessària i suficient perquè a sigui norma d'un element no nul de $K(\sqrt{b})$ és que puguem prendre $x_1 + x_3\sqrt{b} \neq 0$ que, alhora, equival a poder prendre una solució no trivial de l'equació (c). Però ja vàrem veure en parlar del teorema de Legendre (cf. el teorema **8.2.1**) que condició necessària i suficient perquè l'equació (c) tingui solucions no trivials és que a sigui la norma d'un element no nul de $K(\sqrt{b})$. Això demostra l'equivalència de (b) amb (c).

Com que l'àlgebra de les matrius $\mathbf{M}(2, K)$ no és un cos, és clar que (a) implica (d). Per a veure la implicació que resta demostrarem que si l'equació (d) té una solució no trivial, aleshores l'àlgebra $\left(\dfrac{a, b}{K}\right)$ és isomorfa a $\mathbf{M}(2, K)$. Suposem que $x, y, z \in K$ no són tots tres nuls i satisfan l'equació $ax^2 + by^2 = z^2$; si tenim en compte l'isomorfisme $\left(\dfrac{a, b}{K}\right) \cong \left(\dfrac{b, a}{K}\right)$, podem suposar que $y \neq 0$. Siguin e_0, e_1, e_2, e_3, les matrius de $\mathbf{M}(2, K)$

$$e_0 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, e_1 := \begin{bmatrix} 0 & y \\ a/y & 0 \end{bmatrix}, e_2 := \begin{bmatrix} z/y & x \\ -ax/y^2 & -z/y \end{bmatrix}, e_3 := e_1e_2 = \begin{bmatrix} -ax/y & -z \\ az/y^2 & ax/y \end{bmatrix}.$$

És immediat comprovar les igualtats $e_1^2 = ae_0$, $e_2^2 = be_0$, i $e_1e_2 = -e_2e_1 = e_3$; a més a més, les matrius e_0, e_1, e_2, e_3 són K-linealment independents, fet que es comprova sense dificultat tenint en compte la relació $ax^2 + by^2 = z^2$. Per tant, l'àlgebra $\mathbf{M}(2, K)$ és (isomorfa a) l'àlgebra de quaternions de paràmetres a, b. □

Corol·lari 10.5.6. *Siguin $a, b \in K$ elements no nuls. Aleshores:*

$$\left(\frac{a, -a}{K}\right) \cong \left(\frac{a, 1-a}{K}\right) \cong \left(\frac{a, b^2}{K}\right) \cong \left(\frac{a, 1}{K}\right) \cong \mathbf{M}(2, (K).$$

DEMOSTRACIÓ: Els primers isomorfismes són casos particulars de la proposició **10.5.4** que s'obtenen en fer $b = 1$; i el darrer és conseqüència de la proposició anterior, ja que, clarament, l'equació $ax^2 + y^2 = z^2$ té solucions no trivials. □

Proposició 10.5.7. *Siguin $a, b, c \in K$ elements no nuls i suposem que $\left(\dfrac{a, b}{K}\right)$ és (isomorfa a) $\mathbf{M}(2, K)$. Aleshores, se satisfà la propietat següent de simplificació:*

$$\left(\frac{ac, b}{K}\right) \cong \left(\frac{c, b}{K}\right).$$

DEMOSTRACIÓ: Si b és el quadrat d'un element de K, aleshores les dues àlgebres $\left(\frac{ac,b}{K}\right)$ i $\left(\frac{c,b}{K}\right)$ són isomorfes a $\mathbf{M}(2,K)$; per tant, podem suposar que b no és un quadrat en K. La hipòtesi sobre l'àlgebra $\left(\frac{a,b}{K}\right)$ ens permet assegurar que l'equació $ax^2+by^2=z^2$ té solució no trivial en K; i, com que b no és un quadrat, ha de ser $x\neq 0$. Si dividim per x, podem suposar que existeixen elements $y,z\in K$ no tots dos nuls, tals que $a=z^2-by^2$.

Sigui $\{e_0,e_1,e_2,e_3\}$ una base de $\left(\frac{c,b}{K}\right)$ tal que $e_0=1$, $e_1^2=c$, $e_2^2=b$ i $e_3=e_1e_2=-e_2e_1$. Aleshores, els vectors $e_0':=e_0$, $e_1':=ze_1+ye_3$, $e_2':=e_2$, i $e_3':=e_1'e_2'=bye_1+ze_3$ són linealment independents, ja que el determinant d'aquests vectors en la base $\{e_0,e_1,e_2,e_3\}$ és el determinant

$$\begin{vmatrix} z & y \\ by & z \end{vmatrix} = z^2-by^2=a\neq 0.$$

A més a més, se satisfan les propietats ${e_1'}^2=z^2e_1^2+y^2e_3^2+zy(e_1e_3+e_3e_1)=z^2c-y^2bc=ac$, ${e_2'}^2=e_2^2=b$, i $e_2'e_1'=ze_2e_1+ye_2e_3=-ze_1e_2-ye_3e_2=-e_1'e_2'=-e_3'$. Per tant, l'àlgebra $\left(\frac{c,b}{K}\right)$ conté com a subàlgebra, de la mateixa dimensió, l'àlgebra $\left(\frac{ac,b}{K}\right)$, de manera que coincideixen. □

10.6 Símbol de Hilbert

L'objectiu d'aquesta secció és donar la definició del símbol de Hilbert i fer el seu càlcul en el cas dels cossos $\mathbb{R}$ i $\mathbb{Q}_p$, per a tot nombre primer p.

Ja hem observat que si K és un cos de característica diferent de 2, i si $a,b\in K$ són elements no nuls, aleshores l'àlgebra de quaternions $\left(\frac{a,b}{K}\right)$ o bé és un cos no commutatiu o bé és l'àlgebra $\mathbf{M}(2,K)$.

Definició 10.6.1. Sigui K un dels cossos $\mathbb{R}$ o $\mathbb{Q}_p$, p primer, i siguin $a,b\in K$ elements no nuls. Posarem $(a,b)_K=-1$ quan l'àlgebra de quaternions $\left(\frac{a,b}{K}\right)$ sigui un cos (no commutatiu) i $(a,b)_K=1$ quan sigui $\mathbf{M}(2,K)$. Direm que $(a,b)_K$ és el símbol de Hilbert sobre K de la parella (a,b). Sovint escriurem $(a.b)_\infty$ quan $K=\mathbb{R}$ i $(a,b)_p$ quan $K=\mathbb{Q}_p$.

Corol·lari 10.6.2. *Condició necessària i suficient perquè el símbol de Hilbert $(a,b)_K$ sigui 1 és que la forma quadràtica $aX^2+bY^2-Z^2$ representi zero en K.* □

Les propietats de les àlgebres de quaternions de la secció anterior es tradueixen en les següents per als símbols de Hilbert.

Corol·lari 10.6.3. *Siguin $a,b,c\in K$ elements no nuls qualssevol. Es tenen igualtats $(a,b)_K=(b,a)_K=(a,-ab)_K=(a,(1-a)b)_K=(a,bc^2)_K=(ac^2,b)_K$, la igualtat amb $(a,(1-a)b)_K$, sempre que $a\neq 1$. A més a més:*

$$(a,-a)_K=(a,1-a)_K=(a,b^2)_K=(a,1)_K=1.$$

Per últim, si $(a,b)_K=1$, aleshores $(ac,b)_K=(c,b)_K$. □

Observació 10.6.4. Quan $(a,b)_K = 1$ obtenim la igualtat $(ac,b)_K = (a,b)_K(c,b)_K$. Més endavant veurem que se satisfà sense aquesta hipòtesi restrictiva.

El càlcul del símbol de Hilbert en el cas $K = \mathbb{R}$ és gairebé immediat.

Proposició 10.6.5. *Siguin $a, b \in \mathbb{R}$ nombres no nuls. Aleshores:*

$$(a,b)_\infty = \begin{cases} -1, & \text{si } a,b < 0, \\ 1, & \text{si } a > 0 \text{ o bé } b > 0. \end{cases}$$

Demostració: Com que tot nombre real positiu és el quadrat d'un nombre real, si un dels dos nombres a, b és positiu, aleshores $(a,b)_\infty = 1$; d'altra banda, si $a < 0$, $b < 0$, aleshores $(a,b)_\infty = (-1,-1)_\infty = -1$, ja que l'equació $-x^2 - y^2 - z^2 = 0$ només té la solució trivial. □

La resta de la secció es dedica al càlcul del símbol de Hilbert en el cas $K = \mathbb{Q}_p$.

Lema 10.6.6. *Sigui p un nombre primer senar i siguin $u, v \in {\mathbb{Z}_p}^*$. Aleshores, $(u,v)_p = 1$.*

Demostració: La reducció mòdul $p\mathbb{Z}_p$ permet pensar u, v com a elements de ${\mathbb{F}_p}^*$; ara bé, hem provat més amunt que la forma quadràtica $ux^2 + vy^2 - z^2$ representa zero en ${\mathbb{F}_p}^*$, i que podem prendre $y = 1$. El lema de Hensel ens permet assegurar que podem trobar elements $x, y, z \in \mathbb{Z}_p$, no tots tres nuls, i tals que $ux^2 + vy^2 - z^2 = 0$ en $\mathbb{Z}_p$; per tant, $(u,v)_p = 1$, com volíem veure. □

Lema 10.6.7. *Siguin p un nombre primer senar i $v \in {\mathbb{Z}_p}^*$. Aleshores, $(p,v)_p = \left(\dfrac{v}{p}\right)$, el símbol de Legendre de la reducció mòdul p de l'element v.*

Demostració: Si v és un quadrat mòdul p, és a dir, si $\left(\dfrac{v}{p}\right) = 1$, en virtut del lema de Hensel v és un quadrat en $\mathbb{Z}_p$ i la forma quadràtica $px^2 + vy^2 - z^2$ representa zero en $\mathbb{Z}_p$; per tant, $(p,v)_p = 1$. Recíprocament, suposem que la forma quadràtica $px^2 + vy^2 - z^2$ representa zero en $\mathbb{Q}_p$; multiplicant els elements x, y, z per una potència adequada de p, podem suposar que $x, y, z \in \mathbb{Z}_p$ i que y, z no són divisibles per p. Aleshores, la reducció mòdul p de l'equació ens proporciona una igualtat $v = z^2 y^{-2}$ en ${\mathbb{F}_p}^*$, de manera que v és un quadrat en ${\mathbb{F}_p}^*$ i $\left(\dfrac{v}{p}\right) = 1$. □

Proposició 10.6.8. *Sigui p un nombre primer senar i siguin $a, b \in {\mathbb{Q}_p}^*$, escrits en la forma $a := p^r u$, $b := p^s v$, amb $r, s \in \mathbb{Z}$, i $u, v \in {\mathbb{Z}_p}^*$. Aleshores, $(a,b)_p = (up^r, vp^s)_p = (-1)^{rs\varepsilon(p)} \left(\dfrac{u}{p}\right)^s \left(\dfrac{v}{p}\right)^r$, on $\varepsilon(p) := \dfrac{p-1}{2}$.*

Demostració: Per les propietats del símbol de Hilbert, podem suposar que $r, s \in \{0,1\}$, de manera que només cal considerar tres casos: $r = s = 0$; $r = 1$, $s = 0$; i $r = s = 1$. El cas $r = s = 0$ és el contingut del lema **10.6.6**. En el cas $r = 1$, $s = 0$, i en virtut del fet, ja provat, que $(u,v)_p = 1$, obtenim que $(up, v)_p = (p, v)_p$, de manera que podem suposar que $u = 1$, i el resultat és el contingut del lema **10.6.7**. Per últim, podem escriure les igualtats $(up, vp)_p = (up, -uvp^2)_p = (up, -uv)_p = (p, -uv)_p = \left(\dfrac{-uv}{p}\right) = (-1)^{\varepsilon(p)} \left(\dfrac{u}{p}\right)\left(\dfrac{v}{p}\right)$, que és el que cal demostrar en aquest cas. □

Resta fer el càlcul en el cas $p = 2$. Per a això podem usar una versió diferent del lema de Hensel de la versió que s'ha demostrat més amunt; concretament, es farà ús del resultat següent que es proposa com a exercici (o bé, cf. [La 70]).

Lema 10.6.9. *Siguin K un cos complet respecte de la topologia definida per un valor absolut discret i A l'anell de la valoració. Sigui $f(X) \in A[X]$ un polinomi i $\alpha_0 \in A$ un element tals que $|f(\alpha_0| < |f'(\alpha_0)|^2$. Aleshores, la successió $\{\alpha_n\}_n$ definida recurrentment per la fórmula*

$$\alpha_{n+1} := \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

és convergent a un element $\alpha \in A$. Aquest element α és una arrel de $f(X)$ i se satisfà la desigualtat

$$|\alpha - \alpha_0| \leq \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1.$$

□

Corol·lari 10.6.10. *Sigui $a \in \mathbb{Z}_2^*$. Condició necessària i suficient perquè a sigui el quadrat d'un element de $\mathbb{Z}_2$ és que $a \equiv 1 \pmod 8$.*

Demostració: Considerem el polinomi $f(X) := X^2 - a$; si prenem $\alpha_0 = 1$, aleshores $|f(\alpha_0)|_2 \leq |8|_2 < |2|_2^2 = |f'(\alpha_0)|_2^2$, de manera que $X^2 - a$ té una arrel en $\mathbb{Z}_2$. El recíproc és clar, ja que si a és el quadrat d'un element de $\mathbb{Z}_2^*$, la seva reducció mòdul 8 és un quadrat en $(\mathbb{Z}/8\mathbb{Z})^*$, de manera que $a \equiv 1 \pmod 8$. □

Siguin, doncs, $a, b \in \mathbb{Q}_2^*$ elements no nuls escrits en la forma $a = 2^r u$, $b = 2^s v$, amb $r, s \in \mathbb{Z}$ i $u, v \in \mathbb{Z}_2^*$. Per a fer el càlcul del símbol de Hilbert $(a, b)_2$, podem suposar que $r, s \in \{0, 1\}$. Comencem, com abans, pel cas $r = s = 0$.

Lema 10.6.11. *Siguin $u, v \in \mathbb{Z}_2^*$. Aleshores, $(u, v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)}$.*

Demostració: Cal considerar les classes residuals mòdul 8 de u, v i aplicar el corol·lari anterior. Si $u \equiv 1 \pmod 8$, aleshores u és un quadrat en $\mathbb{Z}_2$, de manera que la forma quadràtica $ux^2 + vy^2 - z^2$ representa zero i $(u, v)_2 = 1$. Si $u \equiv 5 \pmod 8$, aleshores $u + 4v \equiv 1 \pmod 8$, ja que v no és divisible per 2; per tant, $u + 4v$ és un quadrat i l'equació $ux^2 + vy^2 - z^2 = 0$ té una solució $x = 1$, $y = 2$, z convenient; per tant, $(u, v)_2 = 1$; però $u \equiv 1 \pmod 4$, de manera que $\varepsilon(u)\varepsilon(v)$ és parell. Per simetria, resta considerar el cas $u \equiv v \equiv 3 \pmod 4$. Si l'equació $ux^2 + vy^2 - z^2$ tingués una solució en $\mathbb{Q}_2$, en multiplicar x, y, z per una potència adequada de 2 podríem suposar que exactament un dels elements x, y, z és divisible per 2; la reducció mòdul 4 de l'equació donaria una solució no trivial de $ux^2 + vy^2 - z^2 \equiv -x^2 - y^2 - z^2 \equiv 0 \pmod 4$, fet que no es dóna mai ja que el quadrat d'un nombre senar de $\mathbb{Z}/4\mathbb{Z}$ sempre és 1, de manera que la suma de dos d'ells no pot ser zero. Per tant, $(u, v)_2 = -1 = (-1)^{\varepsilon(u)\varepsilon(v)}$. □

Lema 10.6.12. *Siguin $u, v \in \mathbb{Z}_2^*$ qualssevol. Aleshores, $(2u, v)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$, on $\omega(v) := \dfrac{v^2 - 1}{8} \in \mathbb{Z}/2\mathbb{Z}$.*

Demostració: Comencem pel cas $u \equiv 1 \pmod 4$. Com que $(u, v)_2 = 1$, aleshores $(2u, v)_2 = (2, v)_2$ i cal veure que $(2, v)_2 = (-1)^{\omega(v)}$. Ara bé, si $(2, v)_2 = 1$, aleshores existeixen elements $x \in \mathbb{Z}_2$, $y, z \in \mathbb{Z}_2^*$ tals que $2x^2 + vy^2 - z^2 = 0$; en aquest cas, doncs,

com que $y^2 \equiv z^2 \equiv 1 \pmod 8$, és $2x^2 + v - 1 \equiv 0 \pmod 8$. Si tenim en compte que els quadrats mòdul 8 són els elements $0, 1, 4$, obtenim que $v \equiv 1 \pmod 8$, en el cas que $x \in 2\mathbb{Z}_2$ i que $v \equiv -1 \pmod 8$ en el cas que $x \in \mathbb{Z}_2^*$; per tant, $(-1)^{\omega(v)} = 1 = (2, v)_2$, com calia provar. Recíprocament, si $v \equiv 1 \pmod 8$, aleshores v és un quadrat en $\mathbb{Z}_2^*$ i $(2, v)_2 = 1$; i si $v \equiv -1 \pmod 8$, aleshores $2 + v \equiv 1 \pmod 8$ i $2 + v$ és un quadrat en $\mathbb{Z}_2^*$; aleshores, l'equació $2x^2 + vy^2 - z^2 = 0$ té solució $x = y = 1$, z convenient, i és $(2, v)_2 = 1$.

En segon lloc, si $v \equiv 1 \pmod 4$, aleshores $(u, v)_2 = 1$ i la igualtat $(2u, v)_2 = (2, v)_2$ acaba la prova, ja que $(2, v)_2 = (-1)^{\omega(v)}$ és el cas que hem provat. Encara, en el cas $u \equiv -1 \pmod 4$, $v \equiv -1 \pmod 8$, hem vist que $(2, v)_2 = 1$, de manera que la igualtat $(2u, v)_2 = (u, v)_2$ també acaba la prova.

Resten, per últim, els casos $u \equiv 3 \pmod 4$, $v \equiv 3 \pmod 8$. Un d'ells és el cas $u \equiv -1 \pmod 8$, $v \equiv 3 \pmod 8$; aleshores, $-u$, $v/3$ són quadrats de $\mathbb{Z}_2$ i podem escriure $(2u, v)_2 = (-2(-u), 3(v/3))_2 = (-2, 3)_2 = 1$, ja que l'equació $-2x^2 + 3y^2 - z^2 = 0$ té, evidentment, la solució $x = y = z = 1$ en $\mathbb{Z}_2$. Anàlogament, en l'altre cas podem escriure $(2u, v)_2 = (6, -5)_2 = 1$, ja que l'equació $6x^2 - 5y^2 - z^2 = 0$ té, també, la solució $x = y = z = 1$. □

Proposició 10.6.13. *Siguin $a, b \in \mathbb{Q}_2^*$, que escrivim en la forma $a := 2^r u$, $b := 2^s v$, amb $r, s \in \mathbb{Z}$, i $u, v \in \mathbb{Z}_2^*$. Aleshores,*

$$(2^r u, 2^s v)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + r\omega(v) + s\omega(u)},$$

on $\omega(x) := \dfrac{p^2 - 1}{8}$.

Demostració: Immediata a partir dels resultats anteriors. □

Corol·lari 10.6.14. *El símbol de Hilbert és una forma bilineal simètrica no degenerada sobre el $\mathbb{F}_2$-espai vectorial ${\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$.*

Demostració: En virtut de les propietats anteriors i del càlcul del valor del símbol que s'acaba de fer, només cal veure que és no degenerada. Per a això, donat un element $a \in {\mathbb{Q}_p}^*$ cal trobar-ne un altre, b, tal que $(a, b)_p = -1$. I això és senzill. Si p és senar, prenguem $u \in {\mathbb{Z}_p}^*$ tal que $\left(\dfrac{u}{p}\right) = -1$; aleshores, $\{1, u, p, up\}$ és un sistema de representants de ${\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$ i se satisfan les igualtats $(p, u)_p = (u, p)_p = (up, u)_p = -1$, de manera que per a cada element $x \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$ diferent del neutre la forma lineal $(x, *)_p$ és no trivial.

Anàlogament, en el cas $p = 2$ observem que $(-5, -1)_2 = (5, 2u)_2 = -1$, on u és una unitat que no és un quadrat. Això ja és suficient per a provar que la forma quadràtica és no degenerada, ja que els elements de $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ són els u o bé $2u$ amb $u \in \{1, -1, 5, -5\}$ i la forma és simètrica. □

10.7 Invariant de Hasse-Witt

A part de la dimensió, el rang i el discriminant, per a classificar les formes quadràtiques sobre $\mathbb{Q}_p$ cal un altre invariant.

Definició 10.7.1. Donada una forma quadràtica diagonal i no degenerada sobre $\mathbb{Q}_p$, $q := \langle a_1, \ldots, a_n \rangle$, posarem $w_p(q) := \prod_{1 \leq i < j \leq n} (a_i, a_j)_p$ i direm que $w_p(q)$ és l'invariant de Hasse-Witt de la forma quadràtica q.

Notem que $w_p(q) = \pm 1$; i cal veure que $w_p(q)$ no depèn de la base ortogonal en què haguem diagonalitzat la forma quadràtica.

Proposició 10.7.2. *Siguin $\{e_1, \ldots, e_n\}$, $\{e'_1, \ldots, e'_n\}$ bases ortogonals (ordenades) per a la forma quadràtica q. Aleshores,*

$$\prod_{1 \leq i < j \leq n} (a_i, a_j)_p = \prod_{1 \leq i < j \leq n} (a'_i, a'_j)_p.$$

Demostració: Si $n = 1$ no hi ha res a provar, ja que el producte és buit. Si $n = 2$, dir que $(a_1, a_2)_p = 1$ equival a dir que la forma quadràtica $a_1X^2 + a_2Y^2 - Z^2$ representa zero o, equivalentment, que la forma quadràtica q representa 1; i això no depèn de la base considerada. Resta el cas $n \geq 3$. En aquest cas, farem la prova en dues etapes: primerament veurem que si totes dues bases tenen un element en comú, aleshores se satisfà la igualtat desitjada, i a continuació provarem que existeix una successió de bases ortogonals, que comença amb la base $\{e_i\}$ i acaba amb la $\{e'_i\}$, de manera que cada una té un element en comú amb la següent.

Suposem que les dues bases tenen un element en comú. Com que el símbol de Hilbert és simètric, si permutem els elements d'una base, aleshores el valor del producte corresponent no canvia; per tant, podem suposar que $e'_1 = e_1$. Ara, la bilinealitat del símbol permet escriure el producte associat a la base $\{e_i\}$ en la forma

$$(a_1, a_2 \cdots a_n)_p \prod_{2 \leq i < j \leq n} (a_i, a_j)_p$$

i l'altre en la forma

$$(a'_1, a'_2 \cdots a'_n)_p \prod_{2 \leq i < j \leq n} (a'_i, a'_j)_p.$$

Si tenim en compte que el discriminant (mòdul quadrats) és el producte $a_1 \cdots a_n = a'_1 \cdots a'_n$, obtenim la igualtat $(a_1, a_2 \cdots a_n)_p = (a'_1, a'_2 \cdots a'_n)_p$. El lema de simplificació de Witt ens permet acabar la prova per inducció; en efecte, per ser e_1 no isòtrop, el seu ortogonal és no singular, de manera que se satisfà la igualtat

$$\prod_{2 \leq i < j \leq n} (a_i, a_j)_p = \prod_{2 \leq i < j \leq n} (a'_i, a'_j)_p$$

per hipòtesi d'inducció.

Veiem, doncs, l'existència de la successió de bases ortogonals que necessitem. Per a començar, suposem que existeix una parella d'elements $e \in \{e_i\}$ i $e' \in \{e'_i\}$ de manera que $(e \cdot e)(e' \cdot e') - (e \cdot e')^2 \neq 0$. Aleshores, e i e' són linealment independents i el subespai de dimensió 2 que generen, posem P, és un subespai no singular (observem que la desigualtat de què partim és el determinant de la matriu de la mètrica associada a aquest subespai). Podem, doncs, elegir una base ortogonal d'un suplementari ortogonal a P. Aleshores, es

passa de la base $\{e_i\}$ a la base $\{e'_i\}$ per les dues bases ortogonals que s'obtenen en afegir a aquesta base sengles bases ortogonals de P, una que contingui e i una que contingui e'.

Suposem, doncs, que per a totes les parelles (e, e') com abans se satisfà la igualtat $(e \cdot e)(e' \cdot e') - (e \cdot e')^2 = 0$. Si demostrem que existeix un vector no isòtrop u de la forma $u := e'_1 + \alpha e'_2$, i tal que el subespai $P := \langle e, u\rangle$ és no degenerat i de dimensió 2, ja haurem acabat, ja que, d'una banda, podem canviar els dos primers elements de la base $\{e'_i\}$ per u i un vector de $\langle e'_1, e'_2\rangle$ ortogonal a u, i de l'altra, acabarem com abans, si tenim en compte que P és un subespai no singular de dimensió 2.

El càlcul de $u \cdot u$ dóna $u \cdot u = e'_1 \cdot e'_1 + \alpha^2 e'_2 \cdot e'_2$; per tant, perquè u sigui no isòtrop cal elegir α de manera que $\alpha^2 \neq -(e'_1 \cdot e'_1)/(e'_2 \cdot e'_2)$ ($= -1$ si el cos és $\mathbb{F}_3$, en virtut de la hipòtesi); d'altra banda, que l'espai generat per e i u sigui no singular equival a dir, tenint en compte la hipòtesi, que $-2\alpha(e \cdot e'_1)(e \cdot e'_2) \neq 0$ o, equivalentment, que $\alpha \neq 0$. Així, només cal excloure (com a màxim) els valors de α que farien falses aquestes dues hipòtesis; i això es pot fer sempre si el cos té més de tres elements, o prenent $\alpha = 1$ si el cos és $\mathbb{F}_3$. □

10.8 Representació de nombres per formes

Per a dur a terme la classificació de les formes quadràtiques sobre el cos $\mathbb{Q}_p$ és convenient fer l'estudi, en primer lloc, de les condicions d'isotropia i de representació d'un nombre per una forma quadràtica.

Recordem que hem reduït la classificació de les formes quadràtiques al cas de formes quadràtiques no singulars i que, a més a més, podem suposar-les diagonalitzades. D'altra banda, podem suposar fixats els invariants rang i discriminant, així com l'invariant de Hasse-Witt.

Lema 10.8.1. *Sigui (V, q) un espai quadràtic no singular sobre un cos qualsevol K de caraterística diferent de 2. Si la forma q representa zero, aleshores representa tot element de K.*

Demostració: Sigui $v \in V$ un vector isòtrop no nul, que existeix per hipòtesi. Aleshores, podem trobar un pla hiperbòlic de la forma $H := \langle v, w\rangle$ de manera que $V = H \perp H^\perp$; és suficient, doncs, demostrar que el resultat és cert per a un pla hiperbòlic. Podem prendre una base v, w de manera que la matriu de la mètrica en aquesta base sigui la matriu

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

i, aleshores, el vector $x := v + \dfrac{\alpha}{2} w$ és tal que $q(v) = \alpha$, qualsevol que sigui l'element $\alpha \in K$. □

Proposició 10.8.2. *Siguin q una forma quadràtica no singular i $\alpha \in K$ un element no nul. Posem $q_\alpha := q \perp \langle -\alpha\rangle$ la suma ortogonal de la forma q amb la forma $\langle -\alpha\rangle$. Aleshores, condició necessària i suficient perquè q representi α és que q_α representi 0.*

Demostració: Clarament, si q representa α, aleshores q_α representa 0. Recíprocament, si la forma q_α representa zero, podem prendre elements $x_1, \ldots, x_n, y \in K$, no tots nuls,

de manera que $q(x_1,\dots,x_n)=\alpha y^2$; si $y=0$, aleshores q representa zero i, en virtut del lema anterior, representa tot element no nul de K, en particular, α. Si, en canvi, $y\neq 0$, podem escriure $q\left(\frac{x_1}{y},\dots,\frac{x_n}{y}\right)=\alpha$, que dóna una representació de α per la forma q. □

Ara estem en condicions d'estudiar les condicions d'isotropia d'una forma quadràtica no singular sobre el cos $\mathbb{Q}_p$. De fet, enunciarem simultàniament les condicions d'isotropia i les condicions que han de satisfer els invariants d'una forma quadràtica definida sobre $\mathbb{Q}_p$ a fi que aquesta forma quadràtica representi un elemenet donat $\alpha\in\mathbb{Q}_p$.

Proposició 10.8.3. *Siguin p un nombre primer, q una forma quadràtica no singular de rang n sobre $\mathbb{Q}_p$, $\Delta(q)$ el seu discriminant (mòdul quadrats no nuls de $\mathbb{Q}_p$), i $w_p(q)$ el seu invariant de Hasse-Witt. La taula següent resumeix les condicions que han de satisfer el rang, el discriminant i l'invariant de Hasse-Witt perquè la forma quadràtica q sigui isòtropa; és a dir, perquè representi* 0.

$rang(q)$	$\Delta(q)$	$w_p(q)$
2	-1	$*$
3	$*$	$(-1,-\Delta(q))_p$
4	$\neq 1$	$*$
4	1	$(-1,-1)_p$
≥ 5	$*$	$*$

Anàlogament, donat un element qualsevol $\alpha\in{\mathbb{Q}_p}^*$, la taula següent ens ensenya les condicions que han de satisfer els invariants perquè la forma quadràtica q representi α.

$rang(q)$	$\Delta(q)$	$w_p(q)$
1	α	$*$
2	$*$	$(\alpha,-\Delta(q))_p$
3	$\neq -\alpha$	$*$
3	$-\alpha$	$(-1,-\Delta(q))_p$
≥ 4	$*$	$*$

Demostració: La demostració de la proposició es fa alhora per a les dues taules. Comencem per veure que de les condicions d'isotropia per a rang n es dedueixen les condicions de representació d'un element α per a rang $n-1$. En efecte, donat $\alpha\in{\mathbb{Q}_p}^*$, posem q_α la suma ortogonal de les formes q i $\langle-\alpha\rangle$. Aleshores, $\mathrm{rang}(q_\alpha)=1+\mathrm{rang}(q)$, $\Delta(q_\alpha)=-\alpha\Delta(q)$, $w_p(q_\alpha)=(\Delta(q),-\alpha)_p w_p(q)$, i sabem que q representa α si, i només si, q_α representa 0. Per tant, només cal mirar les dues taules i la demostració és evident. Potser només remarcar l'invariant de Hasse-Witt de la fila 2 de la segona taula: dir que q representi α equival a dir que q_α representi 0, és a dir, que $w_p(q_\alpha)=(-1,-\Delta(q_\alpha))_p=(-1,\alpha\Delta(q))_p$; per tant,

$$\begin{aligned} w_p(q) &= w_p(q_\alpha)(\Delta(q),-\alpha)_p \\ &= (-1,\alpha\Delta(q))_p(\Delta(q),-\alpha)_p \\ &= (-1,-\Delta(q))_p(-1,-\alpha)_p(\Delta(q),-\alpha)_p \\ &= (-1,-\Delta(q))_p(-\Delta(q),-\alpha)_p \\ &= (-\Delta(q),\alpha)_p. \end{aligned}$$

El contingut de la fila 4 es demostra anàlogament tenint en compte que $\Delta(q) = -\alpha$.

Resta, doncs, demostrar la primera taula. Comencem pel cas de rang 2; el fet que la forma q representi 0 equival a dir que l'espai quadràtic és un pla hiperbòlic; i això és dir que $\Delta(q) = -1$.

Estudiem el cas de rang 3. Ara podem escriure q en la forma $q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ i dir que q és isòtropa equival a dir que ho és $-a_3q$; però $-a_3q$ és equivalent a la forma $\langle -a_3a_1, -a_3a_2, -1\rangle$, de manera que, per definició del símbol de Hilbert, condició necessària i suficient perquè q representi 0 és que sigui $(-a_3a_1, -a_3a_2)_p = 1$. Però

$$\begin{aligned}(-a_3a_1, -a_3a_2)_p &= (a_1, -a_3a_2)_p(-a_3, -a_3a_2)_p\\ &= (a_1, a_2)_p(a_1, a_3)_p(a_1, -1)_p(-1, -a_2a_3)_p(a_3, -a_2a_3)_p\\ &= (a_1, a_2)_p(a_1, a_3)_p(-1, -a_1a_2a_3)_p(a_3, -a_2a_3)_p\\ &= (a_1, a_2)_p(a_1, a_3)_p(-1, -a_1a_2a_3)_p(a_3, a_2)_p\\ &= (-1, -a_1a_2a_3)_p w_p(q),\end{aligned}$$

de manera que la condició que sigui 1 és equivalent a dir que $w_p(q) = (-1, -\Delta(q))_p$.

Anem a veure el cas de rang 4. La forma s'escriu com la suma ortogonal de les dues formes de rang 2 $\langle a_1, a_2\rangle$ i $\langle a_3, a_4\rangle$, i representa 0 si, i només si, existeix un element $\beta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$ tal que les formes $\langle a_1, a_2\rangle$ i $\langle -a_3, -a_4\rangle$ representen β; però per a això podem mirar la segona taula per a rang 2, que ja s'ha demostrat. Dir que $\langle a_1, a_2\rangle$ representa β equival a dir que se satisfà la condició $w_p(\langle a_1, a_2\rangle) = (\beta, -\Delta(\langle a_1, a_2\rangle))_p$; és a dir, que és $(a_1, a_2)_p = (\beta, -a_1a_2)_p$. Anàlogament, dir que $\langle -a_3, -a_4\rangle$ representa β equival a dir que se satisfà la condició $(-a_3, -a_4)_p = (\beta, -a_3a_4)_p$. Posem

$$\begin{aligned}A &:= \{\beta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2} : (\beta, -a_1a_2)_p = (a_1, a_2)_p\},\\ B &:= \{\beta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2} : (\beta, -a_3a_4)_p = (-a_3, -a_4)_p\}.\end{aligned}$$

Amb aquestes notacions hem vist que q representa 0 si, i només si, $A \cap B$ és no buit. Ara bé, les condicions perquè això succeeixi les deduirem del resultat següent.

Lema 10.8.4. *Donat $\alpha \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$, posem $H_\alpha^w := \{\beta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2} : (\beta, \alpha)_p = w\}$, per a $w = \pm 1$. Aleshores:*

(a)
$$\#H_\alpha^w = \begin{cases} 4, & \text{si } \alpha = 1,\ w = 1,\ p \neq 2,\\ 8, & \text{si } \alpha = 1,\ w = 1,\ p = 2,\\ 0, & \text{si } \alpha = 1,\ w = -1,\\ 2, & \text{si } \alpha \neq 1,\ p \neq 2,\\ 4, & \text{si } \alpha \neq 1,\ p = 2.\end{cases}$$

(b) *Si H_α^w i $H_{\alpha'}^{w'}$ són no buits, aleshores condició necessària i suficient perquè siguin disjunts és que $\alpha = \alpha'$ i $w = -w'$.*

Demostrarem el lema més endavant; ara l'aplicarem per a acabar de provar la proposició. Observem que els conjunts A i B de la proposició són els casos particulars $\alpha = -a_1a_2$, $w = (a_1, a_2)_p$, i $\alpha = -a_3a_4$, $w = (-a_3, -a_4)_p$, respectivament, dels conjunts H_α^w. Per tant, cal veure en quines condicions $H_{-a_1a_2}^{(a_1,a_2)_p} \cap H_{-a_3a_4}^{(-a_3,-a_4)_p}$ és no buit.

Observem, en primer lloc, que $(a_1, -a_1a_2)_p = (a_1, a_2)_p$ i que, de manera similar, $(-a_3, -a_3a_4)_p = (-a_3, -a_4)_p$, de manera que $a_1 \in A$ i $-a_3 \in B$ i A i B són no buits. Per tant, aquesta intersecció és buida quan se satisfan simultàniament les condicions $-a_1a_2 = -a_3a_4$ i $(a_1, a_2)_p = -(-a_3, -a_4)_p$. Com que el discriminant és $\Delta(q) = a_1a_2a_3a_4$, mòdul quadrats, la primera condició equival a dir que $\Delta(q) = 1$ i, en conseqüència, condició necessària i suficient perquè $A \cap B = \varnothing$ és que $\Delta(q) = 1$ i $(a_1, a_2)_p = -(-a_3, -a_4)_p$. D'altra banda, si calculem l'invariant de Hasse-Witt de la forma q obtenim que

$$\begin{aligned}
w_p(q) &= (a_1, a_2)_p(a_3, a_4)_p(a_1a_2, a_3a_4)_p \\
&= (a_1, a_2)_p(a_3, a_4)_p(a_3a_4, a_3a_4)_p(\Delta(q), a_3a_4)_p \\
&= (a_1, a_2)_p(a_3, a_4)_p(-1, a_3a_4)_p(\Delta(q), a_3a_4)_p \\
&= (a_1, a_2)_p(-1, -1)_p(-1, -1)_p(a_3, a_4)_p(-1, a_3a_4)_p(\Delta(q), a_3a_4)_p \\
&= (a_1, a_2)_p(-1, -1)_p(a_3, a_4)_p(-1, -a_3a_4)_p(\Delta(q), a_3a_4)_p \\
&= (a_1, a_2)_p(-1, -1)_p(-1, a_3)_p(-1, -a_4)_p(a_3, a_4)_p(\Delta(q), a_3a_4)_p \\
&= (a_1, a_2)_p(-1, -1)_p(-1, -a_4)_p(a_3, -a_4)_p(\Delta(q), a_3a_4)_p \\
&= (a_1, a_2)_p(-1, -1)_p(-a_3, -a_4)_p(\Delta(q), a_3a_4)_p.
\end{aligned}$$

Podem acabar immediatament la prova del cas de rang 4. Condició necessària i suficient perquè q representi 0 és que la intersecció $A \cap B$ sigui no buida; és a dir, que $\Delta(q) \neq 1$ o bé que $\Delta(q) = 1$ i $(a_1, a_2)_p = (-a_3, -a_4)_p$; i això equival, en el cas $\Delta(q) = 1$, a dir que $w_p(q) = (-1, -1)_p$, ja que $w_p(q) = (a_1, a_2)_p(-1, -1)_p(-a_3, -a_4)_p$.

Resta demostrar el cas de rang ≥ 5 de la primera taula i el lema. Per a demostrar el cas de rang ≥ 5 és suficient, ja que no hi ha condicions, demostrar-lo en el cas de rang 5. Suposem, doncs, que $q := \langle a_1, a_2, a_3, a_4, a_5\rangle$ és de rang 5. Posem $d := a_1a_2$, $w := (a_1, a_2)_p$; la fila corresponent a rang 2 de la segona taula (que ja ha estat provada) ens permet assegurar que la forma $\langle a_1, a_2\rangle$ representa tots els elements de H^w_{-d}. En efecte, donat $\alpha \in {\mathbb{Q}_p}^*$, condició necessària i suficient perquè la forma $\langle a_1, a_2\rangle$ representi β és que $(\beta, -d)_p = w$; és a dir, que $\beta \in H^w_{-d}$. Suposem que $H^w_{-d} = \varnothing$; equivalentment, $-d = 1$ i $w = -1$; això implica que $a_1 = -a_2$, de manera que, evidentment, la forma q representa 0. En el cas $H^w_{-d} \neq \varnothing$, existeix $\beta \in H^w_{-d}$ tal que $\beta \neq \Delta(q)$, ja que el conjunt H^w_{-d} té, com a mínim, dos elements. Això ens permet assegurar que q és la suma ortogonal de la forma $\langle\beta\rangle$ amb una forma q' de rang necessàriament 4 i de determinant $\beta\Delta(q) \neq 1$; en virtut del que hem provat més amunt, la forma q' representa 0 i, en conseqüència, la forma q també. □

Resta, doncs, demostrar el lema. Si $\alpha = 1$, aleshores $(\beta, \alpha)_p = 1$ per a tot element β, de manera que els tres primers casos del primer apartat són immediats. D'altra banda, considerem $\alpha \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$, $\alpha \neq 1$. Com que el símbol de Hilbert $(\alpha, \beta)_p$ és no degenerat, l'aplicació ${\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2} \xrightarrow{w_\alpha} \{\pm 1\}$ donada per l'assignació $\beta \mapsto (\alpha, \beta)_p$ és exhaustiva. En conseqüència, $H^1_\alpha = \mathrm{Ker}(w_\alpha)$ és un subgrup d'índex 2 de ${\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$ i H^{-1}_α és el complementari, de manera que el cardinal coincideix i és la meitat de l'ordre de ${\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$. Això demostra la primera part.

Per a la segona, suposem que H^w_α i $H^{w'}_{\alpha'}$ són no buits; això només exclou el conjunt H^{-1}_1. Si $H^w_\alpha \cap H^{w'}_{\alpha'} = \varnothing$, aleshores $H^w_\alpha = H^{-w'}_{\alpha'}$, de manera que també $H^{-w}_\alpha = H^{w'}_{\alpha'}$; i, com que $1 \in H^1_\alpha \cap H^1_{\alpha'}$, ha de ser $H^1_\alpha = H^1_{\alpha'}$. En conseqüència, per a tot element $\beta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$ és $(\beta, \alpha')_p = (\beta, \alpha)_p$ i, com que el símbol de Hilbert és no degenerat, ha de ser $\alpha' = \alpha$; d'aquí es dedueix, doncs, que $w' = -w$. El recíproc és immediat. □

10.9 Descripció de les classes d'equivalència

Els resultats de la secció anterior són, de fet, la classificació de les formes quadràtiques no degenerades sobre $\mathbb{Q}_p$. En aquesta, es tracta de fer una descripció de les classes d'equivalència.

Teorema 10.9.1 (Classificació de les formes quadràtiques no degenerades sobre $\mathbb{Q}_p$)**.** *Siguin q_1, q_2 formes quadràtiques no degenerades sobre $\mathbb{Q}_p$. Condició necessària i suficient perquè q_1 i q_2 siguin equivalents és que tinguin el mateix rang, el mateix discriminant i el mateix invariant de Hasse-Witt.*

Demostració: Només resta demostrar la suficiència. La proposició anterior ens permet assegurar que si les formes tenen aquests mateixos tres invariants, aleshores representen els mateixos elements de $\mathbb{Q}_p$; per tant, existeix $\alpha \in {\mathbb{Q}_p}^*$ tal que q_1 i q_2 representen α. Si les formes són de rang 1, són necessàriament equivalents a la forma $\langle\alpha\rangle$ i, per tant, equivalents entre si. Si el rang és > 1, aleshores existeixen formes q_1', q_2' de rang una unitat inferior tals que $q_1 = \langle\alpha\rangle \perp q_1'$ i $q_2 = \langle\alpha\rangle \perp q_2'$; per definició de discriminant i de l'invariant de Hasse-Witt, les formes q_1' i q_2' tenen també el mateix discriminant i el mateix invariant de Hasse-Witt, de manera que podem acabar la prova per inducció sobre el rang. □

Corol·lari 10.9.2. *Existeix una forma quadràtica de rang 4 sobre $\mathbb{Q}_p$, i només una llevat d'equivalència, que no representa 0. Es pot escriure en la forma $X^2 - aY^2 - bZ^2 + abT^2$ per a qualsevol parella d'elements $a, b \in {\mathbb{Q}_p}^*$ tals que $(a, b)_p = -1$.*

Demostració: L'existència és clara; si hom pren $a, b \in {\mathbb{Q}_p}^*$ tals que $(a, b)_p = -1$, fet que és possible perquè el símbol de Hilbert és no degenerat, la forma de l'enunciat no representa zero, per definició del símbol de Hilbert. Cal veure la unicitat. Però això és una conseqüència immediata de la proposició que caracteritza les condicions d'isotropia d'una forma. En efecte, perquè una forma de rang 4 no representi 0 és necessari i suficient que el seu discriminant sigui 1 i el seu invariant de Hasse-Witt sigui $-(-1, -1)_p$. En particular, això determina els invariants de la forma, de manera que la unicitat és conseqüència del teorema de classificació anterior. □

Corol·lari 10.9.3. *Sobre $\mathbb{Q}_p$ només hi ha dues classes d'isomorfisme d'àlgebres de quaternions: una és l'àlgebra de matrius quadrades $\mathbf{M}(2, \mathbb{Q}_p)$ i l'altra és un cos no commutatiu, donat per qualsevol parella de paràmetres $a, b \in {\mathbb{Q}_p}^*$ tals que $(a, b)_p = -1$.* □

De vegades és convenient saber si hi ha alguna forma quadràtica que tingui invariants donats. El resultat següent ho caracteritza.

Proposició 10.9.4. *Siguin p un nombre primer, $n \geq 1$ un nombre enter, $w \in \{\pm 1\}$, i $\Delta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$. Condició necessària i suficient perquè existeixi una forma quadràtica no degenerada sobre $\mathbb{Q}_p$ de rang n, discriminant Δ i invariant de Hasse-Witt w és que se satisfacin les restriccions següents:*

(a) *Si $n = 1$, aleshores $w = 1$;*

(b) *Si $n = 2$, aleshores $\Delta \neq -1$ o bé $\Delta = -1$ i $w = 1$.*

DEMOSTRACIÓ: El cas de rang $n = 1$ és clar, ja que l'invariant de Hasse-Witt d'una forma quadràtica no degenerada de rang 1 és 1 i la forma ΔX^2 és de discriminant Δ.

El cas $n = 2$ amb $\Delta = -1$ també és clar. En efecte, la forma quadràtica $aX^2 + bY^2$ és de discriminant $\Delta := ab$ i té invariant de Hasse-Witt $w_p := (a, b)_p = (a, -ab)_p = (a, -\Delta)_p$; per tant, si $\Delta = -1$, aleshores $w_p = 1$. Això demostra la necessitat. La suficiència és clara ja que, d'una banda, un pla hiperbòlic és de discriminant -1 i el valor del seu invariant de Hasse-Witt és 1; i de l'altra, si $\Delta \neq -1$, aleshores podem trobar un element $a \in {\mathbb{Q}_p}^*$ tal que $(a, -\Delta)_p = w_p$, perquè el símbol de Hilbert és no degenerat; en aquest cas, els invariants de la forma $\langle a, a\Delta\rangle$ són els donats.

Anem al cas $n \geq 3$. Si demostrem que en el cas $n = 3$ sempre podem trobar una forma amb els invariants donats, el mateix succeirà en els casos $n > 3$, ja que podem prendre la forma quadràtica q de la forma $q := \langle 1\rangle \perp \cdots \perp \langle 1\rangle \perp q'$, amb $n - 3$ formes $\langle 1\rangle$ i una forma q' de rang 3, amb discriminant i invariant de Hasse-Witt iguals que els que volem. Però si prenem $a \in {\mathbb{Q}_p}^*$ diferent de $-\Delta$ mòdul quadrats, acabem de veure en el cas $n = 2$ que existeix una forma quadràtica q' de rang 2 amb invariants $a\Delta \neq -1$ i invariant de Hasse-Witt $(a, -\Delta)_p w$; la forma $q := \langle a\rangle \perp q'$ satisfà el que desitgem. □

Corol·lari 10.9.5. *El nombre de classes d'equivalència de formes quadràtiques no degenerades de rang n sobre $\mathbb{Q}_p$ és donat per la taula següent:*

rang(q)	p	*nombre*
1	$\neq 2$	4
1	$= 2$	8
2	$\neq 2$	7
2	$= 2$	15
≥ 3	$\neq 2$	8
≥ 3	$= 2$	16

□

Capítol 11

Formes quadràtiques racionals

En aquest capítol es procedeix a fer l'estudi i la classificació de les formes quadràtiques sobre el cos dels nombres racionals.

11.1 Propietats globals del símbol de Hilbert

Per a començar la classificació de les formes quadràtiques sobre el cos dels nombres racionals cal establir la fórmula del producte per als símbols de Hilbert associats a una parella de nombres racionals no nuls.

Donats $a, b \in \mathbb{Q}^*$, podem considerar tots els símbols de Hilbert $(a,b)_p$ i $(a,b)_\infty$, ja que $\mathbb{Q}$ es pot considerar com a subcòs de cada un dels cossos $\mathbb{Q}_p$ i $\mathbb{R}$.

Teorema 11.1.1 (Fórmula del producte)**.** *Sigui P el conjunt de tots els nombres naturals primers. Donats $a, b \in \mathbb{Q}^*$, el conjunt dels nombres $p \in P$ tals que $(a,b)_p \neq 1$ és finit i se satisfà la igualtat*

$$\prod_{p \in P \cup \{\infty\}} (a,b)_p = 1.$$

Demostració: Si tenim en compte la bilinealitat dels símbols de Hilbert $(*,*)_p$ per a $p \in P \cup \{\infty\}$, és suficient considerar els casos $a, b \in \{-1, \ell\}$, per a $\ell \in P$. Posarem $\Pi := \prod_{p \in P \cup \{\infty\}} (a,b)_p$ i distingirem casos.

Cas $a = b = -1$. Si $p \in P$ i $p \neq 2$, el càlcul que hem fet en el capítol anterior dels símbols de Hilbert ens permet assegurar que $(-1,-1)_p = 1$; en particular, el producte és finit i val $\Pi = (-1,-1)_2(-1,-1)_\infty$. Però ja hem vist, també, que $(-1,-1)_2 = (-1,-1)_\infty = -1$, de manera que el resultat queda provat.

Cas $a = -1$, $b = 2$. Anàlogament, si $p \neq 2$ els elements $-1, 2$ són invertibles en $\mathbb{Z}_p$, de manera que per a $p \in P$, $p \neq 2$, és $(-1,2)_p = 1$. Però ara se satisfan les igualtats $(-1,2)_2 = (-1,2)_\infty = 1$, la primera en virtut del càlcul que hem esmentat més amunt i la segona perquè $2 > 0$ en $\mathbb{R}$, per exemple. En particular, $(-1,2)_p = 1$ per a tot $p \in P \cup \{\infty\}$.

Cas $a = -1$, $b = \ell \neq 2$. Si $p \in P$ és diferent de 2 i de ℓ, i també si $p = \infty$, és $(-1,\ell)_p = 1$; i, d'altra banda, $(-1,\ell)_2 = (-1,\ell)_\ell = (-1)^{\varepsilon(\ell)}$.

Cas $a = b = \ell \in P$. La igualtat $(\ell,\ell)_p = (\ell,-\ell^2)_p = (-1,\ell)_p$ redueix aquest cas als anteriors.

Cas $a = 2$; $b = \ell \neq 2$. Si $p \in P \cup \{\infty\}$, $p \neq 2, \ell$, aleshores $(2, \ell)_p = 1$; d'altra banda, $(2, \ell)_2 = (-1)^{\omega(\ell)}$ i $(2, \ell)_\ell = \left(\frac{2}{\ell}\right) = (-1)^{\omega(\ell)}$.

Cas $a = \ell$, $b = \ell'$, $\ell \neq \ell'$, $\ell, \ell' \in P$. Si $p \in P \cup \{\infty\}$, $p \neq 2, \ell, \ell'$, aleshores $(\ell, \ell')_p = 1$; a més a més, $(\ell, \ell')_2 = (-1)^{\varepsilon(\ell)\varepsilon(\ell')}$, mentre que $(\ell, \ell')_{\ell'} = (-1)^{\varepsilon(\ell)\varepsilon(\ell')}(\ell, \ell')_\ell$, de manera que el producte és, certament, 1. □

No perdem de vista que l'objectiu d'aquest capítol és classificar les formes quadràtiques racionals. Per tant, podem començar per recordar els invariants associats a una forma quadràtica racional.

Sigui $q := \langle a_1, \ldots, a_n \rangle$ una forma quadràtica diagonalitzada, no singular, amb $a_i \in \mathbb{Q}^*$, per a $1 \leq i \leq n$. Aleshores, podem fer la llista següent dels invariants associats a q. D'una banda, el rang, n, i el discriminant, $\Delta(q) := a_1 \cdot \cdots \cdot a_n \in \mathbb{Q}^*/\mathbb{Q}^{*2}$; i, de l'altra, per a cada nombre primer $p \in P$, l'invariant de Hasse-Witt, $w_p(q) := \prod_{1 \leq i < j \leq n} (a_i, a_j)_p = \pm 1$, l'invariant de Hasse-Witt $w_\infty(q) := \prod_{1 \leq i < j \leq n} (a_i, a_j)_\infty = \pm 1$, i la signatura de q. Recordem que la forma quadràtica q és equivalent a una única forma quadràtica real de la forma $X_1^2 + \cdots + X_r^2 - (Y_1^2 + \cdots + Y_s^2)$, amb $r + s = n$; la signatura la definim com la parella de nombres naturals (r, s). En particular, el discriminant es pot considerar de manera única com un nombre enter lliure de quadrats.

De totes maneres, no és cert que aquests invariants siguin independents. De fet, la fórmula del producte ens proporciona algunes restriccions importants.

Lema 11.1.2. *Amb les notacions precedents, per a tot nombre primer $p \neq 2$ tal que p no divideix el producte $a_1 \cdot \cdots \cdot a_n$ és $w_p(q) = 1$. A més a més, se satisfà la igualtat* $\prod_{p \in P \cup \{\infty\}} w_p(q) = 1$.

Demostració: La primera propietat es dedueix immediatament del fet que per a tot nombre primer $p \neq 2$ que no divideix el producte $a_i a_j$ el símbol de Hilbert $(a_i, a_j)_p$ és trivial. A més a més, per a cada parella (i, j), el producte dels símbols de Hilbert $(a_i, a_j)_p$ sobre tots els elements de $P \cup \{\infty\}$ és 1; per tant, la segona propietat es dedueix per multiplicació finita. □

11.2 Lema d'aproximació

A l'hora de fer la classificació de les formes quadràtiques racionals i, sobretot, a l'hora de descriure les classes d'equivalència, és convenient de saber en quines condicions existeixen nombres racionals amb símbols de Hilbert donats. I per a això, convé disposar del lema d'aproximació.

Teorema 11.2.1 (Lema d'aproximació)**.** *Sigui $S \subseteq P \cup \{\infty\}$ un subconjunt finit. La imatge del morfisme diagonal $\mathbb{Q} \longrightarrow \prod_{p \in S} \mathbb{Q}_p$ (on $\mathbb{Q}_\infty := \mathbb{R}$) és densa.*

Demostració: A l'hora de fer la prova podem suposar que $\infty \in S$, ja que si la imatge de $\mathbb{Q}$ en $\prod_{p \in S \cup \{\infty\}} \mathbb{Q}_p$ és densa, també ho és la imatge de $\mathbb{Q}$ en $\prod_{p \in S} \mathbb{Q}_p$.

Donat un element $\mathbf{x} := (x_\infty, x_1, \ldots, x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n}$, cal veure que $\mathbf{x}$ pertany a l'adherència de $\mathbb{Q}$ en aquest producte. I si multipliquem $\mathbf{x}$ per un enter adequat per a treure els denominadors, podem suposar que, per a $1 \leq i \leq n$, és $x_i \in \mathbb{Z}_{p_i}$.

Cal comprovar que per a tot nombre real $\varepsilon > 0$ i per a tot nombre natural $N > 0$, existeix un element $x \in \mathbb{Q}$ tal que $|x - x_\infty| \leq \varepsilon$ i $v_p(x - x_i) \geq N$, per a tot índex i. Posem $m_i := p_i^N$. El teorema xinès del residu ens permet assegurar que existeix $x_0 \in \mathbb{Z}$ tal que per a tot índex i se satisfà la desigualtat $v_{p_i}(x_0 - x_i) \geq N$. D'altra banda, és un exercici elemental veure que, donat un nombre enter $q \geq 2$ de manera que $\mathrm{mcd}(q, p_1 \cdots p_n) = 1$, el subconjunt $\{a/q^m : a \in \mathbb{Z}, m \geq 0\}$ és dens en $\mathbb{R}$. Per tant, podem elegir un nombre enter a i un nomre natural m de manera que $\left| \dfrac{x_0 - x_\infty}{p_1^N \cdots p_n^N} + \dfrac{a}{q^m} \right| \leq \dfrac{\varepsilon}{p_1^N \cdots p_n^N}$, desigualtat que es pot escriure en la forma $|x_0 - x_\infty + u p_1^N \cdots p_n^N| \leq \varepsilon$, on $u := aq^{-m}$. Si ara prenem $x := x_0 + u p_1^N \cdots p_n^N$, se satisfan les desigualtats que volíem, ja que, per a tot índex i, és $v_{p_i}(x - x_i) \geq \inf(v_{p_i}(x - x_0), v_{p_i}(x_0 - x_i)) \geq N$. □

Per a la demostració de l'existència de nombres racionals amb símbols de Hilbert donats utilitzarem el teorema de Dirichlet de la progressió aritmètica. Aquest teorema, que ara enunciarem en la forma feble que farem servir, es demostrarà més endavant (cf. el teorema **14.3.1**).

Teorema 11.2.2 (Dirichlet)**.** *Donats nombres $a, m \in \mathbb{N}$ primers entre si, $a, m \neq 0$, el conjunt $\{a + \lambda m : \lambda \in \mathbb{N}\}$ conté una infinitat de nombres primers.*

El darrer resultat que provarem en aquesta secció és l'existència de nombres racionals amb símbols de Hilbert donats.

Proposició 11.2.3. *Considerem un conjunt finit $\{a_1, \ldots, a_n\} \subseteq \mathbb{Q}^*$ fixat i, per a tot element $\ell \in P \cup \{\infty\}$, siguin $w_{1,\ell}, \ldots, w_{n,\ell} \in \{\pm 1\}$. Condició necessària i suficient perquè existeixi un nombre racional $x \in \mathbb{Q}^*$ tal que $(a_i, x)_\ell = w_{i,\ell}$, per a tota parella (i, ℓ), és que se satisfacin les restriccions següents:*

(a) *per a tota parella (i, ℓ), llevat d'un nombre finit, $w_{i,\ell} = 1$;*

(b) *per a tot i, $\displaystyle\prod_{\ell \in P \cup \{\infty\}} w_{i,\ell} = 1$; i*

(c) *per a tot $\ell \in P \cup \{\infty\}$ existeix $x_\ell \in \mathbb{Q}_\ell^*$ tal que per a $1 \leq i \leq n$ és $(a_i, x_\ell)_\ell = w_{i,\ell}$.*

Demostració: La necessitat és immediata, en virtut de la fórmula del producte per al símbol de Hilbert. Es tracta de demostrar la suficiència.

Si cal, multipliquem per quadrats no nuls, i podem suposar que els nombres a_i són enters lliures de quadrats. A més a més, els conjunts

$$S := \{2, \infty\} \cup \{\ell : \text{ existeix } i \text{ tal que } \ell \text{ divideix } a_i\},$$

$$T := \{\ell \in P \cup \{\infty\} : w_{i,\ell} = -1, \text{ per a algun índex } i\}$$

són finits. Farem la demostració en dos casos.

Primer cas: $S \cap T = \varnothing$.

Siguin $a := \prod\{\ell : \ell \in T - \{\infty\}\}$, $m := 8 \prod\{\ell : \ell \in S - \{2, \infty\}\}$. Com que $S \cap T = \varnothing$, aleshores $\mathrm{mcd}(a, m) = 1$ i el teorema de Dirichlet de la progressió aritmètica ens permet

assegurar que existeix un nombre primer p tal que $p \notin S \cup T$ i $p \equiv a \pmod{m}$. Posem $x := ap > 0$. Només cal veure que, per a tota parella (i, ℓ), és $(a_i, x)_\ell = w_{i,\ell}$.

Observem, en primer lloc, que x és un quadrat en $\mathbb{R}$; d'altra banda, x és un quadrat no nul mòdul 8 i mòdul ℓ per a tot nombre primer $\ell \in S$; en conseqüència, el lema de Hensel ens permet assegurar que x és un quadrat en $\mathbb{Q}_\ell$ per a tot nombre primer $\ell \in S$; en particular, $(a_i, x)_\ell = 1$ per a $\ell \in S$. Però, com que S està inclòs en el complementari de T, és $w_{i,\ell} = 1$, per a tot i i tot $\ell \in S$.

Podem suposar, doncs, que $\ell \notin S$. Aleshores, $\ell \neq 2$ i, per a tot índex i, ℓ no divideix a_i. En conseqüència, a_i és una unitat en $\mathbb{Z}_\ell$ i el càlcul del símbol de Hilbert ens permet assegurar que, per a tot element no nul $b \in \mathbb{Q}_\ell$, és $(a_i, b)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(b)}$. Si $\ell \notin T \cup \{p\}$, aleshores $w_{i,\ell} = 1$ i ℓ no divideix x, de manera que $(a_i, x)_\ell = 1$, ja que x també és una unitat en $\mathbb{Z}_\ell$. Si $\ell \in T$, aleshores $v_\ell(x) = 1$. Però, en virtut de la hipòtesi (c), existeix un element $x_\ell \in {\mathbb{Q}_\ell}^*$ tal que per a tot índex i és $(a_i, x_\ell)_\ell = w_{i,\ell}$; per tant, i com que algun dels valors $w_{i,\ell}$ és -1, ha de ser $v_\ell(x_\ell)$ és senar. En conseqüència, obtenim la igualtat $(a_i, x)_\ell = \left(\frac{a_i}{\ell}\right) = (a_i, x_\ell)_\ell = w_{i,\ell}$. Per últim, si $\ell = p$ la fórmula del producte i la propietat (b) permeten concloure.

En el cas general, $S \cap T$ pot ser no buit. Es tracta de reduir el problema al cas anterior. Podem considerar els elements x_ℓ donats per la condició (c).

Per a tot nombre primer ℓ, ${\mathbb{Q}_\ell}^{*2}$ és un subgrup obert de ${\mathbb{Q}_\ell}^*$, ja que és d'índex finit. Així, $x_\ell {\mathbb{Q}_\ell}^{*2}$ és un subconjunt obert de ${\mathbb{Q}_\ell}^*$; per tant, el conjunt $\prod_{\ell \in S} x_\ell {\mathbb{Q}_\ell}^{*2}$ és obert en $\prod_{\ell \in S} {\mathbb{Q}_\ell}^*$. El lema d'aproximació ens permet assegurar que existeix $x' \in \mathbb{Q}^* \cap \prod_{\ell \in S} x_\ell {\mathbb{Q}_\ell}^{*2}$; és a dir, per a tot nombre primer $\ell \in S$ és $\dfrac{x'}{x_\ell} \in {\mathbb{Q}_\ell}^{*2}$. Dit d'una altra manera, per a tota parella (i, ℓ) tal que $\ell \in S$ se satisfà la igualtat $(a_i, x')_\ell = (a_i, x_\ell)_\ell = w_{i,\ell}$.

Posem, per a tota parella (i, ℓ), $w'_{i,\ell} := w_{i,\ell}(a_i, x')_\ell$. Aleshores, la família formada pels elements $w'_{i,\ell}$ satisfà les condicions de l'enunciat i, a més a més, és $w'_{i,\ell} = 1$ per a tot $\ell \in S$. Els conjunts S' i T' construïts per als $w'_{i,\ell}$ són disjunts, de manera que podem aplicar el cas anterior; obtenim un element $y \in \mathbb{Q}^*$ tal que per a tota parella (i, ℓ) se satisfà que $(a_i, y)_\ell = w'_{i,\ell}$. Posem $x := yx'$. Aleshores, per a tota parella (i, ℓ) se satisfà que $(a_i, x)_\ell = (a_i, y)_\ell (a_i, x')_\ell = w_{i,\ell}$, com volíem veure. □

11.3 El teorema de Hasse-Minkowski

El teorema de Hasse-Minkowski és l'ingredient essencial de la classificació que fem de les formes quadràtiques no singulars sobre el cos dels nombres racionals.

Teorema 11.3.1 (Hasse-Minkowski)**.** *Sigui q una forma quadràtica racional no singular. Condició necessària i suficient perquè q representi 0 es $\mathbb{Q}$ és que q representi 0 en $\mathbb{R}$ i en $\mathbb{Q}_p$ per a tot nombre primer p.*

Demostració: Clarament, i com que $\mathbb{Q} \subseteq \mathbb{R}$ i $\mathbb{Q} \subseteq \mathbb{Q}_p$ per a tot nombre primer p, la condició és necessària. Es tracta de provar-ne la suficiència.

Considerem una diagonalització de la forma quadràtica q; és a dir, considerem nombres racionals no nuls $a_1, a_2, \ldots, a_n \in \mathbb{Q}$ de manera que $q = \langle a_1, a_2, \ldots, a_n \rangle$. A fi de caracteritzar quan aquesta forma representa zero, podem suposar sense pèrdua de generalitat que $a_1 = 1$. Farem la prova distingint casos segons el rang, n. El cas de rang 1 és trivial, ja que la forma X^2 no representa 0 sobre cap cos.

Cas $n = 2$. Podem escriure la forma de la manera $q := X^2 - aY^2$ per a un cert nombre racional no nul a; com que q representa 0 en $\mathbb{R}$, cal que sigui $a > 0$; podem considerar una factorització de a, $a = \prod_p p^{v_p(a)}$, amb $v_p(a) \in \mathbb{Z}$; com que q representa 0 en $\mathbb{Q}_p$, obtenim que a és un quadrat en cada $\mathbb{Q}_p$, de manera que, per a tot nombre primer p, $v_p(a)$ és parell. En particular, a és un quadrat en $\mathbb{Q}$ i, en conseqüència, q representa a en $\mathbb{Q}$.

Cas $n = 3$. Si cal, podem multiplicar els coeficients per quadrats de $\mathbb{Q}^*$, i fer la forma equivalent a una forma quadràtica $q = \langle 1, -a, -b \rangle$, amb $a, b \in \mathbb{Z}$, no nuls i lliures de quadrats; i podem suposar que $|a| \leq |b|$. Sigui $m := |a| + |b|$; es tracta de fer la demostració per inducció sobre el nombre natural m. Si $m = 2$, aleshores la forma és una de les $q = \langle 1, \pm 1, \pm 1 \rangle$, la forma $\langle 1, 1, 1 \rangle$ exclosa perquè q representa zero en $\mathbb{R}$; i, de manera trivial, i les altres tres representen zero en $\mathbb{Q}$. Suposem, doncs, que $m > 2$; en aquest cas és $|b| \geq 2$ i podem considerar una factorització $b = \pm p_1 \cdot \cdots \cdot p_k$ de b amb els p_i nombres naturals primers diferents. Es tracta de veure que a és un residu quadràtic mòdul p_i per a tot índex $1 \leq i \leq k$. Ens fixarem en un índex i i escriurem $p := p_i$. Si p divideix a, aleshores és clar que a és un residu quadràtic mòdul p; en cas contrari, a és un element invertible de $\mathbb{Z}_p$. Per hipòtesi, la forma quadràtica $\langle 1, -a, -b \rangle$ representa 0 en $\mathbb{Q}_p$, de manera que existeixen elements $x, y, z \in \mathbb{Z}_p$, no tots ells divisibles per p, de manera que $0 = z^2 - ax^2 - by^2$. Com que p divideix b, podem escriure $z^2 \equiv ax^2 \pmod{p}$; si p dividís x, aleshores p també dividiria y i això és contrari a l'elecció que hem fet de x, y, z; per tant, podem suposar que p no divideix a. Però, en aquest cas, a és un residu quadràtic mòdul p, com volíem veure.

Ara aplicarem aquest resultat parcial. El fet que a sigui un residu quadràtic mòdul p per a tot nombre enter primer p que divideix l'enter lliure de quadrats b, ens permet assegurar que a és un residu quadràtic mòdul b. Això ens permet establir l'existència de nombres enters $t, b' \in \mathbb{Z}$ tals que $t^2 = a + bb'$ i podem suposar que $|t| \leq \dfrac{|b|}{2}$, si prenem un sistema adequat de representants de les classes laterals mòdul b. Ara, la propietat $bb' = t^2 - a = \mathrm{N}(t + \sqrt{a})$ ens permet dir que una condició necessària i suficient perquè $b \in \mathrm{N}(K(\sqrt{a})|K)$ és que $b' \in \mathrm{N}(K(\sqrt{a})|K)$, on $K = \mathbb{Q}_p$ o bé $K = \mathbb{Q}$. En conseqüència, la forma quadràtica q de partida representa 0 en K si, i només si, la forma quadràtica $q' := \langle 1, -a, -b' \rangle$ representa 0 en K (cf. el teorema de Legendre **8.2.1** i el lema **8.2.3**). Per tant, podem suposar que, per a tot nombre primer p, la forma quadràtica $\langle 1, -a, -b' \rangle$ representa 0 en $\mathbb{Q}_p$. Ara bé, com que $|b| \geq 2$, podem escriure que

$$|b'| = \left| \frac{t^2 - a}{b} \right| \leq \frac{|b|}{4} + 1 < |b|.$$

Posem $b' =: b''u^2$ amb $b'', u \in \mathbb{Z}$, b'' lliure de quadrats; se satisfà, doncs, la desigualtat $|b''| < |b|$. D'altra banda, i per construcció, la forma quadràtica racional $q'' := \langle 1, -a, -b'' \rangle$ és equivalent a la forma q' i, per hipòtesi d'inducció, ja que $|a| + |b''| < |a| + |b|$, q'' representa 0 en $\mathbb{Q}$. Per tant, la forma quadràtica q' representa 0 en $\mathbb{Q}$ i, en conseqüència, la forma quadràtica q representa 0 en $\mathbb{Q}$.

Cas $n = 4$. Podem escriure $q = \langle a, b, -c, -d\rangle$ amb $a, b, c, d \in \mathbb{Z}$ no nuls. Donat un índex $p \in P \cup \{\infty\}$, com que q representa 0 en $\mathbb{Q}_p$, per hipòtesi, podem trobar un element $x_p \in \mathbb{Q}_p$ ($x_\infty \in \mathbb{R}$ si $p = \infty$) tal que les formes quadràtiques $\langle a, b\rangle$ i $\langle c, d\rangle$ representen x_p. Però això ens assegura que se satisfan les igualtats $(x_p, -ab)_p = (a, b)_p$ i $(x_p, -cd)_p = (c, d)_p$ entre els símbols de Hilbert. La fórmula del producte ens permet escriure les igualtats

$$\prod_{p\in P\cup\{\infty\}} (a, b)_p = \prod_{p\in P\cup\{\infty\}} (c, d)_p = 1,$$

de manera que podem aplicar l'existència de nombres racionals amb símbols de Hilbert donats (cf. la proposició **11.2.3**) de la manera següent: posem $a_1 := -ab$, $a_2 := -cd$; aleshores, existeix un nombre racional x tal que per a tot $p \in P \cup \{\infty\}$ se satisfan les igualtats $(a_1, x)_p = (a, b)_p$, $(a_2, x)_p = (c, d)_p$.

Considerem la forma quadràtica $q_x := \langle a, b, -x\rangle$. Per construcció, i en tenir en compte les condicions perquè la forma de rang 2 $\langle a, b\rangle$ representi x sobre $\mathbb{Q}_p$, la forma quadràtica q_x representa 0 en $\mathbb{Q}_p$ per a tot $p \in P \cup \{\infty\}$; com que és de rang 3 i, en aquest cas, ja hem demostrat el teorema, podem assegurar que la forma quadràtica q_x representa 0 en $\mathbb{Q}$. Anàlogament, la forma quadràtica $\langle c, d, -x\rangle$ representa 0 en $\mathbb{Q}$. Però això ens diu que les formes quadràtiques $\langle a, b\rangle$ i $\langle c, d\rangle$ representen x en $\mathbb{Q}$, de manera que q representa 0 en $\mathbb{Q}$.

Cas $n \geq 5$. Farem la demostració per inducció sobre n. Per a això considerarem una descomposició de q com a suma ortogonal de dues formes $q_1 := \langle a_1, a_2\rangle$ i $q_2 := \langle a_3, \ldots, a_n\rangle$ i el conjunt finit $S := \{2, \infty\} \cup \{p \in P : v_p(a_i) > 0,$ per a algun índex $i \geq 3\}$. Per hipòtesi, per a tot $p \in P \cup \{\infty\}$ existeix $a_p \in \mathbb{Q}_p$ tal que q_1 i $-q_2$ representen a_p. A més a més, podem suposar que $a_p \in {\mathbb{Q}_p}^*$, ja que si una forma quadràtica representa 0 en $\mathbb{Q}_p$, aleshores representa tot element de $\mathbb{Q}_p$.

Donat $p \in S$, el subgrup ${\mathbb{Q}_p}^{*2}$ de ${\mathbb{Q}_p}^*$ és un subgrup d'índex finit; per tant, és un subgrup obert; en conseqüència, el conjunt $a_p{\mathbb{Q}_p}^{*2}$ és un obert de ${\mathbb{Q}_p}^*$ i, com que ${\mathbb{Q}_p}^*$ és un subconjunt obert de $\mathbb{Q}_p$, obtenim que $a_p{\mathbb{Q}_p}^{*2}$ és un subconjunt obert de $\mathbb{Q}_p$. D'aquesta manera, $\prod_{p\in S} a_p{\mathbb{Q}_p}^{*2}$ és un subconjunt obert de $\prod_{p\in S} \mathbb{Q}_p$. D'altra banda, l'aplicació

$$\prod_{p\in S} \mathbb{Q}_p \times \prod_{p\in S} \mathbb{Q}_p \longrightarrow \prod_{p\in S} \mathbb{Q}_p$$

donada per la fórmula

$$(\{y_{p,1}\}_p, \{y_{p,2}\}_p) \mapsto \{q_1(y_{p,1}, y_{p,2})\}_p$$

és contínua; per tant, l'antiimatge de l'obert $\prod_{p\in S} a_p{\mathbb{Q}_p}^{*2}$ en $\prod_{p\in S} \mathbb{Q}_p \times \prod_{p\in S} \mathbb{Q}_p$ és un obert.

Ara, el lema d'aproximació (cf. **11.2.1**) ens permet assegurar que tot subconjunt obert de $\prod_{p\in S} \mathbb{Q}_p \times \prod_{p\in S} \mathbb{Q}_p$ talla $\mathbb{Q} \times \mathbb{Q}$; per tant, existeixen nombres racionals x_1, x_2 tals que per a tot $p \in S$ és $q_1(x_1, x_2) \in a_p{\mathbb{Q}_p}^{*2}$. En conseqüència, si $a := q_1(x_1, x_2)$, aleshores $a \in \mathbb{Q}$ i per a tot $p \in S$ és $aa_p^{-1} \in {\mathbb{Q}_p}^{*2}$.

Considerem, ara, la forma quadràtica f, suma ortogonal de les formes quadràtiques $\langle a\rangle$ i q_2. Si $p \in S$, com que $-q_2$ representa a_p i $a \in a_p{\mathbb{Q}_p}^{*2}$, també $-q_2$ representa a; per tant, f representa 0 en $\mathbb{Q}_p$ per a tot $p \in S$. D'altra banda, si $p \notin S$, aleshores

els coeficients $-a_3, \ldots, -a_n$ de $-q_2$ són invertibles en $\mathbb{Z}_p$, de manera que els símbols de Hilbert $(-a_i, -a_j)_p$ són trivials si $3 \leq i < j \leq n$ i, en conseqüència, per a $p \notin S$ és $w_p(-q_2) = 1$, ja que $2 \in S$. A més a més, el discriminant també és invertible en $\mathbb{Z}_p$, de manera que $(-1, \Delta(-q_2))_p = 1$; podem aplicar les condicions d'isotropia d'una forma de rang ≥ 3 i obtenim que, per a tot $p \notin S$, $-q_2$ representa 0 en $\mathbb{Q}_p$ i, per tant, f també representa 0 en $\mathbb{Q}_p$. Per hipòtesi d'inducció, podem assegurar que f representa 0 en $\mathbb{Q}$. Però això ens permet assegurar que la forma quadràtica q_2 representa a en $\mathbb{Q}$; i com que q_1 representa a en $\mathbb{Q}$, la forma q representa 0 en $\mathbb{Q}$, com volíem demostrar. □

Corol·lari 11.3.2. *Siguin q una forma quadràtica no degenerada sobre $\mathbb{Q}$ i $\alpha \in \mathbb{Q}$ un nombre racional qualsevol. Condició necessària i suficient perquè q representi α en $\mathbb{Q}$ és que q representi α sobre $\mathbb{R}$ i sobre $\mathbb{Q}_p$ per a tot nombre primer p.*

Demostració: En efecte, considerem la forma quadràtica $q' := q \perp \langle -\alpha \rangle$ i apliquem el teorema tenint en compte que una condició necessària i suficient perquè q representi α sobre un cos K que conté $\mathbb{Q}$ és que q' representi 0 sobre K. □

Corol·lari 11.3.3. *Sigui q una forma quadràtica racional, no degenerada, de rang $n \geq 5$ i indefinida sobre $\mathbb{R}$ (és a dir, de signatura $(r, s) \neq (n, 0)$ i $(r, s) \neq (0, n)$). Aleshores, q representa 0 en $\mathbb{Q}$.* □

Observació 11.3.4. El teorema de Hasse-Minkowski dóna una altra interpretació del teorema de Legendre.

Si p és un nombre primer i $m \geq 1$ un enter qualsevol, direm que una forma quadràtica $aX^2 + bY^2 + cZ^2$ de coeficients enters a, b, c, representa zero primitivament en $\mathbb{Z}/p^m\mathbb{Z}$, quan existeixen enters x, y, z no tots múltiples de p tals que $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p^m}$. Amb aquesta noció, la condició que dóna el teorema de Legendre admet algunes formes equivalents.

Corol·lari 11.3.5. *Siguin $a, b, c \in \mathbb{Z}$ enters no nuls, lliures de quadrats, primers dos a dos, i no tots del mateix signe. Aleshores, les condicions següents són equivalents.*

(a) *L'equació $aX^2 + bY^2 + cZ^2 = 0$ admet solucions enteres no trivials.*

(b) *Per a tot nombre primer p i tot enter $m \geq 1$, l'equació $aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{p^m}$ admet solucions primitives.*

(c) *Per a tot nombre primer p que divideix abc, l'equació $aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{p^2}$ admet solucions primitives.*

(d) *Per a tot nombre primer p, la forma quadràtica $aX^2 + bY^2 + cZ^2$ representa 0 primitivament en $\mathbb{Z}_p$.*

(e) *Per a tot nombre primer p, la forma quadràtica $aX^2 + bY^2 + cZ^2$ representa 0 en $\mathbb{Q}_p$.*

Demostració: Les implicacions de (b) per (a) i de (c) per (b) són immediates. Veiem que (c) implica (a). Sigui p un nombre primer i suposem que p divideix a i que (x, y, z) és una solució primitiva mòdul p^2. Veiem que p no divideix el producte yz. Si p dividís y, aleshores p dividiria $ax^2 + by^2$, de manera que p també dividiria cz^2. Però com que a, c són primers entre si, p dividiria z; per tant, p^2 dividiria $by^2 + cz^2$, d'on p^2 dividiria ax^2; com que a és lliure de quadrats, p també dividiria x i (x, y, z) no seria una solució

primitiva de l'equació mòdul p^2. Per tant, p no divideix y i, per simetria, p tampoc no divideix z.

De la igualtat $by^2+cz^2\equiv 0 \pmod p$ obtenim que $-bcy^2\equiv (cz)^2 \pmod p$ i, com que p no divideix y, obtenim que $-bc$ és un residu quadràtic mòdul p. Com que això se satisfà per a tot nombre primer p que divideix a i a és lliure de quadrats, $-bc$ és un residu quadràtic mòdul a.

Anàlogament, $-ca$ és un residu quadràtic mòdul b i $-ab$ és un residu quadràtic mòdul c; el teorema de Legendre ens permet concloure.

Per últim, l'equivalència de (b) i (d) és la definició de $\mathbb{Z}_p$ i la de (d) i (e) és immediata si "treiem denominadors". □

Això és un cas particular de l'anomenat principi de Hasse: una forma quadràtica racional q, indefinida com a forma real, representa zero en $\mathbb{Q}$ si, i només si, representa zero primitivament en tots els anells $\mathbb{Z}/p^m\mathbb{Z}$, on p és un primer i $m\geq 1$ un enter qualsevol.

Dit d'una altra manera, una hiperquàdrica projectiva, (absolutament) irreductible, definida sobre $\mathbb{Q}$ té punts racionals si, i només si, té punts reals i a cada un dels anells $\mathbb{Z}/p^m\mathbb{Z}$, per a tot nombre primer p i tot enter $m\geq 1$.

11.4 Classificació de les formes quadràtiques racionals

El teorema de Hasse-Minkowski permet acabar de manera senzilla la classificació de les formes quadràtiques no degenerades sobre el cos dels nombres racionals.

Teorema 11.4.1 (Classificació de formes quadràtiques sobre $\mathbb{Q}$)**.** *Siguin q, q' formes quadràtiques racionals no degenerades. Les condicions següents són equivalents:*

(a) *q és racionalment equivalent a q';*

(b) *per a tot $p\in P\cup\{\infty\}$ q és $\mathbb{Q}_p$-equivalent a q';*

(c) *se satisfan les igualtats:*

$$\begin{cases}(r,s)=(r',s')\in\mathbb{Z}\times\mathbb{Z},\\ \Delta(q)=\Delta(q')\in\mathbb{Q}^*/\mathbb{Q}^{*2},\\ w_p(q)=w_p(q'), & \text{per a tot } p\in P\cup\{\infty\},\end{cases}$$

on $(r,s),(r',s')$ denoten la signatura de q i la de q' com a formes quadràtiques reals, respectivament.

Demostració: Clarament, (a) implica (b) i, en virtut del teorema de classificació de formes quadràtiques sobre $\mathbb{Q}_p$ (cf. el teorema **10.9.1**), (b) i (c) són equivalents. Només resta veure que (b) implica (a). Per a això, observem que de (b) es dedueix immediatament que totes dues formes són del mateix rang i tenen el mateix discriminant no nul mòdul quadrats. Ara, la demostració s'acaba per inducció sobre el rang, tenint en compte el teorema de simplificació de Witt. Concretament, si les formes són de rang 1, el sol fet

que els seus discriminants siguin iguals fa que totes dues formes siguin $\mathbb{Q}$-equivalents. Suposem, doncs, que $n := \operatorname{rang}(q) > 1$. Sigui $a \in \mathbb{Q}^*$ un nombre racional no nul representat racionalment per la forma q. Aleshores, q representa a sobre $\mathbb{Q}_p$ per a tot $p \in P \cup \{\infty\}$ i, per tant, q' també representa a sobre $\mathbb{Q}_p$ per a tot $p \in P \cup \{\infty\}$. En virtut del corol·lari anterior, q' representa a sobre $\mathbb{Q}$. Això ens permet escriure $q = \langle a \rangle \perp q_1$ i $q' = \langle a \rangle \perp q'_1$ per a certes formes quadràtiques racionals q_1, q'_1, de rang $n-1$. Podem fer el càlcul dels invariants d'aquestes dues formes quadràtiques: el discriminant, mòdul quadrats, és $\Delta(q_1) = a\Delta(q) = a\Delta(q') = \Delta(q'_1)$; la signatura de q_1 i la de q'_1 coincideixen, ja que a és el mateix per a les dues formes; i, per a tot $p \in P \cup \{\infty\}$, és $w_p(q_1) = w_p(q'_1)$, ja que podem escriure $(a, \Delta(q_1))_p w_p(q_1) = w_p(q) = w_p(q') = (a, \Delta(q'_1)) w_p(q'_1) = (a, \Delta(q_1)) w_p(q'_1)$. És a dir, les formes quadràtiques q_1 i q'_1 són $\mathbb{Q}_p$-equivalents per a tot $p \in P \cup \{\infty\}$. Per hipòtesi d'inducció, q_1 és $\mathbb{Q}$-equivalent a q'_1, de manera que q és $\mathbb{Q}$-equivalent a q', com calia veure. □

No es pot considerar acabada la classificació de les formes quadràtiques sense una descripció de les classes d'equivalència. L'objectiu de la proposició següent és determinar les condicions que han de satisfer els invariants perquè existeixi una forma quadràtica racional amb aquests invariants.

Proposició 11.4.2. *Siguin $\Delta \in \mathbb{Q}^*$, $r, s \in \mathbb{Z}$, $r, s \geq 0$, i, per a tot $p \in P \cup \{\infty\}$, $w_p \in \{\pm 1\}$. Perquè existeixi una forma quadràtica racional q amb invariants $\Delta(q) = \Delta$, signatura (r, s) (que, en particular, determina el rang $n = r + s$), i invariants de Hasse-Witt $w_p(q) = w_p$, per a tot $p \in P \cup \{\infty\}$, és condició necessària i suficient que per als nombres Δ, r, s i w_p se satisfacin les propietats següents:*

(a) *per a tot $p \in P \cup \{\infty\}$ llevat, potser, d'un subconjunt finit, és $w_p = 1$ i, a més a més, $\prod_{p \in P \cup \{\infty\}} w_p = 1$;*

(b) *si $r + s = 1$, aleshores $w_p = 1$ per a tot p;*

(c) *per a tot $p \in P \cup \{\infty\}$, si $r + s = 2$ i $\Delta = -1 \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$, aleshores $w_p = 1$;*

(d) *$(-1)^s \Delta > 0$;*

(e) *$w_\infty = (-1)^{s(s-1)/2}$.*

Demostració: La necessitat de les condicions és immediata, si tenim en compte que una tal forma quadràtica racional és, automàticament, una forma quadràtica sobre $\mathbb{Q}_p$, per a tot $p \in P \cup \{\infty\}$, que té els invariants predits. Cal veure'n la suficiència. Ho farem per inducció sobre $n := r + s$, essent immediat el cas de rang $n = 1$.

Suposem que $n = 2$. Com que el símbol de Hilbert és no degenerat, la condició (c) ens permet elegir, per a cada $p \in P \cup \{\infty\}$, un element $x_p \in {\mathbb{Q}_p}^*$ tal que $(x_p, -\Delta)_p = w_p$. Tenint en compte la condició (a), el teorema d'existència de nombres racionals amb símbols de Hilbert donats (cf. la proposició **11.2.3**) ens permet assegurar que existeix un nombre racional no nul $x \in \mathbb{Q}^*$ tal que per a tot $p \in P \cup \{\infty\}$ és $(x, -\Delta)_p = w_p$. Considerem la forma quadràtica $q := \langle x, x\Delta \rangle$; és immediat comprovar que la forma racional q té els invariants demanats.

Considerem, ara, el cas $n = 3$. El conjunt $S := \{p \in P \cup \{\infty\} : (-1, -\Delta)_p = -w_p\}$ és finit, ja que el símbol de Hilbert $(-1, -\Delta)_p$ és trivial per a gairebé tot p i, en canvi,

$w_p = 1$ per a gairebé tot p. Per a qualsevol $p \in S$, podem elegir $c_p \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$ tal que $c_p \neq -\Delta \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$; en virtut del lema d'aproximació, existeix $c \in \mathbb{Q}^*$ tal que per a tot $p \in S$ és $c = c_p \in {\mathbb{Q}_p}^*/{\mathbb{Q}_p}^{*2}$. Podem elegir, doncs, una forma quadràtica racional de rang 2, q_1, de manera que $\Delta(q_1) = c\Delta$ i, per a tot $p \in P \cup \{\infty\}$, sigui $w_p(q_1) = (c, -\Delta)_p w_p$, ja que se satisfan les condicions de l'enunciat i el cas de rang 2 ja s'ha provat. Posem $q := \langle c \rangle \perp q_1$; és immediat comprovar que q és una forma quadràtica que té els invariants predits en l'enunciat.

Cas $n \geq 4$. Suposem que $r \geq 1$. Per hipòtesi d'inducció, existeix una forma quadràtica racional q_1 de rang $n-1$, discriminant Δ, invariants de Hasse-Witt w_p i signatura $(r-1, s)$. Aleshores, la forma $q := \langle 1 \rangle \perp q_1$ satisfà les condicions exigides.

En el cas contrari, és $r = 0$ i $n = s$. Però, per hipòtesi d'inducció, podem elegir una forma quadràtica radional, q_1, de rang $n-1$, signatura $(0, s-1)$, discriminant $-\Delta$, i invariants de Hasse-Witt $w_p(q_1) = (-1, -\Delta)_p w_p$; si posem $q := q_1 \perp \langle -1 \rangle$, la forma q satisfà les condicions exigides. $\square$

Capítol 12

Sèries de Dirichlet

En aquest capítol s'inicia, pròpiament, la part de mètodes analítics del curs. Comença amb la descripció d'algunes funcions aritmètiques i de la seva relació amb les sèries de Dirichlet, per a passar de seguida a fer l'estudi d'aquestes sèries i de les funcions que defineixen.

12.1 La fórmula d'inversió de Möbius

Una funció aritmètica és, per definició, una successió; és a dir, una aplicació definida en el conjunt dels nombres enters positius. El canvi de nom, però, respon al fet que no es tracta d'estudiar-ne la convergència, com és habitual, sinó d'estudiar altres propietats més aritmètiques.

Definició 12.1.1. Siguin A un anell i $f : \mathbb{N} \longrightarrow A$ una funció aritmètica. Direm que f és multiplicativa quan per a tota parella de nombres naturals no nuls m, n, primers entre si, sigui $f(mn) = f(m)f(n)$. Direm que és completament multiplicativa quan la propietat $f(mn) = f(m)f(n)$ se satisfaci per a tota parella m, n sense restricció.

El conjunt de totes les funcions aritmètiques en un anell A es pot dotar d'una estructura d'anell diferent de l'estructura estàndard, en què la suma i el producte de funcions són definits per les fórmules $(f + g)(n) := f(n) + g(n)$ i $(f \cdot g)(n) := f(n) \cdot g(n)$, per a $n \in \mathbb{N}$.

Definició 12.1.2. Siguin f, g dues funcions aritmètiques en un anell A. Definim el producte de Dirichlet, també anomenat convolució de Dirichlet, de les funcions f, g com la funció aritmètica definida per la fórmula

$$(f * g)(n) := \sum_{d|n} f(d)g(n/d).$$

Proposició 12.1.3. *El conjunt de totes les funcions aritmètiques en A amb la suma habitual i el producte de Dirichlet és un anell commutatiu i unitari. L'element unitat és la funció aritmètica u definida per*

$$u(n) := \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n \neq 1. \end{cases} \square$$

Més interessant és la propietat següent.

Proposició 12.1.4. *Si f, g són funcions aritmètiques multiplicatives, aleshores $f*g$ també és una funció aritmètica multiplicativa.*

Demostració: En efecte, si m, n són primers entre si, tot divisor del producte nm s'escriu de manera única en la forma dd' per a un divisor d de n i un divisor d' de m que, en conseqüència, són primers entre si; per tant, podem escriure

$$\begin{aligned}(f*g)(nm) &= \sum_{d|n}\sum_{d'|m} f(dd')g(nm/dd') \\ &= \sum_{d|n}\sum_{d'|m} f(d)g(n/d)f(d')g(m/d') \\ &= (f*g)(n)(f*g)(m),\end{aligned}$$

ja que n/d i m/d' també són primers entre si. □

Entre els exemples més importants de funcions aritmètiques multiplicatives hi ha la funció μ de Möbius, que es defineix de la manera següent:

$$\mu(n) := \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n \text{ és divisible pel quadrat d'algun nombre primer,} \\ (-1)^k, & \text{si } n \text{ és el producte de } k \text{ nombres primers diferents.} \end{cases}$$

La seva importància rau en les dues propietats següents.

Proposició 12.1.5. *La funció μ de Möbius és una funció aritmètica multiplicativa, invertible per al producte de Dirichlet.*

Demostració: En efecte; la multiplicativitat de la funció és una comprovació trivial a partir de la definició. D'altra banda, considerem la funció constant de valor 1, posem $U(n) := 1$. Es tracta de veure que U és la inversa de μ. Com que, trivialment, $(\mu*U)(1) = 1$, això és veure que, si $n > 1$, aleshores $\sum_{d|n} \mu(d) = 0$. Com que la funció μ és multiplicativa —i la funció constant de valor 1 també—, podem suposar que $n = p^r$ és potència d'un nombre primer p; en aquest cas, i tenint en compte que si $p^2|d$, aleshores $\mu(d) = 0$, la suma $\sum_{d|p^r} \mu(d)$ es converteix en $\mu(1) + \mu(p) = 1 + (-1) = 0$, com calia demostrar. □

Proposició 12.1.6 (Fórmula d'inversió de Möbius)**.** *Siguin f, g funcions aritmètiques qualssevol. Aleshores, les propietats següents són equivalents:*

(a) *per a tot n,* $g(n) := \sum_{d|n} f(d)$;

(b) *per a tot n,* $f(n) := \sum_{d|n} g(d)\mu(n/d)$.

Demostració: Les igualtats anteriors expressen, respectivament, les igualtats $g = f*U$ i $f = g*\mu$; i com que μ és invertible amb inversa U, la propietat és immediata. □

Com a aplicació elemental d'aquest resultat, es proposa com a exercici la determinació del nombre de polinomis irreductibles sobre els cossos finits. Concretament, es demana provar que, si $\psi_q(n)$ és el nombre de polinomis mònics irreductibles de grau n sobre el cos $\mathbb{F}_q$, aleshores se satisfà la igualtat

$$n\psi_q(n) = \sum_{d|n} \mu(d) q^{n/d}.$$

Altres exemples interessants de funcions aritmètiques multiplicatives i la seva relació amb la funció de Möbius se solen proposar com a exercicis.

12.2 Sèries de Dirichlet

En aquesta secció es tracta d'introduir unes eines que seran bàsiques per a la resta del curs i d'estudiar les seves propietats generals: les sèries de Dirichlet.

Definició 12.2.1. Una sèrie de Dirichlet (complexa) és una sèrie funcional, en la variable complexa s, de la forma

$$\sum_{n\geq 1} f(n) n^{-s},$$

on f és una funció aritmètica complexa.

Proposició 12.2.2. *Sigui $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ una sèrie de Dirichlet. Suposem que per a un cert valor complex de s, la sèrie $F(s)$ és absolutament convergent. Aleshores, existeix $\sigma \in \mathbb{R}$ i per a tot nombre complex s' tal que $\Re(s') > \sigma$ la sèrie $F(s')$ és absolutament convergent; és a dir, $\sum_{n\geq 1} |f(n)n^{-s'}|$ és convergent.*

Demostració: En efecte, si $s, s' \in \mathbb{C}$ són tals que $\Re(s') > \Re(s)$, aleshores se satisfà la desigualtat $|f(n)n^{-s'}| = |f(n)|n^{-\Re(s')} \leq |f(n)|n^{-\Re(s)} = |f(n)n^{-s}|$; per tant, podem aplicar el criteri de comparació per a la convergència de sèries de nombres reals positius i obtenim que si $F(s)$ és absolutament convergent i $\Re(s') > \Re(s)$, aleshores $F(s')$ és absolutament convergent. El valor de σ que cerquem es pot prendre $\sigma := \Re(s)$. □

Corol·lari 12.2.3. *Sigui $F(s)$, com abans, una sèrie de Dirichlet. Suposem que $F(s)$ no és absolutament convergent en tot $\mathbb{C}$ ni divergent en tot $\mathbb{C}$. Aleshores, existeix un nombre real σ_a tal que per a tot nombre complex s de part real $\Re(s) > \sigma_a$ la sèrie $F(s)$ és absolutament convergent i per a tot nombre complex s de part real $\Re(s) < \sigma_a$ la sèrie $F(s)$ no és absolutament convergent.*

Demostració: Per hipòtesi, el conjunt de nombres reals r tals que existeix un nombre complex s de part real r tal que la sèrie $F(s)$ és absolutament convergent és no buit; d'altra banda, la proposició anterior ens permet assegurar que aquest conjunt és fitat inferiorment, ja que, en cas contrari, la sèrie $F(s)$ seria absolutament convergent en tot $\mathbb{C}$. El nombre real σ_a que cerquem és l'ínfim d'aquest conjunt. □

Dit d'una altra manera, tota sèrie de Dirichlet (complexa) que sigui absolutament convergent en algun punt admet un semiplà de convergència absoluta.

Definició 12.2.4. El nombre σ_a del corol·lari anterior s'anomena l'abscissa de convergència absoluta de la sèrie de Dirichlet $F(s)$. En el cas que la sèrie sigui absolutament convergent en tot $\mathbb{C}$, es posa $\sigma_a = -\infty$, i en el cas que la sèrie no sigui absolutament convergent per a cap nombre complex s, es posa $\sigma_a := +\infty$.

Exemple 12.2.5. L'exemple clàssic més important de sèrie de Dirichlet el proporciona la sèrie de Riemann

$$\zeta(s) := \sum_{n\geq 1} n^{-s}.$$

És un resultat dels cursos elementals de càlcul que la sèrie $\zeta(s)$ és absolutament convergent per a tot nombre real $s > 1$, mentre que és divergent per a $s = 1$. Per tant, l'abscissa de convergència absoluta de $\zeta(s)$ és $\sigma_a = 1$.

Definició 12.2.6. S'anomena funció zeta de Riemann la funció definida en el semiplà $\Re(s) > 1$ per la fórmula $\zeta(s) := \sum_{n\geq 1} n^{-s}$.

Exemple 12.2.7. Altres exemples importants de sèries de Dirichlet els proporcionen els caràcters de Dirichlet. En efecte, suposem que χ és un caràcter qualsevol de Dirichlet i posem $L(\chi, s) := \sum_{n\geq 1} \chi(n)n^{-s}$. Com que la funció aritmètica χ és una funció fitada —els seus valors no nuls són arrels de la unitat—, podem comparar amb la sèrie de Riemann: $|\chi(n)n^{-s}| \leq |n^{-s}|$, de manera que si $\Re(s) > 1$, aleshores $L(\chi, s)$ és absolutament convergent; per tant, l'abscissa de convergència absoluta de les sèries $L(\chi, s)$ és ≤ 1.

De fet, aquest càlcul demostra que si f és una funció aritmètica complexa fitada, aleshores l'abscissa de convergència absoluta de la sèrie $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ és ≤ 1.

Definició 12.2.8. Les funcions $L(\chi, s)$ definides per les igualtats $L(\chi, s) := \sum_{n\geq 1} \chi(n)n^{-s}$ en el semiplà de convergència absoluta s'anomenen les funcions L associades als caràcters de Dirichlet.

Observem que, en particular, la funció zeta de Riemann és la funció L associada al caràcter trivial de Dirichlet.

Ens podem preguntar per la unicitat del desenvolupament en sèrie de Dirichlet de les funcions que admeten aquest desenvolupament. El resultat següent respon a la pregunta.

Proposició 12.2.9. *Siguin $f(n)$ i $g(n)$ funcions aritmètiques tals que les sèries de Dirichlet*

$$F(s) := \sum_{n\geq 1} f(n)n^{-s}, \qquad G(s) := \sum_{n\geq 1} g(n)n^{-s}$$

són absolutament convergents en algun punt $s \in \mathbb{C}$, i suposem que $\{s_k\}_{k\geq 1}$ és una successió de nombres complexos tal que $\Re(s_k) > \sigma_a$, on σ_a és el màxim de les abscisses de convergència absoluta de les dues sèries; $\lim \Re(s_k) = +\infty$; i $F(s_k) = G(s_k)$, per a tot $k \geq 1$. Aleshores, per a tot $n \geq 1$, és $f(n) = g(n)$.

Demostració: Per a tot $n \geq 1$, posem $h(n) := f(n) - g(n)$ i per a tot $s \in \mathbb{C}$, sigui $H(s) := F(s) - G(s)$; aleshores, per a tot $k \geq 1$, és $H(s_k) = 0$ i es tracta de veure que

$h(n) = 0$, per a tot $n \geq 1$. Suposem, contràriament, que existeix un cert $n_0 \geq 1$ tal que $h(n_0) \neq 0$. Podem suposar que n_0 és el menor dels nombres naturals per als quals se satisfà aquesta condició. Podem escriure la igualtat

$$H(s) = \sum_{n\geq 1} h(n)n^{-s} = h(n_0)n_0^{-s} + \sum_{n>n_0} h(n)n^{-s},$$

vàlida per a $\Re(s) > \sigma_a$. Per tant, obtenim el coeficient $h(n_0)$ en la forma

$$h(n_0) = n_0^s H(s) - n_0^s \sum_{n>n_0} h(n)n^{-s},$$

de manera que, per a tot $k \geq 1$,

$$h(n_0) = -n_0^{s_k} \sum_{n>n_0} h(n)n^{-s_k}.$$

Disposem del resultat següent.

Lema 12.2.10. *Siguin $H(s) := \sum_{n\geq 1} h(n)n^{-s}$ una sèrie de Dirichlet absolutament convergent en algun punt $s \in \mathbb{C}$, $c \in \mathbb{R}$ una constant i $s \in \mathbb{C}$ un nombre complex tals que $\Re(s) > c > \sigma_a$, on σ_a denota l'abscissa de convergència absoluta de $H(s)$. Aleshores, per a tot nombre $n_0 \geq 1$, se satisfà la desigualtat*

$$\left|\sum_{n\geq n_0} h(n)n^{-s}\right| \leq n_0^{-\Re(s-c)} \sum_{n\geq n_0} |h(n)|n^{-c}.$$

Demostració: El resultat és gairebé immediat, ja que podem considerar les desigualtats

$$\begin{aligned}\left|\sum_{n\geq n_0} h(n)n^{-s}\right| &\leq \sum_{n\geq n_0} |h(n)|n^{-\Re(s)} \\ &\leq \sum_{n\geq n_0} |h(n)|n^{-c}n^{-\Re(s-c)} \\ &\leq n_0^{-\Re(s-c)} \sum_{n\geq n_0} |h(n)|n^{-c},\end{aligned}$$

la darrera vàlida perquè $\Re(s-c) > 0$. □

Apliquem ara el resultat per a n_0 i un qualsevol dels punts s_k tal que $\Re(s_k) > c > \sigma_a$: obtenim la fita

$$\begin{aligned}|h(n_0)| &\leq n_0^{\Re(s_k)}(n_0+1)^{-\Re(s_k-c)} \sum_{n>n_0} |h(n)|n^{-c} \\ &\leq \left(\frac{n_0}{n_0+1}\right)^{\Re(s_k)} C,\end{aligned}$$

on $C := (n_0+1)^c \sum_{n>n_0} |h(n)|n^{-c}$ és una constant positiva que no depèn del punt s_k que estiguem considerant. Com que podem prendre una infinitat de punts s_k en aquestes condicions, i com que $\lim \Re(s_k) = +\infty$, obtenim que $\lim \left(\frac{n_0}{n_0+1}\right)^{\Re(s_k)} = 0$, de manera que obtenim la contradicció que $|h(n_0)| = 0$. Això acaba la prova de la proposició. □

En particular, el lema anterior ens permet deduir una conseqüència interessant.

Corol·lari 12.2.11. *Sigui* $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ *la funció definida per una sèrie de Dirichlet absolutament convergent en algun semiplà* $\Re(s) > \sigma_a$. *Aleshores, existeix el límit* $\lim_{a\to+\infty} F(a+ib) = f(1)$, *i és uniforme per a* $b \in \mathbb{R}$.

DEMOSTRACIÓ: Només cal veure que $\lim_{a\to+\infty} \sum_{n\geq 2} f(n)n^{-a-bi} = 0$ uniformement per a $b \in \mathbb{R}$. Sigui $c > \sigma_a$, l'abscissa de convergència absoluta. Aleshores, en el semiplà definit per la condició $\Re(s) \geq c$, podem escriure la desigualtat

$$\left|\sum_{n\geq 2} f(n)n^{-s}\right| \leq 2^{-\Re(s-c)} \sum_{n\geq 2} |f(n)|n^{-c} \leq C2^{-\Re(s)},$$

on $C := 2^c \sum_{n\geq 2} |f(n)|n^{-c}$ és una constant real positiva que només depèn de c i de la funció, però no de s tal que $\Re(s) > \sigma_a$. Com que $\lim_{\Re(s)\to+\infty} C2^{-\Re(s)} = 0$, independentment de $\Im(s)$, obtenim el resultat que desitjàvem. □

12.3 Producte de sèries de Dirichlet

El producte de Dirichlet de funcions aritmètiques no s'ha definit així gratuïtament; de fet, ens permet estudiar el producte de les funcions definides per sèries de Dirichlet en el semiplà comú de convergència absoluta. De fet, la tècnica és similar a la definició del producte per a sèries de potències. En aquell cas es defineix el producte a fi que el producte de sèries es correspongui amb el producte de les funcions que les sèries defineixen en el disc de convergència absoluta. Aquí es fa de manera semblant.

Proposició 12.3.1. *Siguin* $F(s) := \sum_{n\geq 1} f(n)n^{-s}$, $G(s) := \sum_{n\geq 1} g(n)n^{-s}$, *sèries de Dirichlet absolutament convergents en algun punt. Aleshores, en el semiplà intersecció dels semiplans de convergència absoluta corresponents, la funció producte* $F(s)G(s)$ *s'expressa en la forma* $F(s)G(s) = \sum_{n\geq 1}(f*g)(n)n^{-s}$, *on* $f*g$ *és el producte de Dirichlet de les funcions aritmètiques* f *i* g.

DEMOSTRACIÓ: Si prenem un punt s del semiplà de convergència absoluta comú a les dues sèries $F(s)$ i $G(s)$, les sèries $F(s)$ i $G(s)$ són absolutament convergents, de manera que podem permutar els seus termes de qualsevol manera sense alterar la suma. Per tant, podem escriure les igualtats

$$\begin{aligned} F(s)G(s) &= \sum_{n\geq 1}\sum_{m\geq 1} f(n)g(m)n^{-s}m^{-s} = \sum_{k\geq 1}\sum_{nm=k} f(n)g(m)k^{-s} \\ &= \sum_{k\geq 1}\sum_{d|k} f(d)g(k/d)k^{-s} = \sum_{k\geq 1}(f*g)(k)k^{-s}, \end{aligned}$$

com volíem demostrar. □

Observació 12.3.2. Recíprocament, si suposem que les sèries $F(s)$, $G(s)$ són absolutament convergents en algun punt $s \in \mathbb{C}$, aleshores, en el semiplà de convergència absoluta comú a $F(s)$ i $G(s)$ la sèrie $H(s) := \sum_{n\geq 1}(f*g)(n)n^{-s}$ és absolutament convergent i defineix la funció producte $F(s)G(s)$.

D'aquest resultat podem obtenir una propietat important per a la funció zeta de Riemann.

Corol·lari 12.3.3. *Per a tot $s \in \mathbb{C}$ tal que $\Re(s) > 1$, se satisfà que $\zeta(s)\sum_{n\geq 1}\mu(n)n^{-s} = 1$. En particular, la funció $\zeta(s)$ no s'anul·la en cap punt s tal que $\Re(s) > 1$.*

Demostració: Observem que la funció μ de Möbius és una funció aritmètica complexa fitada; per tant, la seva abscissa de convergència absoluta és ≤ 1. A més a més, se satisfà la igualtat $\mu * U = u$, on U és la funció constant de valor 1 i u la funció que val 1 per a $n = 1$ i 0 per a $n \neq 1$. Per tant, en el semiplà de $\mathbb{C}$ definit per la condició $\Re(s) > 1$ se satisfà la igualtat de funcions $\zeta(s)\sum_{n\geq 1}\mu(n)n^{-s} = \sum_{n\geq 1}(\mu * U)(n)n^{-s} = \sum_{n\geq 1}u(n)n^{-s} = 1$, com volíem demostrar. □

Anàlogament, per a tot caràcter de Dirichlet χ podem establir la mateixa propietat.

Corol·lari 12.3.4. *Sigui χ un caràcter de Dirichlet. Per a $s \in \mathbb{C}$ tal que $\Re(s) > 1$ és $L(s,\chi) \neq 0$; a més a més, se satisfà la igualtat*

$$\frac{1}{L(s,\chi)} = \sum_{n\geq 1}\chi(n)\mu(n)n^{-s}.$$

Demostració: La funció aritmètica χ no només és multiplicativa, sinó que és completament multiplicativa; això fa que la seva inversa de Dirichlet sigui la funció donada per $n \mapsto \chi(n)\mu(n)$. En efecte, el producte de Dirichlet de χ per aquesta funció és donat per l'expressió $\sum_{d|n}\chi(d)\mu(d)\chi(n/d)$; com que χ és completament multiplicativa, $\chi(d)\chi(n/d) = \chi(n)$ per a tot divisor d de n, de manera que podem treure el factor comú $\chi(n)$ i obtenim l'expressió

$$\chi(n)\sum_{d|n}\mu(d) = \begin{cases} 0, & \text{si } n > 1 \\ 1, & \text{si } n = 1 \end{cases}$$

per al producte. En conseqüència, l'abscissa de convergència absoluta de la sèrie de Dirichlet $\sum_{n\geq 1}\chi(n)\mu(n)n^{-s}$ és menor o igual que la de $L(s,\chi)$ i en el domini de convergència absoluta de la sèrie $L(s,\chi)$ se satisfà la igualtat

$$L(s,\chi)\sum_{n\geq 1}\chi(n)\mu(n)n^{-s} = 1,$$

fet que demostra el resultat que volíem veure. □

12.4 Productes d'Euler

La importància de les sèries de Dirichlet definides per funcions aritmètiques multiplicatives rau en el fet que es pot obtenir una expressió de les funcions que defineixen com a producte infinit.

Proposició 12.4.1. *Sigui $f(n)$ una funció aritmètica multiplicativa i suposem que la sèrie de Dirichlet associada,*

$$F(s) := \sum_{n\geq 1} f(n)n^{-s},$$

és absolutament convergent en un punt s. Aleshores:

(a) *per a cada nombre primer p, la sèrie $E_p(f,s) := \sum_{n\geq 0} f(p^n)p^{-ns}$ és absolutament convergent;*

(b) *en el semiplà de convergència absoluta de $F(s)$, el producte $\prod_p E_p(f,s)$ és absolutament convergent; i*

(c) *en el semiplà de convergència absoluta de $F(s)$ se satisfà que $F(s) = \prod_p E_p(f,s)$.*

Demostració: La propietat (a) és de demostració immediata. En efecte, la sèrie $E_p(f,s)$ és una parcial de la sèrie absolutament convergent $F(s)$, de manera que també és absolutament convergent. D'altra banda, per a tot nombre real $x > 1$, podem considerar el producte (finit) de les sèries $E_p(f,s)$, $\prod_{p\leq x} E_p(f,s)$. Com que les sèries són absolutament convergents, podem permutar els termes de la manera que ens plagui i el producte no canvia. En particular, si tenim en compte que la funció f és multiplicativa, obtenim que els termes d'aquest producte es poden escriure com la suma dels termes de la forma

$$f(p_1^{r_1})p_1^{-r_1 s}f(p_2^{r_2})p_2^{-r_2 s}\dots f(p_k^{r_k})p_k^{-r_k s} = f(p_1^{r_1}p_2^{r_2}\dots p_k^{r_k})(p_1^{r_1}p_2^{r_2}\dots p_k^{r_k})^{-s},$$

on els p_i són els nombres primers $\leq x$ i els exponents $r_i \geq 0$. Per tant, el producte $\prod_{p\leq x} E_p(f,s)$ coincideix amb la suma $\sum_{n\in X} f(n)n^{-s}$, on X designa el conjunt dels nombres enters positius que no són divisibles per primers $> x$. En conseqüència, obtenim la igualtat

$$\sum_{n\geq 1} f(n)n^{-s} - \prod_{p\leq x} E_p(f,s) = \sum_{n\notin X} f(n)n^{-s},$$

que ens permet escriure les desigualtats

$$\left|\sum_{n\geq 1} f(n)n^{-s} - \prod_{p\leq x} E_p(f,s)\right| \leq \sum_{n\notin X} |f(n)n^{-s}| \leq \sum_{n>x} |f(n)n^{-s}|.$$

Com que la sèrie $\sum_{n\geq 1} f(n)n^{-s}$ és absolutament convergent, se satisfà que

$$\lim_{x\to+\infty} \sum_{n>x} |f(n)n^{-s}| = 0, \qquad \text{de manera que} \qquad \lim_{x\to+\infty} \prod_{p\leq x} E_p(f,s) = F(s).$$

D'altra banda, un producte infinit de la forma $\prod_n (1+a_n)$ és absolutament convergent si, i només si, ho és la sèrie $\sum_n a_n$. En el nostre cas,

$$\sum_{p\le x}\left|\sum_{n\ge 1} f(p^n)p^{-ns}\right| \le \sum_{p\le x}\sum_{n\ge 1}|f(p^n)p^{-ns}| \le \sum_{n\ge 2}|f(n)n^{-s}|,$$

de manera que les sumes parcials de la sèrie de nombres reals positius

$$\sum_p \left|\sum_{n\ge 1} f(p^n)p^{-ns}\right|$$

són fitades; per tant, obtenim la convergència absoluta del producte

$$\prod_p \sum_{n\ge 0} f(p^n)p^{-ns}.$$

Això acaba la demostració de (b).

Per últim, només cal observar que, per ser $\prod_p E_p(f,s)$ un producte infinit absolutament convergent, el seu valor es pot calcular com el límit

$$\lim_{x\to+\infty}\prod_{p\le x} E_p(f,s);$$

i això acaba la prova de (c), ja que aquest límit és $F(s)$. □

Definició 12.4.2. La sèrie $E_p(f,s)$ s'anomena el p-èsim factor d'Euler associat a la funció $F(s)$.

En el cas que la funció f sigui completament multiplicativa es pot obtenir una fórmula més compacta. En efecte, en aquest cas podem escriure

$$E_p(f,s) = \sum_{n\ge 0} f(p^n)p^{-ns} = \sum_{n\ge 0}(f(p)p^{-s})^n,$$

la suma d'una progressió geomètrica de raó $f(p)p^{-s}$; el fet que la sèrie sigui absolutament convergent ens permet assegurar que $|f(p)p^{-s}|<1$, i la suma de la sèrie és $E_p(f,s) = \dfrac{1}{1-f(p)p^{-s}}$; per tant, podem escriure la igualtat $F(s) = \prod_p \dfrac{1}{1-f(p)p^{-s}}$.

Corol·lari 12.4.3. *Sigui χ un caràcter de Dirichlet. Aleshores, en el semiplà de $\mathbb{C}$ definit per la condició $\Re(s)>1$ se satisfà la fórmula*

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}}.$$

En particular, per al caràcter trivial obtenim la fórmula

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}.\ \square$$

12.5 Convergència de les sèries de Dirichlet

En aquesta secció ens proposem l'estudi més acurat del conjunt de punts de $\mathbb{C}$ on una sèrie de Dirichlet

$$F(s) := \sum_{n\geq 1} f(n)n^{-s}$$

és convergent. Per a això comencem per establir la següent fórmula de sumació parcial d'Abel.

Lema 12.5.1 (Fórmula de sumació d'Abel)**.** *Donada una funció aritmètica g posem, per a tot nombre real x, $G(x) := \sum_{n\leq x} g(n)$. Siguin $x, y \in \mathbb{R}$ tals que $0 < x < y$ i considerem una funció $\varphi : [x, y] \longrightarrow \mathbb{C}$ de classe C^1. Aleshores,*

$$\sum_{x<n\leq y} g(n)\varphi(n) = G(y)\varphi(y) - G(x)\varphi(x) - \int_x^y G(t)\varphi'(t)dt.$$

Demostració: La funció $G(x)$ és una funció esglaonada amb salts de valor $g(n)$ en els enters positius $n > 1$; per tant, la integral de Riemann-Stieltjes ens proporciona la igualtat

$$\sum_{x<n\leq y} g(n)\varphi(n) = \int_x^y \varphi(t)dG(t).$$

Si ara integrem per parts, obtenim la igualtat

$$\begin{aligned}\sum_{x<n\leq y} g(n)\varphi(n) &= G(y)\varphi(y) - G(x)\varphi(x) - \int_x^y G(t)d\varphi(t)\\ &= G(y)\varphi(y) - G(x)\varphi(x) - \int_x^y G(t)\varphi'(t)dt\end{aligned}$$

que volíem demostrar. □

Proposició 12.5.2. *Siguin f una funció aritmètica i $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ la sèrie de Dirichlet associada. Suposem que la sèrie $F(s)$ és convergent en algun punt $s \in \mathbb{C}$. Aleshores:*

(a) *Per a tot punt $s' \in \mathbb{C}$ tal que $\Re(s') > \Re(s)$, la sèrie $F(s')$ és convergent.*

(b) *La convergència de la sèrie $F(s')$ és uniforme en tot subconjunt compacte del semiplà definit per la condició $\Re(s') > \Re(s)$.*

(c) *Per a tot nombre real $\varepsilon > 0$, la convergència de la sèrie $F(s')$ és absoluta en el semiplà definit per la condició $\Re(s') \geq \Re(s) + 1 + \varepsilon$.*

Demostració: Com que la sèrie $F(s)$ és convergent, les seves sumes parcials són fitades; és a dir, existeix un nombre real $M > 0$ tal que per a tot enter $m \geq 1$ se satisfà la desigualtat $\left|\sum_{n=1}^{m} f(n)n^{-s}\right| \leq M$. Ara podem aplicar la fórmula de sumació parcial d'Abel:

donat un nombre complex s' tal que $\Re(s') > \Re(s)$, considerem la funció aritmètica $g(n) := f(n)n^{-s}$ i la funció $\varphi(x) := x^{s-s'}$. La fórmula de sumació d'Abel ens permet escriure, per a tot $x > 0$, la igualtat

$$\begin{aligned}\sum_{x<n\leq y} f(n)n^{-s'} &= \sum_{x<n\leq y} g(n)\varphi(n)\\ &= G(y)y^{s-s'} - G(x)x^{s-s'} - \int_x^y G(t)(s-s')t^{s-s'-1}dt,\end{aligned}$$

on $G(x) := \sum_{n\leq x} g(n)$. Com que, per a tot nombre real $x > 0$ és $|G(x)| \leq M$, obtenim la cadena de desigualtats

$$\begin{aligned}\left|\sum_{x<n\leq y} f(n)n^{-s'}\right| &\leq My^{\Re(s-s')} + Mx^{\Re(s-s')} + |s-s'|M\int_x^y t^{\Re(s-s'-1)}dt\\ &\leq 2Mx^{\Re(s-s')} + |s'-s|M\left|\frac{y^{\Re(s-s')} - x^{\Re(s-s')}}{\Re(s-s')}\right|\\ &\leq 2Mx^{\Re(s-s')}\left(1 + \frac{|s-s'|}{\Re(s'-s)}\right).\end{aligned}$$

Aquesta desigualtat és la clau de la demostració.

En efecte. Per a provar (a) és suficient provar (b), i la prova de (b) és suficient si la fem per a rectangles de la forma $[a,b]\times[c,d]$ inclosos en el semiplà definit per la condició $\Re(s') > \Re(s)$, és a dir, tals que $a > \Re(s)$. Per a punts s' d'aquest rectangle, podem fitar el parèntesi $\left(1 + \frac{|s-s'|}{\Re(s'-s)}\right)$ independentment de s', de manera que obtenim una desigualtat

$$\left|\sum_{x<n\leq y} f(n)n^{-s'}\right| \leq M'x^{\Re(s)-a},$$

on el nombre $M' > 0$ no depèn del punt s' del rectangle. Com que $\lim_{x\to+\infty} x^{\Re(s)-a} = 0$, obtenim la condició de convergència de Cauchy de manera uniforme sobre el rectangle; és a dir, la convergència uniforme de la sèrie.

Per a veure (c) és suficient provar que la convergència de la sèrie $F(s')$ és absoluta en el semiplà definit per la condició $\Re(s') > 1 + \Re(s)$. Però podem prendre, ja que la sèrie $F(s)$ és convergent, una fita $C > 0$ dels seus termes; això ens permet escriure la desigualtat

$$|f(n)n^{-s'}| = |f(n)n^{-s}||n^{s-s'}| \leq Cn^{\Re(s-s')},$$

de manera que si $\Re(s'-s) > 1$, aleshores la sèrie $\sum_{n\geq 1} |f(n)n^{-s'}|$ és convergent, en virtut del criteri de comparació. □

Com a conseqüència, donada una sèrie de Dirichlet $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ que no sigui convergent en tot $\mathbb{C}$ ni divergent en tot $\mathbb{C}$, existeix un nombre real σ, que s'anomena l'abscissa de convergència, tal que per a tot nombre complex s tal que $\Re(s) > \sigma$ la sèrie $F(s)$ és convergent i per a $\Re(s) < \sigma$ la sèrie $F(s)$ és divergent. A més a més, se satisfan les desigualtats $\sigma \leq \sigma_a \leq \sigma + 1$, entre les abscisses de convergència i de convergència absoluta de la sèrie $F(s)$.

12.6 Analiticitat de les funcions de Dirichlet

En aquesta secció es tracta d'estudiar les propietats diferencials de les funcions definides per sèries de Dirichlet convergents. Concretament, del seu comportament analític i de les seves derivades successives. El caràcter analític és conseqüència de la convergència uniforme.

Proposició 12.6.1. *Siguin* $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ *una sèrie de Dirichlet convergent per a algun nombre complex* s*, i* $\sigma \in \mathbb{R} \cup \{-\infty, +\infty\}$ *l'abscissa de convergència de la sèrie. Aleshores, la funció* $F(s)$ *definida en el semiplà donat per la condició* $\Re(s) > \sigma$ *és analítica i la seva derivada admet el desenvolupament en sèrie de Dirichlet*

$$D(F, s) = -\sum_{n\geq 1} f(n)\log(n)n^{-s}.$$

Demostració: En efecte, cada una de les funcions $s \mapsto f(n)n^{-s}$ és una funció entera i admet per derivada la funció $s \mapsto -f(n)\log(n)n^{-s}$; en conseqüència, i com que la sèrie $F(s)$ és uniformement convergent en el semiplà definit per la condició $\Re(s) > \sigma$, la funció $F(s)$ és derivable respecte de la variable complexa s; és a dir, analítica en $\Re(s) > \sigma$. A més a més, la seva derivada admet l'expressió

$$D(F, s) = -\sum_{n\geq 1} f(n)\log(n)n^{-s},$$

com volíem demostrar. □

En el cas que els coeficients $f(n)$ de la sèrie de Dirichlet són nombres reals no negatius, es pot obtenir l'abscissa de convergència a partir de les propietats de la funció $F(s)$ que defineix la sèrie; concretament, l'abscissa de convergència és determinada per una singularitat de la funció $F(s)$ en l'eix real. De manera explícita, podem escriure el resultat següent.

Proposició 12.6.2. *Sigui* $F(s)$ *una funció que admet un desenvolupament en sèrie de Dirichlet*

$$F(s) = \sum_{n\geq 1} f(n)n^{-s}, \tag{12.6.1}$$

convergent en el semiplà definit per la condició $\Re(s) > \sigma$*,* $\sigma \in \mathbb{R}$*, i on* $f(n)$ *és una funció aritmètica que només pren valors reals no negatius. Suposem que la funció* $F(s)$ *és analítica en un entorn obert de* σ *(encara que no suposem que en aquest entorn la funció admeti un desenvolupament en sèrie de Dirichlet convergent). Aleshores, existeix un nombre real* $\varepsilon > 0$ *de manera que la sèrie* (12.6.1) *és convergent en el semiplà definit per la condició* $\Re(s) > \sigma - \varepsilon$ *i la funció* $F(s)$ *coincideix amb la suma de la sèrie en aquest semiplà.*

Demostració: Sigui $s_0 := 1 + \sigma$; com que $F(s)$ és analítica en s_0, podem expressar la funció $F(s)$ com la suma d'una sèrie de potències

$$F(s) = \sum_{k\geq 0} \frac{D^k(F, s_0)}{k!}(s - s_0)^k,$$

absolutament convergent en un cert disc obert de centre s_0; però com que la funció $F(s)$ és analítica en σ, el radi de convergència d'aquesta sèrie de potències és tal que σ és un punt interior del disc de convergència absoluta; per tant, el radi de convergència de la sèrie de potències és estrictament més gran que 1. Ara bé, les derivades successives de la funció $F(s)$ en el semiplà de convergència són donades per l'expressió

$$D^k(F,s) = (-1)^k \sum_{n\geq 1} f(n)(\log(n))^k n^{-s},$$

fórmula que s'aplica al punt s_0; si substituïm la nova expressió en l'anterior en sèrie de potències podem escriure la igualtat

$$F(s) = \sum_{k\geq 0}\sum_{n\geq 1} \frac{(s_0-s)^k}{k!} f(n)(\log(n))^k n^{-s_0},$$

vàlida en un entorn de s_0 que conté el punt σ; en particular, existeix un nombre real $\varepsilon > 0$ tal que l'expressió anterior és vàlida en $s = \sigma - \varepsilon$. Ara, la sèrie doble té coeficients reals i positius d'un lloc endavant (per exemple, sempre que $\log(n) > 0$, és a dir, per a $n > 1$); per tant, la convergència és automàticament absoluta i podem permutar l'ordre de les dues sumes. D'aquesta manera obtenim l'expressió

$$\begin{aligned} F(\sigma-\varepsilon) &= \sum_{n\geq 1} f(n)n^{-s_0} \sum_{k\geq 0} \frac{((1+\varepsilon)\log(n))^k}{k!} \\ &= \sum_{n\geq 1} f(n)n^{-s_0} \exp((1+\varepsilon)\log(n)) \\ &= \sum_{n\geq 1} f(n)n^{1+\varepsilon-s_0} \\ &= \sum_{n\geq 1} f(n)n^{-(\sigma-\varepsilon)}. \end{aligned}$$

Dit d'una altra manera, la sèrie de Dirichlet $\sum_{n\geq 1} f(n)n^{-s}$ és convergent en $s = \sigma - \varepsilon$ i la seva suma coincideix amb el valor de la funció $F(s)$ en aquest punt; per tant, la sèrie de Dirichlet és convergent també en el semiplà definit per la condició $\Re(s) > \sigma - \varepsilon$, com volíem demostrar. □

Corol·lari 12.6.3. *Suposem que $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ és una sèrie de Dirichlet amb abscissa de convergència $\sigma \in \mathbb{R}$ i tal que $f(n)$ és un nombre real no negatiu, per a tot $n \geq 1$. Aleshores, la funció $F(s)$ té una singularitat en el punt σ de l'eix real.*

Demostració: Acabem de veure que si la funció definida per la sèrie de Dirichlet és analítica en un entorn d'un nombre real, aleshores convergeix en un semiplà que conté aquest nombre; per tant, el semiplà de convergència ha d'ésser limitat per una singularitat de la funció en l'eix real. Això és el que calia demostrar. □

Capítol 13

La funció zeta de Hurwitz

Per a un tractament adequat de la funció zeta de Riemann i de les funcions L associades als caràcters de Dirichlet és molt còmode fer, en primer lloc, l'estudi de la funció zeta de Hurwitz, ja que aquesta funció permet unificar-ne el tractament. Per això, aquest capítol es dedica a l'estudi d'aquesta funció.

Molta més informació sobre aquesta funció, i també sobre altres funcions relacionades, es pot trobar en [W-W 70].

13.1 La funció Gamma d'Euler

La primera secció d'aquest capítol es dedica a l'estudi de la funció Gamma d'Euler. La finalitat d'aquest estudi és obtenir representacions integrals adequades per a poder fer l'extensió meromorfa a tot el pla complex de la funció zeta de Hurwitz.

Definició 13.1.1. La integral impròpia $\displaystyle\int_0^{+\infty} x^{s-1}e^{-x}dx$ és convergent per a tot nombre complex s tal que $\Re(s) > 0$. El valor de la integral es representa per $\Gamma(s)$, de manera que s'obté una funció en el semiplà definit per la condició $\Re(s) > 0$; s'anomena la funció Gamma d'Euler.

Proposició 13.1.2. *Se satisfan les propietats següents.*

(a) (Equació funcional) *Per a tot nombre complex s tal que $\Re(s) > 0$, se satisfà la igualtat* $\Gamma(s+1) = s\Gamma(s)$.

(b) *Per a tot $n \in \mathbb{N}$,* $\Gamma(n+1) = n!$.

(c) *La funció $s \mapsto \Gamma(s)$ és analítica en el semiplà $\Re(s) > 0$. En particular, la seva derivada admet l'expressió*

$$D(\Gamma, s) = \int_0^{+\infty} x^{s-1}\log(x)e^{-x}dx.$$

Demostració: La primera propietat es comprova amb una simple integració per parts. En efecte, podem escriure la igualtat

$$\begin{aligned}\Gamma(s+1) &= \int_0^\infty x^s e^{-x} dx \\ &= \lim_{x\to+\infty}(-x^s e^{-x}) - \lim_{x\to 0}(-x^s e^{-x}) + s\int_0^\infty x^{s-1}e^{-x}dx \\ &= s\int_0^\infty x^{s-1}e^{-x}dx \\ &= s\Gamma(s),\end{aligned}$$

ja que els dos límits valen 0.

La segona propietat es dedueix formalment de la primera a partir del càlcul de la integral

$$\Gamma(1) = \int_0^\infty e^{-x}dx = \lim_{x\to+\infty}(-e^{-x}) - \lim_{x\to 0}(-e^{-x}) = 1.$$

Per últim, la derivació sota el símbol integral permet obtenir immediatament que la funció Γ és derivable respecte de la variable complexa s així com l'expressió de la seva derivada, de manera que $\Gamma(s)$ és una funció analítica del semiplà definit per la condició $\Re(s) > 0$. □

Proposició 13.1.3. *La funció Gamma s'estén a una funció meromorfa de tot el pla complex amb pols simples en els enters no positius. Per a tot enter $n \geq 0$, el residu de la funció en el punt $-n$ és $(-1)^n/n!$.*

Demostració: Com a conseqüència de l'equació funcional, podem estendre la funció Gamma a una funció de tot el pla complex llevat dels nombres enters no positius; en efecte, donat un nombre complex $s \notin -\mathbb{N}$, podem sumar-li un enter $n > 0$ de manera que sigui $\Re(s+n) > 0$ i alhora que $s+n$ no sigui un enter positiu. Així, podem definir $\Gamma(s)$ per la fórmula $\Gamma(s) := \dfrac{\Gamma(s+n)}{s(s+1)(s+2)\cdots(s+n-1)}$. Aquesta definició no depèn del nombre natural n que haguem elegit; així obtenim una funció $\Gamma : \mathbb{C} - (-\mathbb{N}) \longrightarrow \mathbb{C}$ per a la qual se satisfà l'equació funcional $\Gamma(s+1) = s\Gamma(s)$, per a $s \notin -\mathbb{N}$.

La funció així estesa és una funció meromorfa de tot el pla complex, ja que, per a cada punt $s \notin -\mathbb{N}$ hi ha un entorn en el qual $\Gamma(s)$ és el quocient de dues funcions analítiques tals que el denominador no s'anul·la. En particular, podem calcular el residu de la funció $\Gamma(s)$ en els enters $-n$, $n \geq 0$, i obtenir la fórmula donada en l'enunciat: en efecte,

$$\begin{aligned}\lim_{s\to -n}(s+n)\Gamma(s) &= \lim_{s\to -n}\frac{(s+n)\Gamma(s+n+1)}{s(1+s)(2+s)\cdots(n+s)} \\ &= \lim_{s\to -n}\frac{\Gamma(s+n+1)}{s(1+s)(2+s)\cdots(n-1+s)} \\ &= \frac{\Gamma(1)}{(-n)(1-n)(2-n)\cdots(n-1-n)} \\ &= \frac{1}{(-1)^n n!}.\ \square\end{aligned}$$

La proposició següent llista algunes de les propietats importants de la funció Gamma; algunes les farem servir.

Proposició 13.1.4. (a) *Per a tot nombre complex $s \notin -\mathbb{N}$,*

$$\Gamma(s) = \lim \frac{n^s n!}{s(s+1)\cdots(s+n)}.$$

(b) *Per a tot nombre complex $s \notin \mathbb{Z}$*

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

(c) *Per a tot nombre complex s i tot enter $m \geq 1$ tals que els factors estan definits,*

$$\Gamma(s)\Gamma\left(s+\frac{1}{m}\right)\cdots\Gamma\left(s+\frac{m-1}{m}\right) = (2\pi)^{(m-1)/2} m^{(1/2)-ms}\Gamma(ms).$$

(d) *En particular, si $s, s/2, (s+1)/2 \notin -\mathbb{N}$, aleshores*

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

Demostració: La prova es pot trobar en molts llibres d'anàlisi (per exemple, en [W-W 70]). Només convé notar que la darrera propietat és la tercera aplicada a $s/2$ amb $m = 2$. □

Corol·lari 13.1.5. *La funció $s \mapsto \Gamma(s)^{-1}$ és una funció entera amb zeros simples en els punts $s \in -\mathbb{N}$.*

Demostració: Només cal tenir en compte l'expressió

$$\Gamma(s) = \lim \frac{n^s n!}{s(s+1)\cdots(s+n)},$$

que expressa $\Gamma(s)^{-1}$ com el producte infinit

$$\Gamma(s)^{-1} = s(s+1)\prod_{n\geq 2}\left(\frac{n-1}{n}\right)^s \frac{s+n}{n}.$$

Aquest producte és absolutament convergent com a producte infinit i, per tant, no nul. □

13.2 Definició de la funció zeta de Hurwitz

En aquesta secció es tracta de donar la definició i les propietats més elementals de la funció zeta de Hurwitz.

Lema 13.2.1. *Per a tot nombre real a tal que $0 < a \leq 1$, la sèrie*

$$\zeta(s,a) := \sum_{n\geq 0}\frac{1}{(n+a)^s}$$

és absolutament convergent en el semiplà definit per la condició $\Re(s) > 1$. La convergència és uniforme en els semiplans tancats $\Re(s) \geq 1+\varepsilon$, $\varepsilon > 0$. La funció $\zeta(s,a)$ definida per aquesta sèrie és holomorfa en el semiplà $\Re(s) > 1$.

DEMOSTRACIÓ: Per a tot nombre real $\varepsilon > 0$ i tot nombre complex s tal que $\Re(s) \geq 1+\varepsilon$ podem escriure la desigualtat

$$\sum_{n\geq 0} |(n+a)^{-s}| = \sum_{n\geq 0} (n+a)^{-\Re(s)} \leq \sum_{n\geq 0} (n+a)^{-(1+\varepsilon)}.$$

En virtut del criteri de comparació, obtenim la convergència absoluta de la sèrie; i també la convergència uniforme, ja que la darrera sèrie és independent de s. Per últim, com que les funcions $s \mapsto (n+a)^{-s}$ són funcions enteres, la funció $\zeta(s,a)$ és la suma uniforme de funcions holomorfes en el semiplà $\Re(s) > 1$; per tant, una funció holomorfa en aquest semiplà. □

Definició 13.2.2. Sigui $a \in \mathbb{R}$ tal que $0 < a \leq 1$. La funció definida en el semiplà $\Re(s) > 1$ per la sèrie $\zeta(s,a)$ s'anomena la funció zeta de Hurwitz de paràmetre a.

Observació 13.2.3. Cal observar que l'índex de la suma assoleix el valor 0, contràriament a la definició de la funció zeta de Riemann. D'altra banda, per a $\Re(s) > 1$ se satisfà la igualtat $\zeta(s) = \zeta(s,1)$; és a dir, la funció zeta de Riemann és la funció zeta de Hurwitz de paràmetre 1.

Convé recordar el resultat següent dels cursos d'anàlisi.

Teorema 13.2.4 (Levi)**.** *Sigui $\{g_n\}_{n\geq 0}$ una successió de funcions reals definides en un interval I tals que:*

(a) *per a tot $n \geq 0$, la funció g_n és integrable Lebesgue en I;*

(b) *per a tot $n \geq 0$, la funció g_n és no negativa en I, llevat d'un conjunt de mesura nul·la; i*

(c) *la sèrie $\displaystyle\sum_{n\geq 0} \int_I g_n$ és convergent.*

Aleshores, la sèrie

$$g(x) := \sum_{n\geq 0} g_n(x)$$

és convergent en I, llevat d'un conjunt de mesura nul·la, g és integrable en el sentit de Lebesgue en I, i se satisfà la igualtat

$$\int_I g = \sum_{n\geq 0} \int_I g_n. \ \square$$

El resultat següent dóna una representació integral de la funció zeta de Hurwitz.

Proposició 13.2.5. *Siguin $a \in \mathbb{R}$, $s \in \mathbb{C}$ tals que $0 < a \leq 1$ i $\Re(s) > 1$. Aleshores se satisfà la igualtat*

$$\Gamma(s)\zeta(s,a) = \int_0^\infty \frac{x^{s-1}e^{-ax}}{1-e^{-x}}dx.$$

DEMOSTRACIÓ: Començarem la demostració pel cas $s \in \mathbb{R}$, $s > 1$. Per a tot nombre enter $n \geq 0$ podem fer el canvi de variable $x = (n+a)t$ en la integral que defineix la funció $\Gamma(s)$; obtenim l'expressió

$$\Gamma(s) = (n+a)^s \int_0^\infty e^{-(n+a)t} t^{s-1} dt,$$

de manera que obtenim la igualtat

$$(n+a)^{-s}\Gamma(s) = \int_0^\infty e^{-nt} e^{-at} t^{s-1} dt$$

i podem sumar la sèrie

$$\begin{aligned}
\Gamma(s)\zeta(s,a) &= \sum_{n\geq 0} \int_0^\infty e^{-nt} e^{-at} t^{s-1} dt \\
&= \int_0^\infty \sum_{n\geq 0} e^{-nt} e^{-at} t^{s-1} dt \\
&= \int_0^\infty e^{-at} t^{s-1} \sum_{n\geq 0} e^{-nt} dt \\
&= \int_0^\infty \frac{e^{-at} t^{s-1}}{1-e^{-t}} dt,
\end{aligned}$$

la segona igualtat en virtut del teorema de Levi, i la darrera perquè $0 < e^{-t} < 1$, ja que $s > 1$. Això acaba la prova en el cas $s \in \mathbb{R}$.

En el cas general, el principi de prolongació analítica permet que només haguem de comprovar que la funció definida per la integral

$$\int_0^\infty \frac{x^{s-1} e^{-ax}}{1-e^{-x}} dx$$

és holomorfa en el semiplà $\Re(s) > 1$, ja que la funció $\Gamma(s)\zeta(s,a)$ també ho és i totes dues funcions coincideixen en la semirecta $s \in \mathbb{R}$, $s > 1$. Dit d'una altra manera, és suficient provar el resultat següent. □

Lema 13.2.6. *La integral*

$$\int_0^\infty \frac{x^{s-1} e^{-ax}}{1-e^{-x}} dx$$

és uniformement convergent, com a funció de s, en cadascuna de les bandes verticals de la forma $1+\varepsilon \leq \Re(s) \leq c$, $1 < 1+\varepsilon < c$, *del semiplà* $\Re(s) > 1$. *Per tant, defineix una funció holomorfa en el semiplà* $\Re(s) > 1$.

DEMOSTRACIÓ: Considerem fixats $\varepsilon > 0$ i $c > 1+\varepsilon$, i sigui $s \in \mathbb{C}$ un punt qualsevol tal que $1+\varepsilon \leq \Re(s) \leq c$. Podem escriure

$$\begin{aligned}
\int_0^\infty \left| \frac{e^{-at} t^{s-1}}{1-e^{-t}} \right| dt &= \int_0^\infty \frac{e^{-at} t^{\Re(s)-1}}{1-e^{-t}} dt \\
&= \int_0^1 \frac{e^{-at} t^{\Re(s)-1}}{1-e^{-t}} dt + \int_1^\infty \frac{e^{-at} t^{\Re(s)-1}}{1-e^{-t}} dt.
\end{aligned}$$

Considerem la primera integral; com que $0 \leq t \leq 1$, és $t^{\Re(s)-1} \leq t^{\varepsilon}$, de manera que

$$\int_0^1 \frac{e^{-at}t^{\Re(s)-1}}{1-e^{-t}}dt \leq \int_0^1 \frac{e^{-at}t^{\varepsilon}}{1-e^{-t}}dt = \int_0^1 \frac{e^{(1-a)t}t^{\varepsilon}}{e^t-1}dt \leq e^{1-a}\int_0^1 t^{\varepsilon-1}dt, = \frac{e^{1-a}}{\varepsilon},$$

ja que, per a $0 \leq t \leq 1$, és $e^{(1-a)t} \leq e^{1-a}$ i $\dfrac{t}{e^t-1} \leq 1$.

La segona integral es pot fitar de la manera següent; com que $t \geq 1$, és $t^{\Re(s)-1} \leq t^{c-1}$, i podem escriure

$$\int_1^{\infty} \frac{e^{-at}t^{\Re(s)-1}}{1-e^{-t}}dt \leq \int_1^{\infty} \frac{e^{-at}t^{c-1}}{1-e^{-t}}dt \leq \int_0^{\infty} \frac{e^{-at}t^{c-1}}{1-e^{-t}}dt = \Gamma(c)\zeta(c,a),$$

ja que el resultat ja està provat per a $c \in \mathbb{R}$, $c > 1$.

D'aquesta manera, obtenim una fita uniforme de la integral del valor absolut; això ens permet assegurar que la integral és absolutament convergent i uniformement convergent en tots els conjunts de l'enunciat i, en conseqüència, defineix una funció holomorfa en el semiplà $\Re(s) > 1$. □

Corol·lari 13.2.7 (Representació integral de la funció zeta de Riemann)**.** *Per a tot nombre complex s tal que $\Re(s) > 1$ se satisfà la igualtat*

$$\Gamma(s)\zeta(s) = \int_0^{\infty} \frac{x^{s-1}e^{-x}}{1-e^{-x}}dx. \square$$

13.3 Extensió meromorfa de la funció zeta de Hurwitz

Així com la funció zeta de Riemann es pot estendre a una funció meromorfa de tot $\mathbb{C}$, també la funció zeta de Hurwitz es pot estendre a una funció meromorfa de $\mathbb{C}$. L'objectiu d'aquesta secció és dur a terme aquesta prolongació.

Per a aconseguir aquest objectiu, partirem de la fórmula

$$\Gamma(s)\zeta(s,a) = \int_0^{+\infty} \frac{x^{s-1}e^{-ax}}{1-e^{-x}}dx,$$

que és vàlida per a $\Re(s) > 1$ i $0 < a \leq 1$, i considerarem la funció de dues variables definida per la fórmula $f(s,z) := \dfrac{z^{s-1}e^{-az}}{1-e^{-z}}$ per a tots els valors complexos de s, z tals que $z \notin 2\pi i\mathbb{Z}$ (en particular, $z \neq 0$), i on z^{s-1} significa $e^{(s-1)\log(z)}$ per a la determinació del logaritme que és real en els nombres reals positius $x + 0^+i$, i té part imaginària $2\pi i$ en els nombres reals positius $x + 0^-i$. Es tracta de fer una integral de línia d'aquesta funció.

Anem, doncs, a definir un camí d'integració. Fixem un nombre real positiu arbitrari $0 < \varepsilon < 2\pi$ i considerem els tres camins del pla complex definits de la manera següent: γ_1 és el semieix real positiu (recorregut en sentit decreixent) parametritzat per la fórmula $z := r$, per a $r \in \mathbb{R}$, $+\infty > r \geq \varepsilon$; γ_2 és la circumferència de centre a l'origen i radi constant $\varepsilon > 0$, recorreguda en sentit antihorari (és a dir, en sentit positiu), parametritzada per la fórmula $z := \varepsilon e^{i\theta}$, $0 \leq \theta \leq 2\pi$; i γ_3 és el semieix real positiu (com abans, però recorregut en

sentit creixent), parametritzat per la fórmula $z := re^{2\pi i}$, $r \in \mathbb{R}$, $\varepsilon \leq r < +\infty$. Anomenem γ el camí composició dels anteriors, $\gamma := \gamma_3 \circ \gamma_2 \circ \gamma_1$; és clar que γ, així com cada un dels γ_i, depèn de ε.

Ara, per a tot nombre real a, $0 < a \leq 1$, i tot nombre complex s, podem considerar la integral de línia

$$I_\varepsilon(s,a) := \int_\gamma \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz.$$

Es tracta de provar el resultat següent.

Teorema 13.3.1. *Siguin $a, \varepsilon \in \mathbb{R}$, $0 < a \leq 1$, $0 < \varepsilon < 2\pi$. Aleshores:*

(a) *la integral*

$$I_\varepsilon(s,a) := \int_\gamma \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz$$

és uniformement convergent en tot disc tancat de la forma $|s| \leq M$, $M \in \mathbb{R}$, $M > 0$;

(b) *la integral $I_\varepsilon(s,a)$ no depèn del valor de ε elegit en $0 < \varepsilon < 2\pi$;*

(c) *$I_\varepsilon(s,a)$ defineix una funció entera de s; i*

(d) *en el semiplà $\Re(s) > 1$ se satisfà la igualtat $\zeta(s,a) = \Gamma(1-s)I(s,a)$, on*

$$I(s,a) := \frac{e^{-\pi i s}}{2\pi i} I_\varepsilon(s,a) = \frac{e^{-\pi i s}}{2\pi i} \int_\gamma \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz.$$

Demostració: Per a tot nombre complex s, la funció d'una variable $z \mapsto \dfrac{z^{s-1}e^{-az}}{1-e^{-z}}$ és una funció holomorfa de la corona $0 < |z| < 2\pi$ privada dels punts del semieix real positiu; per tant, la forma diferencial $f(s,z)dz$ és tancada en tot obert inclòs en aquest conjunt. Això ens permet assegurar que les integrals $I_\varepsilon(s,a)$ no depenen del valor de ε elegit en $0 < \varepsilon < 2\pi$; en particular, obtindrem (b) com a conseqüència de (a).

D'altra banda, per a tot element z del camí γ, la funció d'una variable $s \mapsto \dfrac{z^{s-1}e^{-az}}{1-e^{-z}}$ és una funció entera; per tant, si demostrem que la integral $I_\varepsilon(s,a)$ és uniformement convergent sobre tots els discs tancats $|s| \leq M$, obtindrem que la funció definida per aquesta integral és una funció entera. Així, obtindrem (c) a partir de (a). Per tant, cal provar (a) i (d).

Posem $\sigma := \Re(s)$, $t := \Im(z)$, les parts real i imaginària de s, de manera que $s = \sigma + it$. Comencem per estudiar la integral

$$\int_{\gamma_2} \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz$$

en el disc tancat $|s| \leq M$. Per a això, posem $g(z) := \dfrac{e^{-az}}{1-e^{-z}}$; obtenim la igualtat

$$\begin{aligned}\int_{\gamma_2} \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz &= \int_{\gamma_2} g(z)z^{s-1}dz \\ &= \int_0^{2\pi} g(\varepsilon e^{i\theta})\varepsilon^{s-1}e^{(s-1)i\theta}i\varepsilon e^{i\theta}d\theta \\ &= i\varepsilon^s \int_0^{2\pi} e^{is\theta}g(\varepsilon e^{i\theta})d\theta.\end{aligned}$$

Observem, ara, que per a $|z| < 2\pi$ la funció $g(z)$ té un únic pol, i simple, en $z = 0$; per tant, existeix un nombre real $B > 0$ tal que per a $|z| \leq \varepsilon$ és $|zg(z)| \leq B$; dit d'una altra manera, per a $0 < |z| \leq \varepsilon$, és $|g(z)| \leq \dfrac{B}{|z|}$. Això ens permet escriure les desigualtats

$$\begin{aligned}\left|\int_{\gamma_2} z^{s-1}g(z)dz\right| &\leq |\varepsilon^s| \int_0^{2\pi} |e^{is\theta}||g(\varepsilon e^{i\theta})|d\theta \\ &\leq \varepsilon^\sigma \int_0^{2\pi} e^{-t\theta}\frac{B}{\varepsilon}d\theta \\ &\leq B\varepsilon^{\sigma-1}2\pi e^{\pi M} \\ &\leq B\varepsilon^{M-1}2\pi e^{\pi M},\end{aligned}$$

ja que $|s| \leq M$ implica que $|\sigma| \leq M$ i $|t| \leq M$.

D'aquí en resulten dues conseqüències importants. D'una banda, una fita uniforme del valor absolut de la integral sobre γ_2. De l'altra, si ens mantenim en el semiplà $\Re(s) > 1$, aleshores $\lim\limits_{\varepsilon\to 0} 2\pi B e^{\pi M}\varepsilon^{\sigma-1} = 0$, de manera que

$$\lim_{\varepsilon\to 0}\int_{\gamma_2} z^{s-1}g(z)dz = 0.$$

Estudiem, ara, la integral sobre γ_1 i sobre γ_3. Mantinguem s en el disc tancat $|s| \leq M$ i considerem $r \geq 1$. Sobre el camí γ_1, podem escriure $|z^{s-1}| = |r^{s-1}| = r^{\sigma-1} \leq r^{M-1}$. Anàlogament, sobre γ_3, i si $r \geq 1$, podem escriure que

$$|z^{s-1}| = |r^{s-1}||e^{2\pi i(s-1)}| = r^{\sigma-1}e^{-2\pi t} \leq r^{M-1}e^{2\pi M},$$

ja que $-M \leq -t \leq M$ i l'exponencial real és creixent. Així, sobre γ_1 i sobre γ_3, i per a $r \geq 1$, podem escriure la desigualtat

$$\left|\frac{z^{s-1}e^{-az}}{1-e^{-z}}\right| \leq \frac{r^{M-1}e^{2\pi M}e^{-ar}}{1-e^{-r}} = \frac{r^{M-1}e^{2\pi M}e^{(1-a)r}}{e^r-1}.$$

D'altra banda, per a $r > \log(2)$ podem escriure $e^r - 1 > e^r/2$, de manera que, per a $r \geq 1$, i sobre els camins γ_1 i γ_3, obtenim la desigualtat

$$\left|\frac{z^{s-1}e^{-az}}{1-e^{-z}}\right| \leq Ar^{M-1}e^{-ar},$$

on $A := 2e^{2\pi M}$ no depèn ni de $r \geq 1$ ni de s tal que $|s| \leq M$.

Ara, en γ_1, per a $|s| \leq M$, i com que $z = r$, podem escriure

$$\begin{aligned}\left|\int_{\gamma_1} \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz\right| &= \left|\int_{+\infty}^{\varepsilon} \frac{r^{s-1}e^{-ar}}{1-e^{-r}}dr\right| \\ &\leq \left|\int_{\varepsilon}^{1} \frac{r^{s-1}e^{-ar}}{1-e^{-r}}dr\right| + \left|\int_1^{+\infty} \frac{r^{s-1}e^{-ar}}{1-e^{-r}}dr\right| \\ &\leq \int_{\varepsilon}^{1} \frac{r^{\sigma-1}e^{-ar}}{1-e^{-r}}dr + A\int_1^{+\infty} r^{M-1}e^{-ar}dr,\end{aligned}$$

que ens permet assegurar que la integral és convergent. En efecte, per a $\varepsilon > 0$ la darrera integral impròpia és convergent i fitada per un nombre real que només depèn de a i M; l'altra integral de la darrera igualtat és la integral d'una funció fitada (per una fita que només depèn de a i M) en un interval tancat, de manera que és fitada per una constant que només depèn de a, M i ε.

Per a la integral que correspon a γ_3 podem procedir anàlogament a partir de la fita

$$\begin{aligned}\left|\int_{\gamma_3} \frac{z^{s-1}e^{-az}}{1-e^{-z}}dz\right| &= \left|\int_{\varepsilon}^{+\infty} \frac{r^{s-1}e^{2\pi i(s-1)}e^{-ar}}{1-e^{-r}}dr\right| \\ &\leq \left|\int_{\varepsilon}^{1} \frac{r^{s-1}e^{2\pi i(s-1)}e^{-ar}}{1-e^{-r}}dr\right| \\ &+ \left|\int_{1}^{+\infty} \frac{r^{s-1}e^{2\pi i(s-1)}e^{-ar}}{1-e^{-r}}dr\right| \\ &\leq \int_{\varepsilon}^{1} \frac{r^{\sigma-1}e^{-2\pi t}e^{-ar}}{1-e^{-r}}dr + A\int_{1}^{+\infty} r^{M-1}e^{-ar}dr.\end{aligned}$$

Per tant, la integral sobre els camins γ_1 i γ_3 és uniformement convergent en tot disc tancat $|s| \leq M$ i, en conseqüència, la integral $I_\varepsilon(s,a)$ és uniformement convergent en tot disc tancat de la forma $|z| \leq M$; això demostra (a).

Cal calcular $I(s,a)$ en el semiplà $\Re(s) > 1$. Per a això, observem que si $\Re(s) > 1$, aleshores podem escriure

$$\begin{aligned}I_\varepsilon(s,a) &= \int_{\gamma_1} z^{s-1}g(z)dz + \int_{\gamma_2} z^{s-1}g(z)dz + \int_{\gamma_3} z^{s-1}g(z)dz \\ &= \int_{+\infty}^{\varepsilon} r^{s-1}g(r)dr + \int_{\gamma_2} z^{s-1}g(z)dz + \int_{\varepsilon}^{+\infty} r^{s-1}e^{2\pi is}g(r)dr \\ &= (e^{2\pi is}-1)\int_{\varepsilon}^{+\infty} r^{s-1}g(r)dr + \int_{\gamma_2} z^{s-1}g(z)dz.\end{aligned}$$

Ja hem vist que el límit de la segona integral és zero; per tant, i com que la funció $I_\varepsilon(s,a)$ no depèn de ε, només cal calcular el límit de la primera. Ara bé, per definició, tenim que aquest límit és

$$(e^{2\pi is}-1)\int_{0}^{+\infty} r^{s-1}g(r)dr = (e^{2\pi is}-1)\Gamma(s)\zeta(s,a),$$

en virtut de la representació integral de la funció ζ de Hurwitz en el semiplà $\Re(s) > 1$ (cf. la proposició **13.2.5**). Per tant, obtenim la igualtat $I_\varepsilon(s,a) = (e^{2\pi is}-1)\Gamma(s)\zeta(s,a)$; i si tenim en compte les igualtats $e^{2\pi is} - 1 = 2ie^{\pi is}\sin(\pi s)$ i $\Gamma(s)\Gamma(1-s) = \dfrac{\pi}{\sin(\pi s)}$, obtenim la igualtat que volíem. □

Definició 13.3.2. Per a tot nombre complex s tal que $\Re(s) \leq 1$ i tot nombre real a, $0 < a \leq 1$, podem definir la funció zeta de Hurwitz per la fórmula $\zeta(s,a) := \Gamma(1-s)I(s,a)$.

En virtut de la proposició, la funció $\zeta(s,a)$ és una funció meromorfa de $\mathbb{C}$. En efecte, la funció $I(s,a)$ és una funció holomorfa de tot $\mathbb{C}$, mentre que la funció $\Gamma(1-s)$ és una funció meromorfa de $\mathbb{C}$, que només té pols simples en els enters $n \geq 1$; per tant, el producte $\zeta(s,a)$ és una funció meromorfa de $\mathbb{C}$ i els seus pols són simples i estan entre els enters $n \geq 1$.

Proposició 13.3.3. *Per a tot nombre real a tal que $0 < a \leq 1$, la funció zeta de Hurwitz té un únic pol, i simple, en $s = 1$. El residu de la funció en $s = 1$ és 1.*

DEMOSTRACIÓ: Cal veure que els enters $s \geq 2$ no són pols de $\zeta(s, a)$, fet que és evident a partir de l'expressió de $\zeta(s, a)$ com a suma de la sèrie $\sum_{n\geq 0}(n+a)^{-s}$, que defineix una funció analítica del semiplà $\Re(s) > 1$. Així, l'única possible singularitat de la funció $\zeta(s, a)$ és el punt $s = 1$. Cal veure que $s = 1$ resta com a pol de $\zeta(s, a)$ i calcular'n-hi el residu.

Per a això, calculem el valor de la funció $I(s, a)$ en $s = 1$; si demostrem que $I(1, a) \neq 0$, obtindrem que $s = 1$ és, efectivament, un pol de $\zeta(s, a)$. Si mantenim les notacions anteriors, per a tot nombre enter n podem fer explícit el valor de la integral de línia

$$I(n, a) = \frac{e^{-\pi i n}}{2\pi i} \int_\gamma \frac{z^{n-1}e^{-az}}{1 - e^{-z}} dz = \frac{(-1)^n}{2\pi i} \int_\gamma \frac{z^{n-1}e^{-az}}{1 - e^{-z}} dz.$$

La suma de les integrals sobre els camins γ_1 i γ_3 s'anul·la, ja que les integrals corresponents són, respectivament,

$$\int_{+\infty}^{\varepsilon} \frac{r^{n-1}e^{-ar}}{1 - e^{-r}} dr = -\int_{\varepsilon}^{+\infty} \frac{r^{n-1}e^{-ar}}{1 - e^{-r}} dr,$$

per al camí γ_1, i

$$\int_{\varepsilon}^{+\infty} \frac{r^{n-1}e^{2\pi i(n-1)}e^{-ar}}{1 - e^{-r}} dr = \int_{\varepsilon}^{+\infty} \frac{r^{n-1}e^{-ar}}{1 - e^{-r}} dr,$$

per al camí γ_3. Per tant,

$$I(n, a) = \frac{(-1)^n}{2\pi i} \int_{\gamma_2} \frac{z^{n-1}e^{-az}}{1 - e^{-z}} dz = (-1)^n \operatorname*{Res}_{z=0} \frac{z^{n-1}e^{-az}}{1 - e^{-z}}.$$

En particular, per a $n = 1$ podem escriure la igualtat

$$I(1, a) = -\lim_{z\to 0} \frac{ze^{-az}}{1 - e^{-z}} = -1.$$

Això demostra que $\zeta(s, a)$ té un pol en $s = 1$. Per últim, el càlcul del residu de la funció $\zeta(s, a)$ en $s = 1$ és senzill. Podem escriure

$$\lim_{s\to 1}(s - 1)\zeta(s, a) = -\lim_{s\to 1}(1 - s)\Gamma(1 - s)I(s, a) = -\lim_{s\to 1}\Gamma(2 - s)I(s, a) = 1,$$

ja que les funcions $I(s, a)$ i $\Gamma(2 - s)$ són contínues en $s = 1$ i totes dues valen 1. □

En particular, obtenim la prolongació meromorfa de la funció zeta de Riemann a tot el pla complex a partir de la fórmula $\zeta(s) := \Gamma(1 - s)I(s, 1)$. D'aquesta manera, la funció zeta de Riemann és una funció meromorfa de $\mathbb{C}$ amb un únic pol, i simple, en $s = 1$ i residu 1.

13.4 Polinomis de Bernoulli

L'objectiu d'aquesta secció és de fer el càlcul d'alguns valors de la funció zeta de Hurwitz; concretament, els valors $\zeta(n, a)$ per als nombres enters $n \leq -1$. Amb aquesta finalitat, introduïm els polinomis i els nombres de Bernoulli.

A la representació integral de la funció zeta de Hurwitz intervé de manera decisiva la funció donada per l'expressió $\dfrac{z^{s-1}e^{-az}}{1-e^{-z}} = \dfrac{z^{s-1}e^{(1-a)z}}{e^z-1}$. Aquesta expressió pot considerar-se formalment de la manera següent.

La sèrie de potències $\exp(z) := \displaystyle\sum_{n\geq 0}\frac{z^n}{n!} \in \mathbb{Q}[[z]]$ és tal que $(\exp(z)-1)z^{-1}$ és una sèrie invertible, ja que el seu terme constant és 1; per tant, $\dfrac{z}{\exp(z)-1} \in \mathbb{Q}[[z]]$. D'altra banda, si considerem x com una nova indeterminada, la sèrie $xz \in \mathbb{Q}[[x,z]]$ no té terme constant, de manera que té sentit considerar la sèrie substituïda $\exp(xz) \in \mathbb{Q}[[x,z]]$; i, en conseqüència, té sentit considerar la sèrie de potències de dues indeterminades

$$\frac{z\exp(xz)}{\exp(z)-1} \in \mathbb{Q}[[x,z]].$$

Així, per a tot nombre enter $n \geq 0$, existeix una única sèrie de potències $B_n(x) \in \mathbb{Q}[[x]]$ tal que

$$\frac{z\exp(xz)}{\exp(z)-1} = \sum_{n\geq 0}\frac{B_n(x)}{n!}z^n \in \mathbb{Q}[[x]][[z]].$$

Definició 13.4.1. S'anomena n-èsim nombre de Bernoulli, i es designa per B_n, el terme constant $B_n(0) \in \mathbb{Q}$ de la sèrie de potències $B_n(x)$.

Observació 13.4.2. Si fem $x = 0$ en la sèrie doble $\dfrac{z\exp(xz)}{\exp(z)-1}$, obtenim immediatament la igualtat $\dfrac{z}{\exp(z)-1} = \displaystyle\sum_{n\geq 0}\frac{B_n}{n!}z^n$, de manera que podríem haver definit els nombres de Bernoulli directament a partir d'aquesta sèrie. En particular, com que la sèrie $\exp(z)-1$ té coeficient dominant 1, obtenim immediatament el valor $B_0 = 1$.

Proposició 13.4.3. *Per a tot nombre enter $n \geq 0$, la sèrie $B_n(x)$ és, de fet, un polinomi mònic de $\mathbb{Q}[x]$; aquest polinomi admet l'expressió*

$$B_n(x) = \sum_{k=0}^{n}\binom{n}{k}B_k x^{n-k}, \qquad n \geq 2,$$

on B_k són els nombres de Bernoulli.

Demostració: La prova d'aquest resultat és completament formal. Per definició dels nombres de Bernoulli i de multiplicació de sèries de potències, obtenim la igualtat de sèries

$$\begin{aligned}\sum_{n\geq 0}\frac{B_n(x)}{n!}z^n = \frac{z}{\exp(z)-1}\exp(xz) &= \left(\sum_{n\geq 0}\frac{B_n}{n!}z^n\right)\sum_{n\geq 0}\frac{x^n z^n}{n!}\\ &= \sum_{n\geq 0}\left(\sum_{k=0}^{n}\frac{1}{k!(n-k)!}B_k x^{n-k}\right)z^n = \sum_{n\geq 0}\left(\sum_{k=0}^{n}\binom{n}{k}B_k x^{n-k}\right)\frac{z^n}{n!}.\end{aligned}$$

I per definició dels polinomis de Bernoulli les igualtats desitjades. □

Definició 13.4.4. El polinomi $B_n(x) \in \mathbb{Q}[x]$ s'anomena el n-èsim polinomi de Bernoulli.

Observació 13.4.5. Si interpretem B^k com B_k, podem expressar la igualtat anterior formalment en la forma $B_n(x) = (B + x)^n$, per a $n \geq 2$.

Proposició 13.4.6. *Per a tot nombre enter $n \geq 1$ se satisfà la igualtat*

$$B_n(x+1) = B_n(x) + nx^{n-1}.$$

DEMOSTRACIÓ: A partir de la definició, i com que la sèrie $(x+1)z$ no té terme constant, podem escriure les igualtats de sèries de potències

$$z\frac{\exp\left((x+1)z\right)}{\exp(z)-1} - z\frac{\exp\left(xz\right)}{\exp(z)-1} = z\exp(xz).$$

Ara, la definició dels polinomis de Bernoulli com a coeficients de les sèries del primer terme de la igualtat ens permet escriure les igualtats que volíem, $B_n(x+1) - B_n(x) = nx^{n-1}$, sense més que igualar els coeficients de z^n en els desenvolupaments en sèrie de potències. □

Si ara substituïm x per 0, obtenim una altra expressió per als nombres de Bernoulli.

Corol·lari 13.4.7. *Per a tot nombre enter $n \geq 2$ se satisfà que $B_n = B_n(0) = B_n(1)$.* □

Per últim, establirem una altra propietat dels nombres de Bernoulli, que és útil per al seu càlcul.

Corol·lari 13.4.8. *Per a tot enter $n \geq 2$ se satisfà la igualtat $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$.*

DEMOSTRACIÓ: Si substituïm $x = 1$ en la igualtat $B_n(x) = \displaystyle\sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$, vàlida per a $n \geq 2$, obtenim la nova expressió $B_n = B_n(1) = \displaystyle\sum_{k=0}^{n} \binom{n}{k} B_k$, que volíem veure. □

Observació 13.4.9. De nou, i amb el mateix conveni que hem fet servir més amunt, aquesta propietat es pot expressar formalment com $B_n = (B+1)^n$, per a $n \geq 2$.

Aquesta propietat ens permet calcular els nombres de Bernoulli recursivament. En efecte, la fórmula es pot escriure equivalentment en les formes successives

$$0 = \sum_{k=0}^{n-1} \binom{n}{k} B_k, \qquad B_{n-1} = \frac{-1}{n} \sum_{k=0}^{n-2} \binom{n}{k} B_k,$$

de manera que la igualtat per a n dóna el valor de B_{n-1} en funció dels anteriors. Només cal calcular a part el valor $B_0 = 1$, que és trivial a partir de la definició, com ja hem fet observar més amunt. De totes maneres, i per a acabar d'explicitar algunes de les propietats dels nombres de Bernoulli, observem que si canviem z per $-z$ en la sèrie de potències $f(z) := \dfrac{z}{\exp(z)-1} + \dfrac{z}{2}$, obtenim les igualtats

$$\begin{aligned} f(-z) &= \frac{-z}{\exp(-z)-1} - \frac{z}{2} = \frac{-z\exp(z)}{1-\exp(z)} - \frac{z}{2} = \frac{z\exp(z))}{\exp(z)-1} - \frac{z}{2} \\ &= \frac{z(\exp(z)-1)}{\exp(z)-1} + \frac{z}{\exp(z)-1} - \frac{z}{2} = \frac{z}{\exp(z)-1} + \frac{z}{2} = f(z), \end{aligned}$$

de manera que $f(z)$ és una sèrie parella, és a dir, no té termes no nuls de grau senar. En conseqüència, i com que els nombres de Bernoulli són definits per la sèrie $f(z) - \frac{z}{2}$, obtenim el resultat següent.

Corol·lari 13.4.10. *Per a tot nombre senar $n \geq 3$ és $B_n = 0$. A més a més, $B_1 = \frac{-1}{2}$.* □

Observació 13.4.11. A l'apèndix hi ha una taula amb els primers valors dels nombres de Bernoulli i una altra taula amb els primers polinomis.

A la demostració de la proposició **13.3.3** hem vist que, per a tot nombre enter n i per a tot nombre real a, $0 < a \leq 1$, podíem escriure la igualtat

$$I(n,a) = (-1)^n \operatorname*{Res}_{z=0} \frac{z^{n-1}e^{-az}}{1-e^{-z}}.$$

Aquesta igualtat ens permet calcular el valor de la funció zeta de Hurwitz en els nombres enters negatius en funció dels polinomis de Bernoulli.

Proposició 13.4.12. *Per a tot nombre enter $n \geq 0$ i tot nombre real a, $0 < a \leq 1$, se satisfà la igualtat $\zeta(-n,a) = -\frac{B_{n+1}(a)}{n+1}$, on $B_{n+1}(a)$ és el valor en a del $(n+1)$-èsim polinomi de Bernoulli.*

Demostració: Recordem que l'extensió de la funció zeta de Hurwitz a tot el pla complex és donada per la fórmula $\zeta(s,a) = \Gamma(1-s)I(s,a)$. En particular, per a tot nombre enter $n \geq 0$ podem escriure $\zeta(-n,a) = \Gamma(1+n)I(-n,a) = n!I(-n,a)$. Per tant, si tenim en compte que, en canviar z per $-z$ el residu canvia de signe, de la igualtat

$$I(-n,a) = (-1)^n \operatorname*{Res}_{z=0} \frac{z^{-n-1}e^{-az}}{1-e^{-z}} = \operatorname*{Res}_{z=0} \frac{z^{-n-1}e^{az}}{1-e^{z}}$$

obtenim l'expressió

$$\zeta(-n,a) = n! \operatorname*{Res}_{z=0} \frac{z^{-n-1}e^{az}}{1-e^{z}}. \tag{13.4.1}$$

El desenvolupament en sèrie de Laurent de l'expressió $\frac{z^{-n-1}e^{az}}{1-e^{z}} = z^{-n-2}\frac{ze^{az}}{1-e^{z}}$ dóna, per definició dels polinomis de Bernoulli, que $-z^{-n-2}\sum_{k\geq 0}\frac{B_k(a)}{k!}z^k$, de manera que el residu en $z=0$ d'aquesta funció és el coeficient de z^{n+1} de la sèrie $-\sum_{k\geq 0}\frac{B_k(a)}{k!}z^k$; és a dir, $-\frac{B_{n+1}(a)}{(n+1)!}$. Si duem això a la fórmula (13.4.1), obtenim la igualtat $\zeta(-n,a) = -\frac{B_{n+1}(a)}{n+1}$, que desitjàvem. □

Observació 13.4.13. En tot el procés no ha calgut en cap moment utilitzar que la sèrie de potències $\frac{z\exp(xz)}{\exp(z)-1} = \sum_{n\geq 0}\frac{B_n(x)}{n!}z^k$ tingui radi de convergència estrictament positiu en $\mathbb{C}$, llevat d'aquest darrer punt en què hem utilitzat aquesta sèrie com a desenvolupament en sèrie de potències de la funció de la qual volem calcular el residu en $z=0$. De totes

maneres, com que la funció $e^z - 1$ no s'anul·la en el disc obert $\Re(z) < 2\pi$, el radi de convergència és $\geq 2\pi$, fet que garanteix la legitimitat del procés, fins i tot pensant que tot el que s'ha fet s'hagués fet amb la funció $\dfrac{ze^{xz}}{e^z - 1}$ en lloc de la sèrie formal.

Corol·lari 13.4.14. *Els valors de la funció zeta de Riemann en els nombres enters negatius són donats per les fórmules*

$$\zeta(0) = -\frac{1}{2}, \qquad \zeta(-2n) = 0, \qquad \zeta(1-2n) = -\frac{B_{2n}}{2n}, \qquad n \geq 1.$$

Demostració: Només cal tenir en compte que $\zeta(s) = \zeta(s, 1)$, per a tot nombre complex s, i que $B_{2n} = B_{2n}(1)$ i $B_{2n+1} = 0$, per a tot $n \geq 1$. □

Observem que, en particular, obtenim que la funció zeta de Riemann s'anul·la en tots els nombres enters parells negatius. De fet, una cèlebre conjectura de Riemann, datada en 1859 (cf. [Rie 1859]) i coneguda amb el nom d'hipòtesi de Riemann, afirma que, a part d'aquests, que són els anomenats els zeros "trivials", els altres zeros de la funció estan tots a la recta vertical donada per l'equació $\Re(s) = \dfrac{1}{2}$. Per a una versió en català i amb comentaris, cf. [B-G-T 12].

13.5 El teorema de Clausen-von Staudt

El teorema de Clausen-von Staudt proporciona un control absolut dels denominadors dels nombres de Bernoulli; de fet, ens dóna exactament el seu valor. Aquest resultat és bàsic per a dur a terme la interpolació p-àdica dels valors de la funció zeta de Hurwitz en els nombres enters negatius. Comencem per provar dos resultats previs.

Lema 13.5.1. *Siguin $m, n \in \mathbb{Z}$, $m \geq 1$, $n \neq 1$. Aleshores, $B_n = m^{n-1} \displaystyle\sum_{a=1}^{m} B_n\left(\frac{a}{m}\right)$.*

Demostració: Per a tot nombre enter a, $1 \leq a \leq m$, és $\dfrac{a}{m} \in \mathbb{Q}$, $0 < \dfrac{a}{m} \leq 1$; per tant, té sentit considerar el valor dels polinomis de Bernoulli en $\dfrac{a}{m}$ i és $B_n\left(\dfrac{a}{m}\right) \in \mathbb{Q}$. En conseqüència, podem considerar la sèrie de potències $f(z) := \displaystyle\sum_{n\geq 0} \frac{m^{n-1}\sum_{a=1}^{m} B_n\left(\frac{a}{m}\right)}{n!} z^n$, de coeficients racionals. A l'anell $\mathbb{Q}[[z]]$, podem escriure les igualtats

$$\begin{aligned} f(z) &= \sum_{a=1}^{m}\sum_{n\geq 0} \frac{m^{n-1}B_n\left(\frac{a}{m}\right)}{n!} z^n = \frac{1}{m}\sum_{a=1}^{m}\sum_{n\geq 0} \frac{B_n\left(\frac{a}{m}\right)}{n!}(mz)^n = \frac{1}{m}\sum_{a=1}^{m} \frac{(mz)\exp\left(\frac{a}{m}mz\right)}{\exp(mz)-1} \\ &= \frac{z}{\exp(mz)-1}\sum_{a=1}^{m}\exp(az) = \frac{z}{\exp(mz)-1}\exp(z)\frac{\exp(mz)-1}{\exp(z)-1} = \frac{z\exp(z)}{\exp(z)-1} \\ &= \sum_{n\geq 0}\frac{B_n(1)}{n!}z^n. \end{aligned}$$

En igualar els coeficients, obtenim que, per a tot nombre enter $n \geq 0$, se satisfà la igualtat $B_n(1) = m^{n-1} \sum_{a=1}^{m} B_n\left(\frac{a}{m}\right)$. I, com que per a $n \neq 1$ és $B_n = B_n(1)$, obtenim la igualtat que volíem provar. □

Lema 13.5.2. *Sigui $\mathbb{F}_q$ el cos finit de q elements. Aleshores, per a tot nombre enter $n \geq 1$, se satisfà la igualtat* $\sum_{a \in \mathbb{F}_q} a^n = \begin{cases} 0, & \text{si } q-1 \text{ no divideix } n, \\ -1, & \text{si } q-1 \text{ divideix } n. \end{cases}$

Demostració: El grup multiplicatiu $\mathbb{F}_q{}^*$ és cíclic d'ordre $q-1$; per tant, en el cas que $q-1$ no divideix n, hi ha un element $b \in \mathbb{F}_q{}^*$ tal que $b^n \neq 1$. En aquest cas podem escriure

$$\sum_{a \in \mathbb{F}_q} a^n = \sum_{a \in \mathbb{F}_q} (ab)^n = b^n \sum_{a \in \mathbb{F}_q} a^n; \qquad \text{i, per tant,} \qquad \sum_{a \in \mathbb{F}_q} a^n = 0.$$

En el cas que $q-1$ divideix n, per a $a \in \mathbb{F}_q$, $a \neq 0$, és $a^n = 1$, de manera que tenim la igualtat $\sum_{a \in \mathbb{F}_q} a^n = \sum_{a \in \mathbb{F}_q{}^*} a^n = q - 1 = -1$, com volíem demostrar. □

Amb aquests resultats previs, podem procedir a la prova del teorema següent.

Teorema 13.5.3 (Clausen-von Staudt)**.** *Per a tot nombre enter $n \geq 1$,*

$$B_{2n} + \sum_{\substack{p-1 \mid 2n \\ p,\ primer}} \frac{1}{p} \in \mathbb{Z}.$$

Demostració: Per a tot nombre primer p, notarem per $\mathbb{Z}_{(p)}$ l'anell localitzat de $\mathbb{Z}$ en l'ideal primer $p\mathbb{Z}$. El lema **13.5.1** ens permetrà demostrar per inducció sobre n que, per a $n \geq 0$, és $pB_{2n} \in \mathbb{Z}_{(p)}$. En efecte, per a $n = 0$ és $B_{2n} = 1$, de manera que el resultat és clar. D'altra banda, per a tot $n \geq 1$, podem escriure $B_{2n} = p^{2n-1} \sum_{a=1}^{p} B_{2n}\left(\frac{a}{p}\right)$, de manera que, si tenim en compte que $B_{2n}\left(\frac{a}{p}\right) = \sum_{k=0}^{2n} \binom{2n}{k} \frac{a^{2n-k}}{p^{2n-k}} B_k$, podem escriure la igualtat $B_{2n} = \sum_{a=1}^{p} \sum_{k=0}^{2n} \binom{2n}{k} B_k a^{2n-k} p^{k-1}$. Si suposem que, per a $k < n$, és $pB_{2k} \in \mathbb{Z}_{(p)}$, aleshores,

$$\begin{aligned} B_{2n} &= \frac{1}{p} \sum_{a=1}^{p} \sum_{k=0}^{2n} \binom{2n}{k} B_k a^{2n-k} p^k \\ &= \frac{1}{p} \sum_{a=1}^{p} \left(B_0 a^{2n} + 2np B_1 a^{2n-1} + \sum_{k=1}^{n} \binom{2n}{2k} B_{2k} a^{2n-2k} p^{2k} \right) \\ &= \sum_{a=1}^{p} \left(pB_0 a^{2n} p^{-2} + 2np B_1 a^{2n-1} p^{-1} + \sum_{k=1}^{n} \binom{2n}{2k} pB_{2k} a^{2n-2k} p^{2k-2} \right), \end{aligned}$$

ja que els nombres de Bernoulli $B_3, B_5, \ldots B_{2n-1}$ són nuls.

Ara, per la hipòtesi d'inducció, és $\sum_{k=1}^{n-1}\binom{2n}{2k}a^{2n-k}p^{2k-1}B_{2k}\in\mathbb{Z}_{(p)}$, de manera que $B_{2n}-\sum_{a=1}^{p}\left(pB_0a^{2n}p^{-2}+2npB_1a^{2n-1}p^{-1}+pB_{2n}p^{2n-2}\right)\in\mathbb{Z}_{(p)}$. Però també se satisfà que $\sum_{a=1}^{p}2npB_1a^{2n-1}p^{-1}=2nB_1\sum_{a=1}^{p}a^{2n-1}=-n\sum_{a=1}^{p}a^{2n-1}\in\mathbb{Z}$, i s'obté que

$$B_{2n}-\sum_{a=1}^{p}(pB_0a^{2n}p^{-2}+pB_{2n}p^{2n-2})\in\mathbb{Z}_{(p)};\quad\text{és a dir, que}\quad(1-p^{2n})B_{2n}-\frac{1}{p}\sum_{a=1}^{p}a^{2n}\in\mathbb{Z}_{(p)}.$$

Ara, el lema **13.5.2** ens permet deduir immediatament que, si $p-1$ divideix $2n$, aleshores $(1-p^{2n})B_{2n}+\frac{1}{p}\in\mathbb{Z}_{(p)}$ i, que si $p-1$ no divideix $2n$, aleshores $(1-p^{2n})B_{2n}\in\mathbb{Z}_{(p)}$. En el primer cas, $p(1-p^{2n})B_{2n}+1\in p\mathbb{Z}_{(p)}$, de manera que $p(1-p^{2n})B_{2n}\in\mathbb{Z}_{(p)}^*$ i, com que $(1-p^{2n})\in\mathbb{Z}_{(p)}^*$, també $pB_{2n}\in\mathbb{Z}_{(p)}^*$. En particular, $p^{2n}B_{2n}\in\mathbb{Z}_{(p)}$ i $pB_{2n}+1\in p\mathbb{Z}_{(p)}$. En l'altre cas, $B_{2n}\in\mathbb{Z}_{(p)}$, ja que $1-p^{2n}\in\mathbb{Z}_{(p)}^*$.

Ara podem acabar la demostració fàcilment. Per a tot nombre primer ℓ, obtenim que $B_{2n}+\sum_{p-1|2np,\text{ primer}}\frac{1}{p}\in\mathbb{Z}_{(\ell)}$, ja que els quocients $\frac{1}{p}$ són elements de $\mathbb{Z}_{(\ell)}$ per a tot $\ell\neq p$. I com que $\mathbb{Z}$ és la intersecció de tots els anells $\mathbb{Z}_{(\ell)}$, $B_{2n}+\sum_{p-1|2np,\text{ primer}}\frac{1}{p}\in\mathbb{Z}$. □

Corol·lari 13.5.4. *Per a tot nombre enter $n\geq 1$, el denominador del nombre de Bernoulli B_{2n}, considerat com a nombre racional, és el producte dels nombres primers p tals que $p-1$ divideix $2n$.* □

En particular, tots els denominadors són múltiples de 6.

13.6 Interpolació p-àdica de la funció zeta de Hurwitz

L'objectiu final d'aquest capítol és de procedir a fer la interpolació p-àdica d'alguns valors de la funció zeta de Hurwitz. Concretament, volem construir una funció meromorfa p-àdica tal que per als enters negatius, i mòdul un factor conegut, coincideixi amb els valors de la funció zeta de Hurwitz.

Per a això, i per comoditat, convé començar per fer una lleugera modificació de la funció zeta de Hurwitz.

Definició 13.6.1. Donats un nombre complex s i nombres enters a, F tals que $1\leq a\leq F$, posarem $H_\infty(s,a,F):=F^{-s}\zeta\left(s,\frac{a}{F}\right)$, on ζ és la funció zeta de Hurwitz.

Observació 13.6.2. Se satisfan les igualtats, per a $\Re(s)>1$,

$$H_\infty(s,a,F)=\sum_{m\equiv a\pmod F,m>0}m^{-s}=\sum_{n\geq 0}(a+nF)^{-s}.$$

En conseqüència, $H_\infty(s,a,F)$ és una funció meromorfa de $\mathbb{C}$ amb un únic pol, i simple, en $s=1$, i amb residu F^{-1} en aquest punt. El càlcul dels valors de la funció zeta de Hurwitz en els nombres enters negatius ens permet escriure immediatament el resultat següent.

Corol·lari 13.6.3. *Per a tot nombre enter $n \geq 1$ se satisfà la igualtat*

$$H_\infty(1-n,a,F) = -F^{n-1}\frac{B_n\left(\frac{a}{F}\right)}{n} \in \mathbb{Q}. \square$$

Per a procedir a la interpolació ens cal estudiar, encara, una funció p-àdica concreta.

Per a tot nombre primer p, posarem $q := \begin{cases} p, & \text{si } p \neq 2, \\ 4, & \text{si } p = 2. \end{cases}$ Recordem que, amb aquestes notacions, donat un nombre enter p-àdic invertible qualsevol, a, existeix una arrel $\varphi(q)$-èsima de la unitat única, no necessàriament primitiva, $\omega(a)$, tal que $a \equiv \omega(a) \pmod q$. Aleshores, podem posar $\langle a\rangle := \omega(a)^{-1}a \equiv 1 \pmod q$ i definir $\langle a\rangle^s := \exp(s\log_p\langle a\rangle)$. La funció $s \mapsto \langle a\rangle^s$ està ben definida per un desenvolupament en sèrie de potències convergent per a tot element $s \in \mathbb{C}_p$ tal que $|s|_p < qp^{\frac{-1}{p-1}}$.

En efecte. Com que $\langle a\rangle = 1 + (\langle a\rangle - 1)$ i $|\langle a\rangle - 1|_p \leq q^{-1} < p^{\frac{-1}{p-1}}$, és $|\log_p\langle a\rangle|_p \leq q^{-1}$, de manera que si $|s|_p < qp^{\frac{-1}{p-1}}$, aleshores $|s\log_p\langle a\rangle|_p < p^{\frac{-1}{p-1}}$ i la sèrie exponencial és convergent en $s\log_p\langle a\rangle$.

Observem, a més a més, que $qp^{\frac{-1}{p-1}} > 1$ i, en conseqüència, que la funció $\langle a\rangle^s$ és analítica p-àdica en el disc de $\mathbb{C}_p$ definit per la condició $|s|_p < qp^{\frac{-1}{p-1}}$. En particular, és un exercici senzill d'anàlisi p-àdica provar que es té el desenvolupament en sèrie de potències $\langle a\rangle^s = \sum_{n\geq 0}\binom{s}{n}(\langle a\rangle - 1)^n$, on, per definició, escrivim $\binom{s}{n} := \dfrac{s(s-1)\cdots(s-n+1)}{n!}$.

Amb aquests preliminars, podem procedir a la demostració del resultat següent.

Proposició 13.6.4. *Siguin $a, F \in \mathbb{Z}$, $1 \leq a \leq F$, i p un nombre primer. Suposem que p no divideix a i que q divideix F. Aleshores, existeix una funció meromorfa p-àdica $H_p(s,a,F)$, definida en el disc $|s|_p < qp^{\frac{-1}{p-1}}$, tal que per a tot nombre enter $n \geq 1$ és $H_p(1-n,a,F) = \omega(a)^{-n}H_\infty(1-n,a,F)$, on aquesta darrera funció és la funció complexa de més amunt.*

Demostració: Com que $qp^{\frac{-1}{p-1}} > 1$, la condició $|s|_p < qp^{\frac{-1}{p-1}}$ és equivalent a la condició $|1-s|_p < qp^{\frac{-1}{p-1}}$. Definim $H_p(s,a,F) := \dfrac{1}{s-1}\dfrac{1}{F}\langle a\rangle^{1-s}\displaystyle\sum_{k\geq 0}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k$, on B_k són els nombres de Bernoulli.

En virtut del teorema de Clausen-von Staudt, per a tot nombre enter $k \geq 0$ i tot nombre primer p, és $pB_k \in \mathbb{Z}_p$, de manera que $|pB_k|_p \leq 1$. Això ens permet assegurar que

$$\left|\left(\frac{F}{a}\right)^k B_k\right|_p \leq |p|_p^{-1}|q|_p^k = p|q|_p^k, \tag{13.6.1}$$

ja que, per hipòtesi, q divideix F i p no divideix a. En conseqüència, la sèrie

$$\sum_{k\geq 0}\binom{s}{k}\left(\frac{F}{a}\right)^k B_k \tag{13.6.2}$$

defineix una funció analítica p-àdica en el disc $|s|_p < qp^{\frac{-1}{p-1}}$. En efecte, la fita anterior dels coeficients, (13.6.1), ens permet assegurar (exercici) que la funció definida per la sèrie (13.6.2) és el límit uniforme, en aquest disc, de les sumes parcials de la sèrie; i aquestes sumes parcials són funcions analítiques de tot $\mathbb{C}_p$.

Ara, com que la funció $\langle a\rangle^s$ també és analítica en aquest disc, ho és el seu producte per l'anterior i, per tant, la funció $(-s)H_p(1-s,a,F)$ és analítica p-àdica en $|s|_p < qp^{\frac{-1}{p-1}}$. Però ja hem vist que el disc $|s|_p < qp^{\frac{-1}{p-1}}$ coincideix amb el disc $|1-s|_p < qp^{\frac{-1}{p-1}}$, de manera que la funció $(s-1)H_p(s,a,F)$ és analítica. Això demostra la meromorfia de $H_p(s,a,F)$.

El final de la prova és senzill. Si canviem s per $1-n$ i tenim en compte les desigualtats $|1-n|_p \leq 1 < qp^{\frac{-1}{p-1}}$, podem sumar la sèrie i obtenim la igualtat

$$\begin{aligned}
H_p(1-n,a,F) &= \frac{-1}{nF}\langle a\rangle^n \sum_{k\geq 0}\binom{n}{k}\left(\frac{F}{a}\right)^k B_k \\
&= \frac{-1}{nF}\langle a\rangle^n \sum_{k=0}^{n}\binom{n}{k}\left(\frac{F}{a}\right)^k B_k \\
&= \frac{-1}{nF}\langle a\rangle^n \sum_{k=0}^{n}\binom{n}{k}\left(\frac{a}{F}\right)^{-k} B_k \\
&= \frac{-1}{nF}\langle a\rangle^n \left(\frac{F}{a}\right)^n \sum_{k=0}^{n}\binom{n}{k}\left(\frac{a}{F}\right)^{n-k} B_k \\
&= \frac{-1}{nF}\langle a\rangle^n \left(\frac{F}{a}\right)^n B_n\left(\frac{a}{F}\right) \\
&= \frac{-F^{n-1}\omega(a)^{-n}}{n} B_n\left(\frac{a}{F}\right) \\
&= \omega(a)^{-n} H_\infty(1-n,a,F),
\end{aligned}$$

com volíem demostrar. □

Observació 13.6.5. Recordem que la funció $H_\infty(s,a,F)$ és la funció definida per la igualtat $H_\infty(s,a,F) = F^{-s}\zeta\left(s,\frac{a}{F}\right)$; per tant, obtenim la nova igualtat

$$H_p(1-n,a,F)\omega(a)^n F^{1-n} = \zeta\left(1-n,\frac{a}{F}\right),$$

que és la interpolació pròpiament dita dels valors de la funció ζ de Hurwitz de paràmetre $\frac{a}{F}$ en els enters $1-n$, $n\geq 1$. Observem que només té sentit considerar valors racionals de $\frac{a}{F}$, ja que podem incloure $\mathbb{Q}$ en $\mathbb{Q}_p$ i, per tant, en $\mathbb{C}_p$, però no podem incloure, de manera natural, $\mathbb{R}$ en $\mathbb{C}_p$. A més a més, la interpolació es produeix per als casos particulars de $\frac{a}{F}$ tals que q divideix F i p no divideix a.

Capítol 14

El teorema de Dirichlet de la progressió aritmètica

L'objectiu d'aquest capítol és donar la demostració del teorema de Dirichlet de la progressió aritmètica. Aquest resultat ja ha estat usat, en una forma feble, en la prova del teorema de Hasse-Minkowski; però no se n'ha donat cap demostració, ni tan sols d'aquella forma feble.

14.1 Funció zeta associada a un conjunt de nombres primers

Abans de poder enunciar de manera precisa el teorema de Dirichlet de la progressió aritmètica, cal estudiar el concepte de densitat d'un conjunt de nombres primers. I, per a dur a terme aquest estudi, cal introduir la funció zeta associada a un conjunt de nombres primers. L'objectiu d'aquesta secció és, doncs, fer l'estudi d'aquesta funció.

Definició 14.1.1. Sigui A un conjunt de nombres primers. Podem considerar la sèrie de Dirichlet $\zeta_A(s) := \sum_{p\in A} p^{-s}$; s'anomena la sèrie zeta associada al conjunt A.

El criteri de comparació de sèries de nombres reals positius, aplicat a les sèries $\zeta_A(s)$ i $\zeta(s)$, ens permet obtenir de seguida que, per a tot conjunt A de nombres primers, la sèrie $\zeta_A(s)$ és absolutament convergent en el semiplà definit per la condició $\Re(s) > 1$. El primer resultat que provarem fa referència al conjunt $A = P$ de tots els nombres primers.

Observem, en primer lloc, que la funció $\zeta_P(s)$ està definida per a tot nombre real $s > 1$ per la sèrie convergent $\zeta_P(s) = \sum_{p\in P} p^{-s}$ i que, en la semirecta $s \in \mathbb{R}$, $s > 1$, la funció $\zeta_P(s)$ és analítica real. Això es dedueix fàcilment de l'estudi de les sèries de Dirichlet que hem fet en el capítol **12**.

Proposició 14.1.2. *Si* $\log(s)$ *designa el logaritme real, aleshores* $\lim_{s\to 1^+} \dfrac{\zeta_P(s)}{\log(s-1)^{-1}} = 1$, *en el sentit que el límit existeix i val* 1.

DEMOSTRACIÓ: Considerem la funció zeta de Riemann i la seva expressió en forma de producte d'Euler $\zeta(s) = \prod_{p\in P}(1-p^{-s})^{-1}$, convergent en el semiplà complex $\Re(s) > 1$. Si prenem la determinació principal del logaritme, és a dir, la determinació que fa $\log(s) \in \mathbb{R}$ quan $s \in \mathbb{R}$, $s > 0$, obtenim la igualtat $\log\zeta(s) = \sum_{p\in P} -\log(1-p^{-s}) = \sum_{p\in P}\sum_{k\geq 1}\frac{1}{kp^{ks}}$, vàlida per a tot nombre complex tal que $\Re(s) > 1$. En particular, la igualtat és vàlida per a tot nombre real $s > 1$. Per a tot nombre real $s > 1$, posem $\psi(s) := \sum_{p\in P}\sum_{k\geq 2}\frac{1}{kp^{ks}}$. La sèrie és una parcial de la sèrie anterior, de manera que també és absolutament convergent per a $s > 1$ i se satisfà la igualtat $\log\zeta(s) = \sum_{p\in P} p^{-s} + \psi(s) = \zeta_P(s) + \psi(s)$. No només això, sinó que la convergència absoluta ens permet escriure les desigualtats

$$\psi(s) \leq \sum_{p\in P}\sum_{k\geq 2}\frac{1}{p^{ks}} = \sum_{p\in P}\frac{1}{p^s(p^s-1)} \leq \sum_{p\in P}\frac{1}{p(p-1)} \leq \sum_{n\geq 1} n^{-2},$$

fet que demostra que la sèrie és fitada per una constant independent de s.

D'altra banda, si tenim en compte que la funció zeta de Riemann és meromorfa amb un únic pol, i simple, en $s = 1$, i que el residu de la funció en aquest punt és 1, obtenim que $\lim_{s\to 1^+}(s-1)\zeta(s) = 1$, de manera que, en prendre logaritmes, $\lim_{s\to 1^+}\log\zeta(s) - \log(s-1)^{-1} = 0$. Per tant, podem escriure que $\zeta_P(s) = \log(s-1)^{-1} + \lambda(s)$, per a una funció $\lambda(s)$ fitada en un entorn de $s = 1$. Això acaba la demostració. □

Definició 14.1.3. Siguin A un conjunt qualsevol de nombres primers i δ_A un nombre real. Es diu que A té densitat de Dirichlet δ_A quan existeix el límit $\lim_{s\to 1^+}\frac{\sum_{p\in A} p^{-s}}{\log(s-1)^{-1}}$ i és igual a δ_A.

Clarament, si aquest límit existeix ha de ser no negatiu i menor o igual que 1; de manera que la densitat de Dirichlet, si existeix, és un nombre $0 \leq \delta_A \leq 1$. D'altra banda, si A és finit, aleshores $\delta_A = 0$, de manera que hem provat el resultat següent.

Corol·lari 14.1.4. *Si existeix* $\lim_{s\to 1^+}\frac{\zeta_A(s)}{\log(s-1)^{-1}}$ *i és no nul, aleshores A és un conjunt infinit.* □

Ara podem enunciar el teorema de la progressió aritmètica en una forma més forta que la que s'ha fet servir; i que és la forma en què el demostrarem.

Teorema 14.1.5 (Dirichlet)**.** *Siguin $a, m \in \mathbb{Z}$ tals que $m \geq 1$ i $\operatorname{mcd}(a,m) = 1$. El conjunt dels nombres primers de la forma $a + \lambda m$, $\lambda \in \mathbb{Z}$, té densitat de Dirichlet $\frac{1}{\varphi(m)}$, on φ és la funció d'Euler. En particular, és infinit.*

14.2 Funcions L de Dirichlet

Tot i que les funcions L de Dirichlet ja han estat definides en el capítol **12**, és ara el moment de fer-ne un estudi més acurat. Recordem-ne la definició.

Definició 14.2.1. Sigui χ un caràcter de Dirichlet mòdul m. S'anomena sèrie L de Dirichlet associada al caràcter χ la sèrie $L(\chi, s) := \sum_{n\geq 1} \chi(n)n^{-s}$, absolutament convergent en el semiplà $\Re(s) > 1$, on defineix una funció analítica de s.

Observem que, si, per a tot nombre enter n, posem $\chi_1(n) = 1$, la funció definida per aquesta sèrie és exactament la funció zeta de Riemann; per tant, admet un desenvolupament en producte d'Euler. De fet, aquest resultat és general per a tots els caràcters de Dirichlet; el resultat següent ja ha estat provat en el corol·lari **12.4.3**.

Proposició 14.2.2. *Sigui χ un caràcter de Dirichlet mòdul m. Aleshores, el producte infinit $\prod_p (1-\chi(p)p^{-s})^{-1}$ és absolutament convergent en el semiplà $\Re(s) > 1$ i el seu valor coincideix amb el de la funció $L(\chi, s)$ en aquest semiplà.* □

Observació 14.2.3. Si considerem el caràcter trivial definit mòdul m, χ_1, no obtenim la funció zeta de Riemann; en efecte, el caràcter s'anul·la en tots els enters divisibles per algun nombre primer que divideix m, de manera que la igualtat que obtenim és exactament $L(s, \chi_1) = \zeta(s)\prod_{p|m}(1 - p^{-s})$.

Teorema 14.2.4. *Sigui χ un caràcter de Dirichlet qualsevol mòdul m.*

(a) *Si $\chi = \chi_1$ és el caràcter trivial, aleshores la funció $L(\chi_1, s)$ admet una prolongació meromorfa a tot $\mathbb{C}$ amb un únic pol, i simple, en $s = 1$, i amb residu $\dfrac{\varphi(m)}{m}$ en aquest punt.*

(b) *Si χ no és el caràcter trival, aleshores la funció $L(\chi, s)$ s'estén de manera única a una funció entera del pla complex.*

(c) *Si χ no és el caràcter trival, aleshores la sèrie $\sum_{n\geq 1} \chi(n)n^{-s}$ és convergent en $\Re(s) > 0$; en particular, el valor de la funció en $s = 1$ es pot calcular, encara que la convergència no és absoluta, a partir de la igualtat $L(\chi, 1) = \sum_{n\geq 1} \chi(n)n^{-1}$.*

Demostració: Comencem per relacionar la funció $L(\chi, s)$ amb la funció zeta de Hurwitz. Per a això, observem que, si $s \in \mathbb{C}$ és tal que $\Re(s) > 1$, aleshores podem escriure, gràcies a la convergència absoluta, les igualtats

$$\begin{aligned} L(\chi, s) &= \sum_{n\geq 1} \chi(n)n^{-s} = \sum_{r=1}^{m} \sum_{q\geq 0} \chi(r + qm)(r + qm)^{-s} \\ &= m^{-s} \sum_{r=1}^{m} \chi(r) \sum_{q\geq 0} \left(\frac{r}{m} + q\right)^{-s} = m^{-s} \sum_{r=1}^{m} \chi(r)\zeta\left(s, \frac{r}{m}\right), \end{aligned}$$

de manera que la funció $L(\chi, s)$ és, llevat del factor m^{-s}, que només depèn del mòdul de definició del caràcter χ, combinació lineal de funcions zeta de Hurwitz i de coeficients que només depenen del caràcter. Per les propietats conegudes de la funció zeta de Hurwitz, obtenim que la funció $L(\chi, s)$ es pot prolongar a una funció meromorfa de tot el pla complex amb, com a màxim, un pol i simple en $s = 1$.

Ara, el càlcul del límit $\lim_{s\to 1}(s-1)L(\chi,s)$ es pot escriure de la forma

$$\lim_{s\to 1}(s-1)L(\chi,s)=\lim_{s\to 1}(s-1)m^{-s}\sum_{r=1}^{m}\chi(r)\zeta\left(s,\frac{r}{m}\right)=\frac{1}{m}\sum_{r=1}^{m}\chi(r)\lim_{s\to 1}(s-1)\zeta\left(s,\frac{r}{m}\right)$$
$$=\frac{1}{m}\sum_{r=1}^{m}\chi(r)=\begin{cases}\dfrac{\varphi(m)}{m}, & \text{si } \chi=\chi_1 \text{ és el caràcter trivial,}\\ 0, & \text{si } \chi\neq\chi_1.\end{cases}$$

En conseqüència, si $\chi\neq\chi_1$, aleshores la funció $L(\chi,s)$ no té pol en $s=1$, de manera que és una funció entera. I això demostra (b). D'altra banda, per a $\chi=\chi_1$, la mateixa igualtat ens ensenya que $L(\chi,s)$ té un pol simple en $s=1$ i que el residu de la funció en aquest pol és $\dfrac{\varphi(m)}{m}$; i això demostra (a).

Resta per veure que el valor de la funció $L(\chi,s)$ en $s=1$ es pot calcular com la suma de la sèrie $L(\chi,1)=\sum_{n\geq 1}\chi(n)n^{-1}$, si $\chi\neq\chi_1$. I per a això només cal veure que la sèrie és convergent. Observem però, que els coeficients $\chi(n)$ formen una successió periòdica; i, per tant, fitada. Encara més, per a $1\leq j<k$, és $\left|\sum_{n=j}^{k}\chi(n)\right|\leq\varphi(m)$, ja que, per a tot enter $j\geq 1$, se satisfà la igualtat $\sum_{n=j}^{j+m-1}\chi(n)=0$ i el caràcter χ només pren valors no nuls, que són arrels de la unitat, per a $\varphi(m)$ enters diferents en cada interval $j\leq n\leq j+m-1$. En conseqüència, podem aplicar el següent resultat que acaba la prova. □

Lema 14.2.5. *Sigui $F(s):=\sum_{n\geq 1}f(n)n^{-s}$ una sèrie de Dirichlet. Suposem que existeix un nombre real $C>0$ tal que, per a tota parella de nombres enters $1\leq j<k$, se satisfà que $\left|\sum_{n=j}^{k}f(n)\right|\leq C$. Aleshores, la sèrie $F(s)$ és convergent en el semiplà $\Re(s)>0$.*

Demostració: Exercici. □

Per a acabar aquesta secció, demostrarem un resultat que ens assegura que les funcions $L(\chi,s)$ no s'anul·len en $s=1$. Concretament, ho deduirem del resultat següent.

Proposició 14.2.6. *Sigui $m\geq 2$ un nombre enter qualsevol. Per a tot nombre complex s, posem $\zeta_m(s):=\prod_{\chi\in G(m)\widehat{\ }}L(\chi,s)$, on $G(m):=(\mathbb{Z}/m\mathbb{Z})^*$ és el grup dels elements invertibles de $\mathbb{Z}/m\mathbb{Z}$, i $G(m)\widehat{\ }$ designa el grup dels caràcters de Dirichlet mòdul m. Aleshores, $\zeta_m(s)$ és una funció meromorfa de tot $\mathbb{C}$ tal que, en el semiplà $\Re(s)>1$, es pot escriure com el producte convergent $\zeta_m(s)=\prod_{p\nmid m}(1-p^{-f_p s})^{-g_p}$, on f_p és el nombre enter més petit $f_p\geq 1$ tal que m divideix $p^{f_p}-1$, i g_p és definit per la igualtat $f_p g_p=\varphi(m)$.*

Demostració: Donat un nombre primer p que no divideix m, sigui W el conjunt de totes les arrels f_p-èsimes de la unitat de $\mathbb{C}$. Per definició, obtenim la igualtat

$$1-T^{f_p}=\prod_{w\in W}(1-wT)\in\mathbb{C}[T].$$

A més a més, la definició de f_p ens permet assegurar que el subgrup multiplicatiu de $G(m)$ generat per la classe del nombre enter p en $\mathbb{Z}/m\mathbb{Z}$ és d'ordre f_p.

D'altra banda, disposem de la successió exacta dels grups de caràcters

$$1 \longleftarrow \langle p\rangle\widehat{\ } \longleftarrow G(m)\widehat{\ } \longleftarrow (G(m)/\langle p\rangle)\widehat{\ } \longleftarrow 1,$$

que s'obté a partir de la successió exacta

$$1 \longrightarrow \langle p\rangle \longrightarrow G(m) \longrightarrow G(m)/\langle p\rangle \longrightarrow 1.$$

Com que l'ordre de $(G(m)/\langle p\rangle)\widehat{\ }$ és exactament $\dfrac{\varphi(m)}{f_p} = g_p$, obtenim que tot caràcter d'ordre f_p es pot interpretar com la reducció al subgrup $\langle p\rangle$ d'exactament g_p caràcters diferents de $G(m)$.

Però tota arrel f_p-èsima de la unitat determina unívocament un caràcter de $\langle p\rangle$, de manera que, per a tot $w \in W$ hi ha exactament g_p caràcters $\chi \in G(m)\widehat{\ }$ tals que $\chi(p) = w$. En conseqüència, podem escriure la igualtat

$$(1 - T^{f_p})^{g_p} = \left(\prod_{w\in W}(1 - wT)\right)^{g_p} = \prod_{w\in W}\prod_{\chi(p)=w}(1 - \chi(p)T) = \prod_{\chi\in G(m)\widehat{\ }}(1 - \chi(p)T).$$

Aquesta igualtat ens serà útil de seguida, en substituir T per p^{-s}, per a qualsevol nombre complex s tal que $\Re(s) > 1$.

En efecte, a partir de la descomposició de les funcions $L(\chi, s)$ en producte d'Euler, convergent en el semiplà $\Re(s) > 1$, podem escriure les igualtats

$$\begin{aligned}\zeta_m(s) &= \prod_{\chi\in G(m)\widehat{\ }} L(\chi, s) = \prod_{\chi\in G(m)\widehat{\ }}\prod_{p}(1 - \chi(p)p^{-s})^{-1} = \prod_{\chi\in G(m)\widehat{\ }}\prod_{p\nmid m}(1 - \chi(p)p^{-s})^{-1}\\ &= \prod_{p\nmid m}\prod_{\chi\in G(m)\widehat{\ }}(1 - \chi(p)p^{-s})^{-1} = \prod_{p\nmid m}(1 - p^{-f_p s})^{-g_p},\end{aligned}$$

de manera que obtenim el que volíem demostrar. □

Observació 14.2.7. Observem que, per a tot nombre primer p que no divideix m, f_p és el grau residual de p en l'extensió ciclotòmica de $\mathbb{Q}$ generada per una arrel primitiva m-èsima de la unitat, i que g_p és el nombre d'ideals primers de l'anell dels enters d'aquest cos que divideixen p. En particular, si designem per $\mathfrak{p}$ els ideals primers d'aquest anell que divideixen p, podem escriure la igualtat

$$\zeta_m(s) = \prod_{p\nmid m}\prod_{\mathfrak{p}\mid p}(1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1} = \prod_{\mathfrak{p}\nmid m}(1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}.$$

Aquesta igualtat és semblant a la definició de la funció zeta de Dedekind del cos de nombres $\mathbb{Q}(\xi_m)$, per a ξ_m una arrel primitiva m-èsima de la unitat. Aquesta definició es donarà més endavant per a tot cos de nombres.

Corol·lari 14.2.8. *Sigui $m \in \mathbb{Z}$, $m \geq 2$. Per a tot caràcter no trivial de Dirichlet mòdul m, χ, és $L(\chi, 1) \neq 0$.*

DEMOSTRACIÓ: Per reducció a l'absurd. Suposem que hi hagués un caràcter no trivial de Dirichlet χ, mòdul m, tal que $L(\chi,1)=0$. Aleshores, aquest zero eliminaria el pol simple en $s=1$ de la funció $L(\chi_1,s)$ en la funció $\zeta_m(s)$, de manera que la funció $\zeta_m(s)$ seria entera. En virtut de la proposició anterior, els coeficients del desenvolupament en sèrie de Dirichlet, en el semiplà $\Re(s)>1$, de la funció $\zeta_m(s)$ serien nombres reals positius. A més a més, com que la sèrie de Dirichlet que defineix aquesta funció és de coeficients reals positius, la seva abscissa de convergència coincideix amb una singularitat de la funció; i com que hem vist que no hi hauria singularitats, la sèrie seria convergent en $\Re(s)>0$. Però això duu a contradicció. Veiem-ho.

Si pensem en $s\in\mathbb{R}$ tal que $s>0$, podem escriure les desigualtats

$$(1-p^{-f_ps})^{-g_p}=\left(\sum_{k\geq 0}p^{-kf_ps}\right)^{g_p}\geq\sum_{k\geq 0}p^{-kf_pg_ps}=\sum_{k\geq 0}p^{-k\varphi(m)s}=(1-p^{-\varphi(m)s})^{-1}.$$

Però aleshores, obtindríem les desigualtats

$$\zeta_m(s)=\sum_{n\geq 1,\mathrm{mcd}(n,m)=1}b_nn^{-s}\geq\sum_{n\geq 1,\mathrm{mcd}(n,m)=1}n^{-\varphi(m)s},$$

que ens dirien que la darrera sèrie és convergent. I, per a tenir la contradicció, només cal prendre s tal que $0<\varphi(m)s<1$.

En efecte, aquesta darrera sèrie s'expressa en forma de producte d'Euler de la mateixa manera que la sèrie de Riemann, i només les diferencia un nombre finit de factors. Concretament, en el producte d'Euler que li correspon, no apareixen els factors associats als nombres primers p que divideixen m i els altres són els mateixos que els de la funció zeta de Riemann; per tant, la convergència de la sèrie $\displaystyle\sum_{n\geq 1,\mathrm{mcd}(n,m)=1}n^{-\varphi(m)s}$ implicaria la convergència de la sèrie $\displaystyle\sum_{n\geq 1}n^{-s\varphi(m)}$, que no ho és. □

Com a conseqüència d'aquest resultat, podem establir immediatament el següent.

Corol·lari 14.2.9. *La funció $\zeta_m(s)$ té un pol simple en $s=1$.* □

14.3 Demostració del teorema

Aquesta secció es dedica a fer la prova del teorema de Dirichlet de la progressió aritmètica. Repetim l'enunciat.

Teorema 14.3.1 (Dirichlet)**.** *Siguin $a,m\in\mathbb{Z}$, $m\geq 1$, tals que $\mathrm{mcd}(a,m)=1$. El conjunt dels nombres primers de la forma $a+\lambda m$, $\lambda\in\mathbb{Z}$, té densitat de Dirichlet $\dfrac{1}{\varphi(m)}$; en particular, el conjunt és infinit.*

DEMOSTRACIÓ: Posem $A:=\{p\in P:\ \text{existeix } \lambda\in\mathbb{Z} \text{ i } p=a+\lambda m\}$ i considerem la funció zeta associada a aquest conjunt de nombres primers, $\zeta_A(s):=\displaystyle\sum_{p\in A}p^{-s}$. Cal estudiar el comportament de la funció $\zeta_A(s)$; concretament, cal veure la igualtat

$$\lim_{s\to 1^+}\frac{\zeta_A(s)}{\log(s-1)^{-1}}=\frac{1}{\varphi(m)}.$$

Per a tot caràcter de Dirichlet mòdul m, χ, sigui $F_\chi(s)$ la funció definida per la sèrie de Dirichlet $F_\chi(s) := \sum_{p\nmid m} \chi(p)p^{-s}$, convergent absolutament en el semiplà $\Re(s) > 1$. De fet, si tenim en compte que, per a $p|m$, és $\chi(p) = 0$, aleshores $F_\chi(s)$ es pot expressar en la forma $F_\chi(s) := \sum_{p} \chi(p)p^{-s}$, la suma estesa a tots els nombres primers.

El primer resultat que intervé a la demostració és el següent.

Lema 14.3.2. *Per a tot nombre complex s tal que $\Re(s) > 1$ és*

$$\zeta_A(s) = \frac{1}{\varphi(m)} \sum_{\chi\in G(m)\hat{}} \chi(a)^{-1} F_\chi(s).$$

DEMOSTRACIÓ: Se satisfan les igualtats

$$\begin{aligned}\sum_{\chi\in G(m)\hat{}} \chi(a)^{-1} F_\chi(s) &= \sum_{\chi\in G(m)\hat{}} \chi(a)^{-1} \sum_{p\nmid m} \chi(p)p^{-s} = \sum_{p\nmid m} \sum_{\chi\in G(m)\hat{}} \chi(a)^{-1}\chi(p)p^{-s} \\ &= \sum_{p\nmid m} \sum_{\chi\in G(m)\hat{}} \chi(a^{-1}p)p^{-s} = \varphi(m)\zeta_A(s),\end{aligned}$$

ja que $p \in A$ equival a $a^{-1}p \equiv 1 \pmod m$ i, per tant,

$$\sum_{\chi\in G(m)\hat{}} \chi(a^{-1}p) = \begin{cases}\varphi(m), & \text{si } p \in A,\\ 0, & \text{si } p \notin A,\end{cases}$$

en virtut de les relacions d'ortogonalitat dels caràcters. Per a acabar, només cal dividir per $\varphi(m)$. □

Deduirem el resultat que cerquem de l'estudi del comportament, en un entorn de $s = 1$, de les funcions $F_\chi(s)$.

Lema 14.3.3. (a) *Si $\chi = \chi_1$, el caràcter trivial mòdul m, llavors* $\lim_{s\to 1^+} \dfrac{F_\chi(s)}{\log(s-1)^{-1}} = 1.$

(b) *Si $\chi \neq \chi_1$, llavors* $\lim_{s\to 1^+} \dfrac{F_\chi(s)}{\log(s-1)^{-1}} = 0.$

DEMOSTRACIÓ: Les funcions $F_{\chi_1}(s)$ i $\zeta_P(s)$ només difereixen en un nombre finit de termes; els que corresponen als nombres primers que divideixen m. Per tant, el resultat (a) es dedueix immediatament de la proposició **14.1.2**.

Per a la prova de (b), observem que, si $\chi \neq \chi_1$, aleshores $L(\chi, s) = \prod_p (1 - \chi(p)p^{-s})^{-1}$, per a $\Re(s) > 1$. Si prenem logaritmes, podem escriure

$$\begin{aligned}\log L(\chi, s) &= \sum_p \log(1 - \chi(p)p^{-s})^{-1} = \sum_p \sum_{n\geq 1} \frac{\chi(p)^n}{np^{ns}} \\ &= F_\chi(s) + \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}} = F_\chi(s) + \psi'(s),\end{aligned}$$

on $\psi'(s) := \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}$. Ara, la prova del fet que $\lim_{s\to 1^+} \frac{\psi'(s)}{\log(s-1)^{-1}} = 0$, es fa igual que en la demostració de la proposició **14.1.2**; les desigualtats

$$\left|\sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}\right| \leq \sum_p \sum_{n\geq 2} \left|\frac{\chi(p)^n}{np^{ns}}\right| \leq \sum_p \sum_{n\geq 2} \left|\frac{1}{np^{ns}}\right|$$
$$= \sum_p \sum_{n\geq 2} \frac{1}{np^{ns}} \leq \sum_p \sum_{n\geq 2} \frac{1}{p^{ns}} \leq \sum_{n\geq 1} n^{-2},$$

per a $s > 1$, permeten concloure de la mateixa manera. En conseqüència, obtenim que $\lim_{s\to 1^+} \frac{F_\chi(s)}{\log(s-1)^{-1}} = \lim_{s\to 1^+} \frac{\log(L(\chi,s))}{\log(s-1)^{-1}}$. Però, com que el caràcter χ no és el trivial, la funció $L(\chi, s)$ no s'anul·la en $s = 1$; per tant, $\log(L(\chi, s))$ és fitada en un entorn de $s = 1$ i el límit anterior és nul. Això acaba la prova de (b). □

Amb aquests resultats, la prova del teorema de Dirichlet és senzilla. En efecte, obtenim el teorema a partir de la igualtat del lema **14.3.2**,

$$\zeta_A(s) = \frac{1}{\varphi(m)} \sum_{\chi\in G(m)\hat{}} \chi(a)^{-1} F_\chi(s),$$

en dividir per $\log(s-1)^{-1}$ i passar al límit. □

14.4 Valors de les funcions L en els enters negatius

En el capítol anterior hem calculat els valors de la funció zeta de Hurwitz i, en particular, els de la funció zeta de Riemann, en els enters negatius. Aquesta secció es dedica a fer el mateix per a les funcions L associades als caràcters de Dirichlet. Per a això, cal introduir una generalització dels nombres de Bernoulli: els nombres de Bernoulli generalitzats, associats als caràcters de Dirichlet. I per a dur a terme aquesta generalització, cal considerar els caràcters definits mòdul el seu conductor, contràriament a com hem treballat en les seccions anteriors.

Considerem, doncs, un caràcter de Dirichlet, χ; sigui f el conductor de χ, i considerem χ definit mòdul f; és a dir, per a $f' < f$, el morfisme $\chi : G(f) \longrightarrow \mathbb{C}^*$ no factoritza a través de $G(f')$ i $\chi(n) = 0$, si $\mathrm{mcd}(n, f) > 1$.

Definició 14.4.1. S'anomenen nombres generalitzats de Bernoulli associats a χ els coeficients $B_{n,\chi}$ de la sèrie de potències

$$\sum_{n\geq 0} \frac{B_{n,\chi}}{n!} z^n := \sum_{a=1}^{f} \chi(a) \frac{z\exp(az)}{\exp(fz)-1} \in \mathbb{C}[[z]].$$

Observació 14.4.2. Com que $\frac{z\exp(az)}{\exp(fz)-1} \in \mathbb{Q}[[z]]$, i com que els valors no nuls del caràcter χ són arrels f-èsimes de la unitat, els coeficients $B_{n,\chi}$ de la sèrie pertanyen al cos ciclotòmic $\mathbb{Q}(\mu_f)$ generat sobre $\mathbb{Q}$ per les arrels f-èsimes de la unitat; és a dir, se satisfà que $\sum_{n\geq 0} \frac{B_{n,\chi}}{n!} z^n \in \mathbb{Q}(\mu_f)[[z]]$.

Observació 14.4.3. Com que la funció analítica $\exp(fz)-1$ no s'anul·la en el disc $|z|<\dfrac{2\pi}{f}$, el radi de convergència de la sèrie $\displaystyle\sum_{n\geq 0}\frac{B_{n,\chi}}{n!}z^n$ és, com a mínim, $\dfrac{2\pi}{f}$.

Observació 14.4.4. Per a tot nombre enter $n\neq 1$, i si χ_1 designa el caràcter trivial, aleshores $B_{n,\chi_1}=B_n$, el n-èsim nombre de Bernoulli. En efecte, el conductor de χ_1 és $f=1$, de manera que $\displaystyle\sum_{n\geq 0}\frac{B_{n,\chi_1}}{n!}z^n=\frac{z\exp(z)}{\exp(z)-1}=\sum_{n\geq 0}\frac{B_n(1)}{n!}z^n$ i, per tant, resulta que

$$B_{n,\chi_1}=B_n(1)=\begin{cases}B_n, & \text{si } n\neq 1,\\ B_1+1, & \text{si } n=1.\end{cases}$$

Observació 14.4.5. Si $\chi\neq\chi_1$ no és el caràcter trivial, aleshores $B_{0,\chi}=0$. En efecte, $B_{0,\chi}$ és el valor en $z=0$ de la sèrie $\displaystyle\sum_{n\geq 0}\frac{B_{n,\chi}}{n!}z^n$. El càlcul de límits per la regla de l'Höpital, per exemple, ens permet escriure la igualtat

$$\lim_{z\to 0}\sum_{a=1}^{f}\frac{\chi(a)z\exp(az)}{\exp(fz)-1}=\sum_{a=1}^{f}\chi(a)\lim_{z\to 0}\frac{1}{f\exp(fz)}=\frac{1}{f}\sum_{a=1}^{f}\chi(a)=0.$$

Més generalment, podem calcular el valor dels nombres $B_{n,\chi}$ a partir dels polinomis de Bernoulli. En efecte, disposem del resultat següent.

Proposició 14.4.6. *Sigui χ un caràcter de Dirichlet de conductor f. Aleshores, per a tot nombre enter $n\geq 0$, se satisfà la igualtat $B_{n,\chi}=f^{n-1}\displaystyle\sum_{a=1}^{f}\chi(a)B_n\left(\frac{a}{f}\right)$. Més generalment, si F és un múltiple de f, se satisfà la fórmula $B_{n,\chi}=F^{n-1}\displaystyle\sum_{a=1}^{F}\chi(a)B_n\left(\frac{a}{F}\right)$.*

Demostració: Per a la sèrie de potències $g(z):=\displaystyle\sum_{n\geq 0}\frac{F^{n-1}\sum_{a=1}^{F}\chi(a)B_n\left(\frac{a}{F}\right)}{n!}z^n$, és

$$\begin{aligned}g(z)&=\sum_{a=1}^{F}\sum_{n\geq 0}\frac{F^{n-1}\chi(a)B_n\left(\frac{a}{F}\right)}{n!}z^n=\sum_{a=1}^{F}\frac{\chi(a)}{F}\sum_{n\geq 0}\frac{B_n\left(\frac{a}{F}\right)}{n!}(Fz)^n\\&=\sum_{a=1}^{F}\frac{\chi(a)}{F}\frac{Fz\exp\left(\frac{a}{F}Fz\right)}{\exp(Fz)-1}=\sum_{a=1}^{F}\chi(a)\frac{z\exp(az)}{\exp(Fz)-1}.\end{aligned}$$

Si dividim a per f en la forma $a=b+cf$, $1\leq b\leq f$, $0\leq c\leq\dfrac{F}{f}-1$, tenm que

$$\begin{aligned}g(z)&=\sum_{b=1}^{f}\sum_{c=0}^{\frac{F}{f}-1}\chi(b)\frac{z\exp(bz)\exp(cfz)}{\exp(Fz)-1}=\sum_{b=1}^{f}\chi(b)\frac{z\exp(bz)}{\exp(Fz)-1}\sum_{c=0}^{\frac{F}{f}-1}\exp(cfz)\\&=\sum_{b=1}^{f}\chi(b)\frac{z\exp(bz)}{\exp(Fz)-1}\frac{\exp(Fz)-1}{\exp(fz)-1}=\sum_{b=1}^{f}\chi(b)\frac{z\exp(bz)}{\exp(fz)-1}=\sum_{n\geq 0}\frac{B_{n,\chi}}{n!}z^n,\end{aligned}$$

i només cal igualar els coeficients. □

Corol·lari 14.4.7. *Sigui χ un caràcter de Dirichlet de conductor f.*

(a) *Si $\chi \neq \chi_1$, aleshores* $B_{1,\chi} = \dfrac{1}{f}\displaystyle\sum_{a=1}^{f} \chi(a)a$.

(b) *Sigui* $\delta := \begin{cases} 0, & \text{si } \chi(-1) = 1 \text{ (o sigui, si } \chi \text{ és parell)}, \\ 1, & \text{si } \chi(-1) = -1 \text{ (o sigui, si } \chi \text{ és senar)}. \end{cases}$ *Aleshores, per a $n \in \mathbb{Z}$, $n > 1$, i $n \equiv \delta \pmod 2$, és $B_{n,\chi} = 0$.*

Demostració: La proposició anterior ens permet assegurar que

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

ja que per a $\chi \neq \chi_1$ és $\displaystyle\sum_{a=1}^{f}\chi(a) = 0$.

D'altra banda, com que $\chi(f) = 0$, aleshores podem escriure que

$$\begin{aligned} f_\chi(-z) :&= \sum_{a=1}^{f} \chi(a)\frac{-z\exp(-az)}{\exp(-fz)-1} = \sum_{a=1}^{f-1}\chi(a)\frac{-z\exp(-az)}{\exp(-fz)-1} \\ &= \frac{-z\exp(fz)}{1-\exp(fz)}\sum_{a=1}^{f-1}\chi(a)\exp(-az) = \frac{z\exp(fz)}{\exp(fz)-1}\sum_{a=1}^{f-1}\chi(-1)\chi(-a)\exp(-az) \\ &= \sum_{a=1}^{f-1}\chi(-1)\chi(f-a)\frac{z\exp((f-a)z)}{\exp(fz)-1} = \chi(-1)\sum_{a=1}^{f-1}\chi(f-a)\frac{z\exp((f-a)z)}{\exp(fz)-1} \\ &= \chi(-1)f_\chi(z). \end{aligned}$$

Això ens assegura que la sèrie $f_\chi(z)$ té paritat, la mateixa que el caràcter; en conseqüència, els seus coeficients d'índex parell són nuls quan χ és senar i els seus coeficients d'índex senar són nuls quan χ és parell. □

Els resultats anteriors ens permeten expressar còmodament el valor de les funcions L de Dirichlet en els nombres enters negatius.

Proposició 14.4.8. *Sigui χ un caràcter de Dirichlet. Per a tot nombre enter $n \geq 1$ se satisfà la igualtat* $L(\chi, 1-n,) = -\dfrac{B_{n,\chi}}{n}$.

Demostració: Recordem que, per a tot nombre enter $n \geq 0$, hem calculat el valor de la funció zeta de Hurwitz en $-n$ i hem obtingut que $\zeta(-n, a) = -\dfrac{B_{n+1}(a)}{n+1}$. D'altra banda, per a tot nombre complex s hem obtingut l'expressió $L(\chi, s) = f^{-s}\displaystyle\sum_{a=1}^{f}\chi(a)\zeta\left(s, \frac{a}{f}\right)$. Si fem $s = 1-n$, obtenim les igualtats

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

com volíem demostrar. □

Observació 14.4.9. En particular, els valors de les funcions L de Dirichlet en els enters negatius són nombres algebraics; encara més, pertanyen al cos ciclotòmic generat per les arrels f-èsimes de la unitat, on f és el conductor del caràcter χ.

14.5 Interpolació p-àdica les funcions L de Dirichlet

En aquesta secció es tracta de fer la interpolació per funcions p-àdiques dels valors en els enters negatius de les funcions L complexes associades als caràcter de Dirichlet.

Sigui p un nombre primer i escrivim, com abans, $q := \begin{cases} p, & \text{si } p \neq 2, \\ 4, & \text{si } p = 2. \end{cases}$ Acabem de veure que, si χ és un caràcter de Dirichlet de conductor f, aleshores els valors de la funció complexa $L(\chi, s)$ en els nombres enters negatius $s = 1-n$, $n \geq 1$, són nombres algebraics sobre $\mathbb{Q}$. Per tant, si volem construir una funció p-àdica que interpoli aquests valors, cal triar una immersió de la clausura algebraica de $\mathbb{Q}$ dins el cos $\mathbb{C}_p$. Fixem-ne, doncs, una.

Proposició 14.5.1. *Sigui χ un caràcter de Dirichlet de conductor f. Aleshores, existeix una funció meromorfa p-àdica, $L_p(\chi, s)$, definida en el disc $|s|_p < qp^{\frac{-1}{p-1}}$ de $\mathbb{C}_p$, tal que:*

(a) *per a tot nombre enter $n \geq 1$,*

$$\begin{aligned} L_p(\chi, 1-n) &= (1 - \chi\omega^{-n}(p)p^{n-1})L(\chi\omega^{-n}, 1-n) \\ &= -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \end{aligned}$$

on $\omega(a)$ és l'arrel $\varphi(q)$-èsima de la unitat de $\mathbb{C}_p$ tal que $a\omega(a)^{-1} \equiv 1 \pmod{q}$, per a tot nombre enter $a \not\equiv 0 \pmod{p}$, i el producte $\chi\omega^{-n}$ és el producte com a caràcters;

(b) *si $\chi = \chi_1$ és el caràcter trivial, aleshores $L_p(\chi_1, s)$ té un pol simple en $s = 1$ amb residu $1 - \dfrac{1}{p}$; i*

(c) *si $\chi \neq \chi_1$, aleshores $L_p(\chi, s)$ és analítica p-àdica en el disc $|s|_p < qp^{\frac{-1}{p-1}}$.*

Demostració: Considerem un nombre enter $F > 0$ tal que $f, q | F$ i definim

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

on $H_p(s, a, F)$ és la funció p-àdica definida a la demostració de la proposició **13.6.4** per la fórmula $H_p(s, a, F) := \dfrac{1}{s-1}\dfrac{1}{F}\langle a \rangle^{1-s} \displaystyle\sum_{k \geq 0} \binom{1-s}{k} \left(\frac{F}{a}\right)^k B_k$, i on B_k són els nombres de Bernoulli. Recordem que aquesta funció és holomorfa p-àdica en el disc $|s|_p < qp^{\frac{-1}{p-1}}$ llevat, potser, d'un únic pol, i simple, en $s = 1$. Per tant, la funció $L_p(\chi, s)$ també és

holomorfa en aquest disc, llevat del punt $s=1$, on hi pot haver un pol simple. Ara bé, podem calcular

$$\lim_{s\to 1}(s-1)L_p(\chi,s)=\sum_{a=1,\,p\nmid a}^{F}\chi(a)\frac{1}{F}=\frac{1}{F}\sum_{a=1}^{F}\chi(a)-\frac{1}{F}\sum_{b=1}^{F/p}\chi(pb)=\begin{cases}1-\dfrac{1}{p}, & \text{si } \chi=\chi_1,\\ 0, & \text{si } \chi\neq\chi_1;\end{cases}$$

per tant, la funció $L_p(\chi,s)$ té un pol simple en $s=1$ quan $\chi=\chi_1$, amb residu $1-\dfrac{1}{p}$, i no té pol quan $\chi\neq\chi_1$. Això demostra (b) i (c).

D'altra banda, per a tot nombre enter $n\geq 1$, podem escriure que

$$\begin{aligned}L_p(\chi,1-n)&=\sum_{a=1,\,p\nmid a}^{F}\chi(a)H_p(1-n,a,F)=\sum_{a=1,\,p\nmid a}^{F}\chi(a)\omega(a)^{-n}H_\infty(1-n,a,F)\\&=\sum_{a=1,\,p\nmid a}^{F}\chi(a)\omega(a)^{-n}F^{n-1}\zeta\left(1-n,\frac{a}{F}\right)=-\sum_{a=1,\,p\nmid a}^{F}\frac{\chi(a)\omega(a)^{-n}F^{n-1}}{n}B_n\left(\frac{a}{F}\right)\\&=-\frac{1}{n}F^{n-1}\sum_{a=1}^{F}\chi(a)\omega(a)^{-n}B_n\left(\frac{a}{F}\right)+\frac{1}{n}\left(\frac{F}{p}\right)^{n-1}p^{n-1}\sum_{b=1}^{F/p}\chi(pb)\omega(pb)^{-n}B_n\left(\frac{b}{F/p}\right).\end{aligned}$$

El conductor del caràcter ω és un divisor de q; per tant, el conductor de $\chi\omega^{-n}$ és un divisor del mínim múltiple comú de f i q; per tant, el conductor de $\chi\omega^{-n}$ divideix F. Si p divideix el conductor del caràcter $\chi\omega^{-n}$, aleshores $\chi\omega^{-n}(pb)=0$; en cas contrari, el conductor de $\chi\omega^{-n}$ divideix el quocient $\dfrac{F}{p}$. En conseqüència, podem assegurar que se satisfà la igualtat $L_p(\chi,1-n)=-\dfrac{1}{n}\left(B_{n,\chi\omega^{-n}}-\chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}\right)$, per les propietats dels nombres generalitzats de Bernoulli. Això acaba la prova. □

Corol·lari 14.5.2. *Si el caràcter de Dirichlet χ és senar, llavors $L_p(\chi,s)=0$, per a tot s.*

Demostració: En efecte, com que ω és un caràcter senar, si χ és senar, aleshores n i $\chi\omega^{-n}$ són de diferent paritat, de manera que els nombres de Bernoulli $B_{n,\chi\omega^{-n}}$ són tots nuls. Això ens permet assegurar que $L_p(\chi,1-n)=0$, per a tot n; per tant, la funció analítica p-àdica $L_p(\chi,s)$ té una infinitat de zeros que s'acumulen en el punt 1 (per exemple, tots els $1-p^k$); en conseqüència, $L_p(\chi,s)$ ha de ser idènticament nul·la. □

Per a un caràcter no trivial, la funció $L_p(\chi,s)$ és analítica p-àdica en un entorn de $s=1$; en conseqüència, admet un desenvolupament en sèrie de potències de $s-1$ convergent en aquest entorn. Podem donar alguna propietat d'aquest desenvolupament.

Proposició 14.5.3. *Sigui $\chi\neq\chi_1$ un caràcter no trivial de Dirichlet de conductor f i suposem que pq no divideix f. Existeix una successió d'elements $a_n\in\mathbb{C}_p$ tals que*

(a) $v_p(a_0)\geq 0$;

(b) $v_p(a_n)\geq 1$, *per a tot* $n\geq 1$; *i*

(c) $L_p(\chi,s)=\displaystyle\sum_{n\geq 0}a_n(s-1)^n$, *per a* $|s|_p<qp^{\frac{-1}{p-1}}$.

DEMOSTRACIÓ: Podem suposar, ja que per als caràcters senars la funció $L_p(\chi,s)$ és idènticament nul·la, que χ és un caràcter parell. Per hipòtesi, el conductor de χ no és divisible per pq, de manera que podem elegir F com a la proposició anterior, però de manera que, a més a més, F no sigui divisible per pq. D'altra banda, recordem l'expressió $L_p(\chi,s)=\sum_{a=1,\,p\nmid a}^{F}\chi(a)H_p(s,a,F)$, amb $H_p(s,a,F)=\dfrac{1}{s-1}\dfrac{1}{F}\langle a\rangle^{1-s}\displaystyle\sum_{k\geq 0}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k$; és a dir, $L_p(\chi,s)=\dfrac{1}{s-1}\dfrac{1}{F}\displaystyle\sum_{a=1,\,p\nmid a}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{k\geq 0}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k$.

Com que q divideix F, és $|F^{k-1}|_p\leq q^{1-k}$. El nombre de Bernoulli B_k, multiplicat per p, és un nombre enter p-àdic, de manera que $|B_k|_p\leq p$. I la valoració p-àdica de $k!$ no supera $\dfrac{k}{p-1}$. En conseqüència, per a tot nombre enter a no divisible per p, i tot nombre enter $k\geq 0$, podem escriure la desigualtat $\left|\dfrac{B_kF^{k-1}}{k!a^k}\right|_p\leq p^{\frac{k}{p-1}}pq^{1-k}$; per tant, per a $k\geq 6$, és

$$\left|\frac{B_kF^{k-1}}{k!a^k}\right|_p\leq q^{-1},\tag{14.5.1}$$

per a tots els nombres primers p. A més a més, com que $B_3=B_5=0$, i $B_4=-\dfrac{1}{30}$, obtenim que $\left|\dfrac{B_4F^{4-1}}{4!a^4}\right|_p=\left|\dfrac{F^3}{2^43^25a^4}\right|_p\leq q^{-1}$, de manera que (14.5.1) se satisfà per a tot nombre enter $k\geq 3$. En conseqüència, tots els coeficients del desenvolupament en sèrie de potències de $1-s$ de la sèrie $\dfrac{1}{F}\displaystyle\sum_{k\geq 3}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k$ són de valoració p-àdica més gran o igual que 1. Anàlogament, els coeficients, per a $0\leq k\leq 2$, poden tenir q en el denominador, però no pq (comprovació immediata).

D'altra banda, per a tot nombre enter a no divisible per p podem escriure que

$$\langle a\rangle^{1-s}=\exp((1-s)\log_p\langle a\rangle)=\sum_{k\geq 0}\frac{(1-s)^k}{k!}(\log_p\langle a\rangle)^k,$$

de manera que els coeficients de $(1-s)^k$ pertanyen a $\mathbb{Z}_p$ i, com que $\log_p\langle a\rangle$ és divisible per q, els coeficients per a $k\geq 2$ són divisibles per pq (exercici). En conseqüència, el producte dels coeficients del desenvolupament en sèrie de potències de $1-s$ de la funció $\langle a\rangle^{1-s}$ pels d'índex $k\geq 2$ del desenvolupament de $\dfrac{1}{F}\displaystyle\sum_{k\geq 0}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k$ són tots divisibles per p; així, només cal comprovar (a), (b) i (c) per al desenvolupament en sèrie de potències de $1-s$ de la funció

$$\frac{1}{1-s}\sum_{a=1,\,p\nmid a}^{F}\chi(a)(1+(1-s)\log_p\langle a\rangle)\left(\frac{1}{F}-\frac{1-s}{2a}+\frac{(1-s)(1-s-1)F}{12a^2}\right).$$

Podem escriure aquesta funció com a polinomi de Laurent en $(1-s)$

$$b_{-1}(1-s)^{-1}+b_0+b_1(1-s)+b_2(1-s)^2.$$

El càlcul del primer coeficient dóna $b_{-1} = -\frac{1}{F}\sum_{a=1,\,p\nmid a}^{F}\chi(a) = 0$, ja que $\chi \neq \chi_1$. D'altra banda, $b_0 = -\sum_{a=1,\,p\nmid a}^{F}\chi(a)\left(\frac{1}{F}\log_p\langle a\rangle - \frac{1}{2a} - \frac{F}{12a^2}\right)$; ara bé, $\frac{\log_p\langle a\rangle}{F} \in \mathbb{Z}_p$, i també $\frac{F}{12a^2} \in \mathbb{Z}_p$; a més a més, $\sum_{a=1,\,p\nmid a}^{F}\frac{\chi(a)}{2a} \equiv \sum_{a=1,\,p\nmid a}^{F}\frac{\chi(a)}{2\omega(a)} \equiv \frac{1}{2}\sum_{a=1,\,p\nmid a}^{F}\chi\omega^{-1}(a) \equiv 0 \pmod p$. En efecte, si $p \neq 2$, aleshores 2 és invertible en $\mathbb{Z}_p$ i $q = p$, de manera que $a \equiv \omega(a) \pmod p$; i si $p = 2$, aleshores $q = 2p$, i també $a \equiv \omega(a) \pmod 2$; finalment, la darrera suma és nul·la, mòdul p, tenint en compte el conductor del caràcter $\chi\omega^{-1}$. Això demostra que $v_p(b_0) \geq 0$. Calculem, ara, el coeficient b_1. Podem escriure que

$$b_1 = -\sum_{a=1,\,p\nmid a}^{F}\chi(a)\left(\frac{F}{12a^2} - \frac{\log_p\langle a\rangle}{2a} - \frac{F\log_p\langle a\rangle}{12a^2}\right);$$

com que $\frac{\log_p\langle a\rangle}{2a}$ i $\frac{F\log_p\langle a\rangle}{12a^2}$ són elements de $\mathbb{Z}_p$, i divisibles per p, només cal veure que $\frac{F}{12}\sum_{a=1,\,p\nmid a}^{F}\frac{\chi(a)}{a^2}$ és divisible per p en $\mathbb{Q}_p$; si $p \geq 5$, la suma és un nombre enter p-àdic i el quocient $\frac{F}{12}$ és divisible per p; i si $p \in \{2,3\}$, aleshores $\frac{F}{12} \in {\mathbb{Z}_p}^*$; però en aquest cas és $a^2 \equiv 1 \pmod p$, ja que $p \nmid a$, de manera que $\sum_{a=1,\,p\nmid a}^{F}\frac{\chi(a)}{a^2} \equiv \sum_{a=1,\,p\nmid a}^{F}\chi(a) \equiv 0 \pmod p$; per tant, $v_p(a_1) \geq 1$.

Per a acabar, el coeficient b_2 és $b_2 = -\sum_{a=1,\,p\nmid a}^{F}\chi(a)\log_p\langle a\rangle\frac{F}{12a^2}$, i ja hem vist que els sumands són nmbres enters p-àdics divisibles per p. Això acaba la prova de la proposició. □

14.6 Congruències de Kummer

En els seus estudis sobre l'equació de Fermat, Kummer establí molts i bells resultats; un dels que ens interessen en la part final del curs són unes congruències entre nombres de Bernoulli. Com a corol·lari del darrer resultat de la secció anterior, podem establir el següent.

Corol·lari 14.6.1. *Sigui χ un caràcter no trivial de Dirichlet, i suposem que pq no divideix el conductor f de χ. Aleshores, per a tota parella de nombres enters $n, m \in \mathbb{Z}$, els nombres p-àdics $L_p(\chi, n)$, $L_p(\chi, m)$ pertanyen a $\mathbb{Z}_p$ i, a més a més, $L_p(\chi, n) \equiv L_p(\chi, m) \pmod p$.*

Demostració: Amb les notacions del resultat anterior, i com que $|m-1|_p \leq 1 < qp^{\frac{-1}{p-1}}$, podem substituir s per n i per m en la igualtat anterior; i com que els coeficients satisfan que $v_p(a_i) \geq 1$, per a tot $i \geq 1$, obtenim que $L_p(\chi, n) \equiv a_0 \equiv L_p(\chi, m) \pmod p$, com volíem demostrar. □

Corol·lari 14.6.2 (Congruències de Kummer)**.** *Siguin m, n, nombres enters parells i positius. Si $m \equiv n \not\equiv 0 \pmod{(p-1)}$, aleshores $\dfrac{B_m}{m} \equiv \dfrac{B_n}{n} \pmod{p}$. Més generalment, si m, n són nombres enters positius tals que $m \equiv n \pmod{(p-1)p^a}$, i $n \not\equiv 0 \pmod{(p-1)}$, aleshores $(1-p^{m-1})\dfrac{B_m}{m} \equiv (1-p^{n-1})\dfrac{B_n}{n} \pmod{p^{a+1}}$.*

Demostració: Si $m \equiv n \not\equiv 0 \pmod{(p-1)}$, aleshores $\omega^n = \omega^m \neq \chi_1$, de manera que $L_p(\omega^n, s) = L_p(\omega^m, s)$ i $\omega^m \neq \chi_1$. Per tant,

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

Ara bé, amb les mateixes notacions que a la proposició **14.5.3**, podem escriure que

$$\begin{gathered} L_p(\omega^m, 1-m) = a_0 + a_1(-m) + a_2(-m)^2 + \cdots \\ \equiv a_0 + a_1(-n) + a_2(-n)^2 + \cdots = L_p(\omega^n, 1-n) \pmod{p^{a+1}}, \end{gathered}$$

com volíem demostrar. □

Corol·lari 14.6.3. *Sigui $n \in \mathbb{Z}$, $n \geq 1$ senar, i suposem que $n \not\equiv -1 \pmod{(p-1)}$. Aleshores, $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \pmod{p}$, en el sentit que els dos nombres són p-enters i val la igualtat mòdul p.*

Demostració: Com que $n+1 \not\equiv 0 \pmod{(p-1)}$, el caràcter ω^{n-1} no és el caràcter trivial; d'altra banda, com que $\omega^n(p) = 0$, ω^n tampoc no és el caràcter trivial. Aleshores, podem escriure que

$$\begin{gathered} B_{1,\omega^n} = (1-\omega^n(p))B_{1,\omega^n} = -L_p(\omega^{n+1}, 0) \\ \equiv -L_p(\omega^{n+1}, 1-(n+1)) = (1-p^n)\frac{B_{n+1}}{n+1} \equiv \frac{B_{n+1}}{n+1} \pmod{p}, \end{gathered}$$

com volíem veure. □

Capítol 15

Fórmules per als nombres de classes

L'objectiu d'aquest capítol és obtenir fórmules per al càlcul dels nombres de classes d'ideals d'alguns cossos de nombres. Concretament, establirem una fórmula analítica en general i en deduirem fórmules per al càlcul dels nombres de classes d'ideals dels cossos quadràtics i dels cossos ciclotòmics.

15.1 La funció zeta de Dedekind

De la mateixa manera que la funció zeta de Riemann té en compte tots els nombres primers de $\mathbb{Q}$, la funció zeta de Dedekind té en compte tots els ideals primers no nuls de l'anell dels enters d'un cos de nombres arbitrari. L'objectiu d'aquesta secció és fer-ne la introducció i establir-ne les primeres propietats.

Per tant, considerarem un cos de nombres K; és a dir, un cos extensió finita del cos dels nombres racionals. Denotarem per A l'anell dels enters del cos K, per $\mathfrak{p}$ un ideal primer no nul de A, i per n el grau $n := [K : \mathbb{Q}]$. Recordem, també, que si $\mathfrak{a} \subseteq A$ és un ideal no nul qualsevol, la norma de $\mathfrak{a}$, $\mathrm{N}(\mathfrak{a})$, és el cardinal de l'anell quocient $A/\mathfrak{a}$, que si $\mathfrak{p}$ és primer, aleshores $\mathrm{N}(\mathfrak{p}) = p^{f_\mathfrak{p}}$, on $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ i $f_\mathfrak{p}$ és el grau residual en $\mathfrak{p}$, i que la norma és completament multiplicativa, en el sentit que $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$, per a tota parella d'ideals $\mathfrak{a}$, $\mathfrak{b} \subseteq A$.

Definició 15.1.1. La sèrie zeta de Dedekind associada al cos de nombres K és, per definició, la sèrie

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq A} \mathrm{N}(\mathfrak{a})^{-s}, \quad s \in \mathbb{C}.$$

De fet, hauríem de dir en quin ordre es prenen els sumands, ja que en cas contrari la suma no està definida, ni tan sols en el cas que sigui convergent. Veurem de seguida que, en algun semiplà $\Re(s) >> 0$ la sèrie és absolutament convergent; o, per a ser més precisos, que la família $\{\mathrm{N}(\mathfrak{a})^{-s}\}_{\mathfrak{a} \subseteq A}$ és absolutament sumable. Per a veure-ho, però, primerament cal veure que se satisfà la propietat següent.

Lema 15.1.2. *La família $\{\mathrm{N}(\mathfrak{p})^{-s}\}_\mathfrak{p}$ és absolutament i uniformement sumable en tots els semiplans $\Re(s) \geq 1 + \delta$, on $\delta \in \mathbb{R}$, $\delta > 0$.*

Demostració: Sigui C un conjunt finit qualsevol d'ideals primers no nuls $\mathfrak{p} \subseteq A$; per a tot $\mathfrak{p} \in C$, posem $p\mathbb{Z} := \mathfrak{p} \cap \mathbb{Z}$ la seva contracció a l'anell $\mathbb{Z}$ i sigui C' el conjunt

format pels primers p que són contracció d'algun ideal primer $\mathfrak{p} \in C$. Si $s \in \mathbb{C}$ és tal que $1+\delta \leq \Re(s) \leq r$, podem escriure que $\sum_{\mathfrak{p}\in C} |\mathrm{N}(\mathfrak{p})^{-s}| = \sum_{\mathfrak{p}\in C} |p^{-sf_\mathfrak{p}}| \leq \sum_{p\in C'} \sum_{\mathfrak{p}|p} |p^{-sf_\mathfrak{p}}|$. Com que, per a tot ideal primer $\mathfrak{p}$ és $f_\mathfrak{p} \geq 1$, resulta que $p^{f_\mathfrak{p}} \geq p$, i com que el nombre d'ideals primers $\mathfrak{p}$ que divideixen p és menor o igual que el grau, n, obtenim la desigualtat

$$\sum_{\mathfrak{p}\in C} |\mathrm{N}(\mathfrak{p})^{-s}| \leq n \sum_{p\in C'} |p^{-s}| \leq n \sum_{p\in C'} |p^{-(1+\delta)}| \leq n \sum_{m\geq 1} m^{-(1+\delta)} = n\zeta(1+\delta),$$

que és una fita uniforme que no depèn de s ni de C. Això demostra el resultat que volíem veure. □

Corol·lari 15.1.3. *El producte infinit* $\prod_{\mathfrak{p}} (1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}$ *és absolutament i uniformement convergent en tots els semiplans* $\Re(s) \geq 1+\delta$, $\delta \in \mathbb{R}$, $\delta > 0$. □

Teorema 15.1.4. *La suma* $\zeta_K(s) = \sum_{\mathfrak{a}\subseteq A} \mathrm{N}(\mathfrak{a})^{-s}$ *és absolutament i uniformement convergent sobre tots els conjunts compactes del semiplà* $\Re(s) > 1$. *En conseqüència, defineix una funció analítica en aquest semiplà. A més a més, la funció* $\zeta_K(s)$ *admet una expressió en forma de producte d'Euler* $\zeta_K(s) = \prod_{\mathfrak{p}} (1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}$, *en aquest semiplà.*

Demostració: Acabem de veure que el producte és absolutament convergent en el semiplà $\Re(s) > 1$. D'aquí obtindrem que la suma $\sum_{\mathfrak{a}\subseteq A} \mathrm{N}(\mathfrak{a})^{-s}$ també és absolutament convergent en $\Re(s) > 1$ i, a més a més, que se satisfà la igualtat. Comencem, però, per observar que, si fixem un nombre real positiu qualsevol, $x > 0$, podem escriure una igualtat $\prod_{\mathrm{N}(\mathfrak{p})\leq x} (1-\mathrm{N}(\mathfrak{p})^{-\Re(s)})^{-1} = \prod_{\mathrm{N}(\mathfrak{p})\leq x} \sum_{k\geq 0} \mathrm{N}(\mathfrak{p})^{-k\Re(s)}$ entre productes finits, sempre que $\Re(s) > 1$, solament sumant les sèries geomètriques. Ara bé, si $\mathfrak{a} \subseteq A$ és un ideal de norma $\leq x$, aleshores tots els seus divisors primers són també de norma $\leq x$; per tant, $\mathrm{N}(\mathfrak{a})^{-\Re(s)}$ és un dels sumands, $\prod_{\mathfrak{p}|\mathfrak{a}} \mathrm{N}(\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})})^{-\Re(s)}$, del producte anterior; per tant, obtenim la desigualtat $\sum_{\mathrm{N}(\mathfrak{a})\leq x} \mathrm{N}(\mathfrak{a})^{-\Re(s)} \leq \prod_{\mathrm{N}(\mathfrak{p})\leq x} (1-\mathrm{N}(\mathfrak{p})^{-\Re(s)})^{-1}$. Com que aquesta desigualtat és vàlida per a tot nombre real $x > 0$ i el producte infinit és absolutament convergent, també la suma infinita és absolutament convergent.

A més a més, la diferència entre la suma finita i el producte finit es pot fitar, en valor absolut, pel valor absolut de la suma $\sum_{\mathrm{N}(\mathfrak{a})>x} \mathrm{N}(\mathfrak{a})^{-\Re(s)}$, que tendeix a zero quan x tendeix a $+\infty$. Per tant, obtenim la igualtat que desitjàvem entre la suma infinita i el producte d'Euler. □

15.2 El regulador d'un cos de nombres

Per al càlcul de fórmules per al nombre de classes d'un cos de nombres, un dels ingredients és el regulador. Aquessta secció es dedica a la seva introducció i estudi.

En el capítol **4**, hem vist que, si K és un cos de nombres, A el seu anell d'enters, r_1 el nombre d'immersions reals diferents de K, i r_2 el de parelles d'immersions complexes conjugades no reals de K, aleshores, el grup abelià dels elements invertibles de A, U_K, descompon en suma directa d'un grup abelià finit, W_K, format per les arrels de la unitat de K, i un grup abelià lliure de rang $r := r_1 + r_2 - 1$. En particular, existeixen elements $u_1, u_2, \dots, u_r \in U_K$ tals que tota unitat $u \in U_K$ s'escriu de manera única en la forma $u = \zeta u_1^{n_1} \cdot \dots \cdot u_r^{n_r}$, amb $\zeta \in K$, arrel de la unitat i $n_i \in \mathbb{Z}$, per a $1 \leq i \leq r$. Un sistema d'unitats $\{u_i\}_{1 \leq i \leq r}$ com aquest s'anomena un sistema fonamental d'unitats de K.

Recordem, també, que la immersió logarítmica de U_K és definida per

$$u \mapsto (\log|\sigma_1(u)|, \dots, \log|\sigma_{r_1}(u)|, 2\log|\sigma_{r_1+1}(u)|, \dots, 2\log|\sigma_{r_1+r_2}(u)|),$$

on $\sigma_1, \dots, \sigma_{r_1}$ són les r_1 immersions reals i $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ un sistema de representants de les parelles d'immersions complexes conjugades no reals de K, i on $|\ |$ indica el valor absolut usual de $\mathbb{C}$.

Podem considerar, doncs, la matriu de r columnes i $r_1 + r_2 = r + 1$ files formada pels nombres complexos $\varepsilon_i \log|\sigma_i(u_j)|$, on $\varepsilon_i = 1$ si $1 \leq i \leq r_1$, i $\varepsilon_i = 2$ si $r_1 + 1 \leq i \leq r_1 + r_2$; és a dir, la matriu formada pels vectors fila que són les imatges del sistema fonamental d'unitats per la immersió logarítmica.

Amb aquestes notacions, podem establir el resultat següent.

Proposició 15.2.1. *El valor absolut de cada un dels menors d'ordre r de la matriu és independent del menor considerat i del sistema fonamental d'unitats.*

Demostració: Recordem que havíem definit un hiperplà $H \subseteq \mathbb{R}^{r+1}$ per l'equació $\sum_{i=1}^{r_1+r_2} X_i = 0$, i que aquest hiperplà conté la imatge de U_K per la immersió logarítmica $u \mapsto (\log|\sigma_1(u)|, \dots, \log|\sigma_{r_1}(u)|, \log|\sigma_{r_1+1}(u)|^2, \dots, \log|\sigma_{r_1+r_2}(u)|^2)$ (cf. el lema **4.6.2** per al canvi de notació). Encara més, vàrem provar que, via aquesta immersió logarítmica, la imatge de U_K és una xarxa de H (cf. el lema **4.6.3**). D'altra banda, el vector unitari de $\mathbb{R}^{r_1+r_2}$ de coordenades iguals, és a dir, el vector $v := \dfrac{1}{\sqrt{r_1+r_2}}(1, \dots, 1)$, és ortogonal a H, de manera que podem calcular la malla de la xarxa generada per les unitats dins de H com la malla, dins $\mathbb{R}^{r_1+r_2}$, de la xarxa generada per les unitats i aquest vector. I aquesta malla és el determinant de la matriu quadrada formada per qualsevol base de la xarxa de les unitats orlada amb el vector v. Es tracta, doncs, de calcular el determinant

$$\begin{vmatrix} \log|\sigma_1(u_1)| & \dots & \log|\sigma_{r_1}(u_1)| & \log|\sigma_{r_1+1}(u_1)|^2 & \dots & \log|\sigma_{r_1+r_2}(u_1)|^2 \\ \vdots & & \vdots & \vdots & & \vdots \\ \log|\sigma_1(u_r)| & \dots & \log|\sigma_{r_1}(u_r)| & \log|\sigma_{r_1+1}(u_r)|^2 & \dots & \log|\sigma_{r_1+r_2}(u_r)|^2 \\ \dfrac{1}{\sqrt{r_1+r_2}} & \dots & \dfrac{1}{\sqrt{r_1+r_2}} & \dfrac{1}{\sqrt{r_1+r_2}} & \dots & \dfrac{1}{\sqrt{r_1+r_2}} \end{vmatrix}.$$

Com que per als components de les unitats de K pensats com a vectors de $\mathbb{R}^{r_1+r_2}$ via la immersió logarítmica se satisfà l'equació $\sum_{i=1}^{r_1+r_2} \varepsilon_i \log|\sigma_i(u)| = 0$, hi ha una combinació lineal de files d'aquest determinant que anul·la tots els components d'una columna llevat

del darrer; i el valor d'aquest darrer és exactament la suma $\frac{r_1+r_2}{\sqrt{r_1+r_2}} = \sqrt{r_1+r_2}$, independentment de la columna que fem servir per a aconseguir aquesta anul·lació; és a dir, la malla de la xarxa de les unitats és el producte del nombre $\sqrt{r_1+r_2}$, amb un signe, per qualsevol dels menors (desfem, si volem, la combinació lineal) que volíem. Per tant, i com que la malla de la xarxa tampoc no depèn del sistema d'unitats que considerem, el resultat queda provat. □

Definició 15.2.2. S'anomena regulador de K el valor absolut de cada un d'aquests menors.

15.3 Densitat dels ideals d'una classe

Deixem momentàniament de banda l'estudi de la funció zeta de Dedekind per a fer l'estudi del concepte de densitat dels ideals enters de l'anell dels enters A d'un cos de nombres K en una classe d'ideals.

Siguin, doncs, K un cos de nombres, A l'anell dels enters de K, $w := w(K)$ el nombre d'arrels de la unitat de K, r_1 el nombre d'immersions reals de K, r_2 el nombre de parelles d'immersions complexes conjugades no reals de K, $h := h_K$ el nombre de classes d'ideals de A, $R := R_K$ el regulador, i Δ_K el discriminant absolut de K, i fixem una classe d'ideals $\mathfrak{A}$ de A.

Per a cada nombre real positiu x, denotem per $S(x,\mathfrak{A})$ el conjunt format per tots els ideals enters de A que pertanyen a la classe $\mathfrak{A}$ i que, alhora, són de norma $\leq x$. Per a tot $x \in \mathbb{R}$, $x > 0$, el conjunt $S(x,\mathfrak{A})$ és finit, ja que, per a cada nombre enter positiu N, hi ha un nombre finit d'ideals de A que tinguin norma N.

Teorema 15.3.1 (Dirichlet-Dedekind)**.** *Sigui $\mathfrak{A}$ una classe d'ideals de A; aleshores, existeix el límit i val la igualtat* $\lim_{x\to+\infty} \frac{\#S(x,\mathfrak{A})}{x} = \frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|\Delta_K|}}$.

Observació 15.3.2. Podem dir, per tant, que existeix la densitat del conjunt dels ideals enters dins d'una classe d'ideals i que aquesta densitat no depèn de la classe que considerem.

Abans de fer la demostració d'aquest teorema en donarem una conseqüència important. Si designem per $S(x)$ el conjunt de tots els ideals enters no nuls de A que són de norma $\leq x$, sense fixar cap classe d'ideals, obtenim el resultat següent.

Corol·lari 15.3.3. *Existeix el límit i val la igualtat* $\lim_{x\to+\infty} \frac{\#S(x)}{x} = h\,\frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|\Delta_K|}}$.

Demostració: En primer lloc, podem tenir en compte que, per a tot $x > 0$, el conjunt $S(x)$ és la reunió disjunta, quan $\mathfrak{A}$ recorre les h classes d'ideals de A, dels conjunts $S(x,\mathfrak{A})$; després, només cal aplicar la proposició. □

Anem a descriure una demostració del teorema. Fixada la classe d'ideals $\mathfrak{A}$, podem considerar la seva classe inversa, $\mathfrak{A}^{-1}$, un ideal enter, $\mathfrak{a} \in \mathfrak{A}^{-1}$, i la norma de $\mathfrak{a}$, $\mathrm{N}(\mathfrak{a})$. Sigui $\overline{S}(x,\mathfrak{a})$ el conjunt de les classes d'equivalència dels elements no nuls $\omega \in \mathfrak{a}$ tals que $|\mathrm{N}(\omega)| \leq x\mathrm{N}(\mathfrak{a})$, classificats mòdul el producte per unitats de l'anell A.

Lema 15.3.4. *Se satisfà la igualtat* $\#S(x,\mathfrak{A}) = \#\overline{S}(x,\mathfrak{a})$.

Demostració: Donat un ideal enter $\mathfrak{b} \in \mathfrak{A}$, el producte $\mathfrak{ab}$ és un ideal principal enter no nul de A, ja que $\mathfrak{a} \in \mathfrak{A}^{-1}$; per tant, existeix un element no nul $\omega \in A$ tal que $\mathfrak{ab} = \omega A$; a més a més, $\omega \in \mathfrak{a}$ i està definit a menys d'elements invertibles de A. D'altra banda, com que la norma és multiplicativa i $\mathrm{N}(\mathfrak{a}) \geq 1$, obtenim que, per a tot nombre real positiu x, podem escriure l'equivalència $\mathrm{N}(\mathfrak{b}) \leq x \Longleftrightarrow |\mathrm{N}(\omega)| \leq x\mathrm{N}(\mathfrak{a})$; en particular, l'assignació $\mathfrak{b} \mapsto \omega$ defineix una aplicació $S(x,\mathfrak{A}) \longrightarrow \overline{S}(x,\mathfrak{a})$. Aquesta aplicació és injectiva ja que A és un anell de Dedekind i, per tant, hi ha descomposició única dels ideals com a producte d'ideals primers, de manera que si $\mathfrak{ab} = \mathfrak{ab}'$, aleshores $\mathfrak{b} = \mathfrak{b}'$. D'altra banda, donat $\omega \in \mathfrak{a}$, $\omega \neq 0$, tal que $\mathrm{N}(\omega) \leq x\mathrm{N}(\mathfrak{a})$, el quocient $\mathfrak{b} := \omega A\mathfrak{a}^{-1}$ és un ideal enter de $\mathfrak{A}$, ja que $\omega \in \mathfrak{a}$, de norma $\leq x$; i, en conseqüència, l'aplicació és exhaustiva. Això demostra la igualtat que volíem. □

D'aquesta manera, la prova del teorema queda reduïda a la prova de la igualtat

$$\lim_{x\to+\infty} \frac{\#\overline{S}(x,\mathfrak{a})}{x} = \frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|\Delta_K|}},$$

per a qualsevol ideal enter $\mathfrak{a} \in \mathfrak{A}^{-1}$. Ara, recordem que $\mathfrak{a}$ és un grup abelià lliure de rang $n := [K:\mathbb{Q}] = r_1 + 2r_2$ i que A^* és el producte cartesià del grup (finit) de les arrels de la unitat de K per un grup abelià lliure de rang $r := r_1 + r_2 - 1$. Prenguem una $\mathbb{Z}$-base de $\mathfrak{a}$, $\alpha_1, \ldots, \alpha_n \in \mathfrak{a} \subseteq A \subseteq K$, i un sistema fonamental d'unitats $u_1, \ldots, u_r \in A^*$. Denotem també, com és habitual, per $\sigma_1, \ldots, \sigma_{r_1}$ les immersions reals de K, per $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ un sistema de representants de les parelles d'immersions complexes conjugades no reals de K, i per $\sigma_{r_1+r_2+j}$, $1 \leq j \leq r_2$, la imersió complexa conjugada de la σ_{r_1+j}.

Amb aquestes notacions, considerem el conjunt $E(x, \{\alpha_j\}_{1\leq j\leq n})$ format per tots els vectors no nuls $y := (y_1, \ldots, y_n) \in \mathbb{Z}^n$ per als quals se satisfan les dues propietats següents: si posem $\omega := \sum_{j=1}^{n} y_j\alpha_j \in \mathfrak{a}$, aleshores

(a) $|\mathrm{N}(\omega)| \leq x\mathrm{N}(\mathfrak{a})$, i

(b) existeixen nombres reals $0 \leq c_k < 1$, $1 \leq k \leq r$, tals que per a tot índex i, $1 \leq i \leq n$, se satisfà que $\log(|\sigma_i(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}}) = \sum_{k=1}^{r} c_k \log|\sigma_i(u_k)|$.

La primera propietat expressa, simplement, que $\omega \in A^*\overline{S}(x,\mathfrak{a})$; la segona propietat ens permetrà obtenir el factor w de la fórmula que volem provar.

Lema 15.3.5. *Se satisfà la igualtat* $w\#\overline{S}(x,\mathfrak{a}) = \#E(x, \{\alpha_i\}_{1\leq i\leq n})$.

Demostració: Considerem la immersió logarítmica de K^* en $\mathbb{R}^{r_1+r_2}$, donada, per a tot element $\omega \in K^*$, per l'assignació $\omega \mapsto \overline{\log}(\omega)$, on $\overline{\log}(\omega)$ és el vector

$$(\log|\sigma_1(\omega)|, \ldots, \log|\sigma_{r_1}(\omega)|, 2\log|\sigma_{r_1+1}(\omega)|, \ldots, 2\log|\sigma_{r_1+r_2}(\omega)|).$$

Recordem que la imatge per $\overline{\log}$ de les unitats A^* està inclosa en l'hiperplà $H \subseteq \mathbb{R}^{r_1+r_2}$ definit per $y_1 + \cdots + y_{r_1+r_2} = 0$, i que $\overline{\log}(u_1), \ldots, \overline{\log}(u_r)$ és una $\mathbb{R}$-base de H; no només

això, sinó que H és l'hiperplà de $\mathbb{R}^{r_1+r_2}$ que s'obté de la imatge de $\overline{\log}$ en estendre escalars a $\mathbb{R}$. Anem a veure que, donat un element no nul $\omega \in K$, existeixen nombres reals $c_1, \dots, c_r$ tals que, per a $1 \leq i \leq n$, podem escriure les igualtats

$$\log(|\sigma_i(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}}) = \sum_{k=1}^{r} c_k \log(|\sigma_i(u_k)|). \tag{15.3.1}$$

El vector de r components $\left(\log(|\sigma_1(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}}), \dots, \log(|\sigma_r(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}})\right)$ és combinació lineal dels r vectors $(\log(|\sigma_1(u_k)|), \dots, \log(|\sigma_r(u_k)|))$, $1 \leq k \leq r$, ja que aquests formen una $\mathbb{R}$-base de $\mathbb{R}^r$. Per tant, existeixen nombres reals c_k, $1 \leq k \leq r$, tals que (15.3.1) se satisfà per a $1 \leq i \leq r$. Recordem que, si posem $e_i := 1$ per a $1 \leq i \leq r_1$, i $e_i := 2$ per a $r_1 + 1 \leq i \leq n$, se satisfan les igualtats

$$\sum_{i=1}^{r_1+r_2} e_i \log|\sigma_i(u_k)| = 0, \qquad 1 \leq k \leq r. \tag{15.3.2}$$

Però també se satisfà la igualtat

$$\sum_{i=1}^{r_1+r_2} e_i \log(|\sigma_i(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}}) = 0, \tag{15.3.3}$$

ja que podem escriure que

$$\begin{aligned}\sum_{i=1}^{r_1+r_2} e_i \log(|\sigma_i(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}}) &= \log \prod_{i=1}^{r_1+r_2} \left(|\sigma_i(\omega)|^{e_i}|\mathrm{N}(\omega)|^{-\frac{e_i}{n}}\right) \\ &= \log \prod_{i=1}^{n} \left(|\sigma_i(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}}\right) = \log \frac{\prod_{i=1}^{n}|\sigma_i(\omega)|}{|\mathrm{N}(\omega)|} = \log(1) = 0.\end{aligned}$$

En conseqüència, com que $r_1 + r_2 = r + 1$, obtenim la igualtat (15.3.1) per a $i = r + 1$ a partir de les igualtats (15.3.2), (15.3.3), i (15.3.1) per a $1 \leq i \leq r$. I les altres en són conseqüència, ja que $|\sigma_{r_1+r_2+i}(\omega)| = |\sigma_{r_1+i}(\omega)|$ per a $1 \leq i \leq r_2$ i tot $\omega \in K^*$.

Si multipliquem $\omega \in K^*$ per un element de A^*, $u := \varepsilon u_1^{m_1} \cdot \cdots \cdot u_r^{m_r}$, on ε és una arrel de la unitat de K, com que $\log(|\sigma_i(\varepsilon)|) = 0$, obtenim que, per a tot índex i, $1 \leq i \leq n$, se satisfà la igualtat $\log\left(|\sigma_i(u\omega)||\mathrm{N}(u\omega)|^{-\frac{1}{n}}\right) = \sum_{k=1}^{r}(c_k + m_k)\log|\sigma_i(u_k)|$, ja que $|\mathrm{N}(u)|^{-\frac{1}{n}} = 1$. En particular, per a tot element no nul $\omega \in K$, podem elegir els exponents m_k de manera única a fi que se satisfacin les desigualtats $0 \leq c_k + m_k < 1$; dit d'una altra manera, existeixen exactament w elements associats de ω, un per a cada arrel de la unitat de K, tals que per als c_k corresponents se satisfan les desigualtats $0 \leq c_k < 1$.

Això ens permet acabar fàcilment la demostració del lema. En efecte, dir que la classe mòdul unitats d'un element no nul $\omega \in A$ pertany al conjunt $\overline{S}(x, \mathfrak{a})$, equival a dir que ω es pot escriure en la forma $\omega := \sum_{j=1}^{n} y_j\alpha_j \in \mathfrak{a}$ amb els $y_j \in \mathbb{Z}$ no tots nuls i satisfà la propietat (a); i el que acabem de provar equival a dir que hi ha exactament w elements associats a ω que, a més a més, satisfan la propietat (b). Això equival a la igualtat buscada. □

En conseqüència, només cal provar la igualtat

$$\lim_{x\to+\infty}\frac{\#E(x,\{\alpha_j\})}{x}=\frac{2^{r_1}(2\pi)^{r_2}R}{\sqrt{|\Delta_K|}},$$

on ha desaparegut de la fórmula el factor w.

El pas següent consisteix a transformar el límit en una integral; concretament, en el volum d'una certa regió de $\mathbb{R}^n$. Per a això, ens interessa fer ús d'alguna definició. Donats nombres reals $y_1,\dots,y_n$, escriurem

$$\omega:=\sum_{j=1}^n y_j\alpha_j,\qquad \sigma_i(\omega):=\sum_{j=1}^n y_j\sigma_i(\alpha_j),\qquad \mathrm{N}(\omega):=\prod_{i=1}^n\sigma_i(\omega),$$

on σ_i són, com abans, les immersions complexes de K. Per a tot nombre real positiu x, posarem $B(x,\{\alpha_j\})$ per a designar el conjunt dels vectors $y:=(y_1,\dots,y_n)\in\mathbb{R}^n$ per als quals se satisfan les propietats següents:

(a') $0<|\mathrm{N}(\omega)|\le x\mathrm{N}(\mathfrak{a})$; i

(b') existeixen nombres reals $0\le c_k<1$, $1\le k\le r$, tals que per a tot índex i, $1\le i\le n$, se satisfà la igualtat $\log(|\sigma_i(\omega)||\mathrm{N}(\omega)|^{-\frac{1}{n}})=\sum_{k=1}^r c_k\log|\sigma_i(u_k)|$.

Observem que aquesta segona propietat té sentit ja que, si se satisfà la primera, aleshores cada un dels nombres $\sigma_i(\omega)$ és no nul perquè ho és el seu producte. A més a més, aquest conjunt és un subconjunt fitat de $\mathbb{R}^n$. En efecte, la propietat (b') ens permet assegurar que, si $y\in B(x,\{\alpha_j\})$, aleshores, $|\sigma_i(\omega)|=|\mathrm{N}(\omega)|^{\frac{1}{n}}e^{\sum_{k=1}^r c_k\log|\sigma_i(u_k)|}$; i, en tenir en compte la propietat (a'), que $|\sigma_i(\omega)|\le(x\mathrm{N}(\mathfrak{a}))^{\frac{1}{n}}e^{rM}$, on $M:=\max\{|\log(|\sigma_i(u_k)|)|\}_{i,k}$ és una fita que només depèn del cos K i del sistema fonamental d'unitats elegit. Per tant, les coordenades dels vectors ω han d'estar fitades, ja que ho estan les dels $\sigma_i(\omega)$, per a tot índex i.

Convé estudiar el conjunt $B(x,\{\alpha_j\})$ de més aprop. En particular, cal veure que, si $\overline{B}(x,\{\alpha_j\})$ denota l'adherència del conjunt $B(x,\{\alpha_j\})$, aleshores el complementari de $B(x,\{\alpha_j\})$ en la seva adherència, $\overline{B}(x,\{\alpha_j\})$, és un conjunt de mesura zero. Ara bé, el conjunt $B(x,\{\alpha_j\})$ és un subconjunt del conjunt dels vectors $(y_1,\dots,y_n)\in\mathbb{R}^n$ per als quals se satisfà (a'); per tant, $\overline{B}(x,\{\alpha_j\})$ és un subconjunt del conjunt dels vectors $(y_1,\dots,y_n)\in\mathbb{R}^n$ per als quals se satisfà la desigualtat $|\mathrm{N}(\omega)|\le x\mathrm{N}(\mathfrak{a})$; i només hem afegit els vectors per als quals se satisfà la igualtat $\mathrm{N}(\omega)=0$. Si veiem que aquests vectors formen un conjunt de mesura zero ja haurem acabat.

Notem, en primer lloc, que la matriu $(\sigma_i(\alpha_j))$ és invertible. En efecte, el valor absolut del seu determinant és el producte del factor 2^{r_2} per la malla de la xarxa associada a l'ideal $\mathfrak{a}$ a través de la immersió canònica de A en $\mathbb{R}^n$ (cf. la proposició **4.3.2**), ja que els elements α_j formen una $\mathbb{Z}$-base de $\mathfrak{a}$; ara bé, la malla d'aquesta xarxa és $2^{-r_2}\sqrt{|\Delta_K|}\mathrm{N}(\mathfrak{a})\neq 0$ (cf. el corol·lari **4.3.5**); en particular, obtenim la igualtat $|\det(\sigma_i(\alpha_j))|=\sqrt{|\Delta_K|}\mathrm{N}(\mathfrak{a})$, que utilitzarem més endavant.

Com a conseqüència d'aquest fet, l'aplicació lineal $\mathbb{R}^n\xrightarrow{f}\mathbb{R}^n$ definida per la matriu $(\sigma_i(\alpha_j))$ és un automorfisme de $\mathbb{R}^n$ i cadascuna de les formes lineals $(y_1,\dots,y_n)\mapsto\sigma_i(\omega)$

és no nul·la. Així, els vectors $(y_1, \dots, y_n)$ tals que $\mathrm{N}(\omega) = 0$, que formen la reunió dels nuclis d'aquestes formes lineals, estan en un conjunt algebraic de codimensió 1 de $\mathbb{R}^n$; per tant, formen un subconjunt de mesura zero de $\mathbb{R}^n$.

Lema 15.3.6. *El conjunt $\overline{B}(1, \{\alpha_j\})$ és mesurable i*

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n = \lim_{x \to +\infty} \frac{\#E(x, \{\alpha_j\})}{x}.$$

Demostració: Comencem la prova veient que el nombre de punts de $\overline{B}(x, \{\alpha_j\})$ de coordenades enteres i diferents de $(0, \dots, 0)$ és exactament el nombre $\#E(x, \{\alpha_j\})$. Disposem de les inclusions trivials $E(x, \{\alpha_j\}) \subseteq B(x, \{\alpha_j\}) \subseteq \overline{B}(x, \{\alpha_j\})$.

Sigui $(y_1, \dots, y_n) \in \overline{B}(x, \{\alpha_j\})$ un element tal que $y_j \in \mathbb{Z}$ per a tot índex j; en particular, $\omega := \sum_{j=1}^{n} y_j \alpha_j \in \mathfrak{a}$. Si, per a algun índex $1 \leq i \leq n$, tinguéssim la igualtat $\sigma_i(\omega) = 0$, com que $\omega \in \mathfrak{a}$, tots els conjugats $\sigma_i(\omega)$ de ω serien nuls i, com que $\alpha_1, \dots, \alpha_n$ és una $\mathbb{Z}$-base de $\mathfrak{a}$, hauria de ser $y_j = 0$ per a tot índex j; per tant, cap dels nombres $\sigma_i(\omega)$ no pot ser zero i, aleshores, $(y_1, \dots, y_n) \in B(x, \{\alpha_j\}) \cap \mathbb{Z}^n = E(x, \{\alpha_j\})$. D'altra banda, l'homotècia de raó $x^{-\frac{1}{n}}$ transforma el conjunt $\overline{B}(x, \{\alpha_j\})$ en el conjunt $\overline{B}(1, \{\alpha_j\})$; en efecte, la propietat (b') és invariant per homotècies mentre que la primera queda afectada en un costat de la desigualtat per la potència n-èsima de la raó de l'homotècia. Els punts de $E(x, \{\alpha_j\})$ corresponen, via aquesta homotècia, als punts de $\overline{B}(1, \{\alpha_j\})$ de coordenades de la forma $x^{-\frac{1}{n}} y_j$, amb $y_j \in \mathbb{Z}$. Així, per a cada nombre real $x > 0$, disposem d'una partició del conjunt $\overline{B}(1, \{\alpha_j\})$ formada per tants n-cubs d'aresta $x^{-\frac{1}{n}}$ com punts de coordenades enteres de $\overline{B}(x, \{\alpha_j\})$; per definició de la mesura (de Riemann) del conjunt $\overline{B}(1, \{\alpha_j\})$, obtenim la igualtat

$$\begin{aligned} \int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n &= \lim_{x \to +\infty} \frac{\text{nombre de punts de } \overline{B}(x, \{\alpha_j\}) \cup \mathbb{Z}^n}{\text{volum del } n\text{-cub d'aresta } x^{-\frac{1}{n}}} \\ &= \lim_{x \to +\infty} \frac{\#E(x, \{\alpha_j\})}{x}, \end{aligned}$$

com volíem demostrar, ja que el punt $(0, \dots, 0)$ no afecta en el pas al límit. □

Per tant, la prova del teorema ha quedat reduïda a demostrar la igualtat

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n = \frac{2^{r_1} (2\pi)^{r_2} R}{\sqrt{|\Delta_K|}}.$$

Considerem el canvi de variables donat de la manera següent:

$$\begin{aligned} at2z_k &:= \sum_{j=1}^{n} y_j \sigma_k(\alpha_j), && 1 \leq k \leq r_1, \\ z_k + iz_{r_2+k} &:= \sum_{j=1}^{n} y_j \sigma_k(\alpha_j), && r_1 + 1 \leq k \leq r_1 + r_2, at \\ z_k - iz_{r_2+k} &:= \sum_{j=1}^{n} y_j \sigma_{r_2+k}(\alpha_j), && r_1 + 1 \leq k \leq r_1 + r_2. \end{aligned}$$

Observem que el canvi consisteix a fer que les noves variables siguin les $\sigma_k(\omega)$, per a $1 \le k \le r_1 + r_2$; en particular, com que les variables y_k són reals, les immersions $\sigma_1, \dots, \sigma_{r_1}$ són reals, i les immersions $\sigma_{r_1+r_2+k}$ són les conjugades no reals de les σ_{r_1+k}, per a $1 \le k \le r_2$, les variables z_k, per a $1 \le k \le n$, són totes reals. El càlcul del jacobià es fa de manera rutinària; de fet, com que és un canvi lineal, el jacobià és el determinant de la matriu del canvi. Aquest determinant ja s'ha calculat en fer l'estudi de la malla de la xarxa $\sigma(\mathfrak{a})$; en resulta la igualtat $\left|\dfrac{\partial(z_1,\dots,z_n)}{\partial(y_1,\dots,y_n)}\right| = 2^{-r_2}\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})$; en conseqüència, si $\overline{B}'(1,\{\alpha_j\})$ designa el conjunt d'integració que correspon a les noves variables z_k, obtenim la igualtat

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n = \frac{2^{r_2}}{\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})} \int_{\overline{B}'(1,\{\alpha_j\})} dz_1 \dots dz_n.$$

Fem, encara, un canvi a coordenades polars per a les variables z_k, $r_1 + 1 \le k \le n$, de la manera següent:

$$\begin{aligned} z_k &=: \rho_k, && 1 \le k \le r_1, \\ z_{r_1+k} &=: \rho_{r_1+k}\cos(\theta_k), && 1 \le k \le r_2, \\ z_{r_1+r_2+k} &=: \rho_{r_1+k}\sin(\theta_k), && 1 \le k \le r_2. \end{aligned}$$

El jacobià d'aquest canvi de variables és $\left|\dfrac{\partial(z_1,\dots,z_n)}{\partial(\rho_1,\dots,\rho_{r_1+r_2},\theta_1,\dots,\theta_{r_2})}\right| = \rho_{r_1+1}\cdots\rho_{r_1+r_2}$. Ara, el nou conjunt d'integració és el subconjunt de $\mathbb{R}^n$ determinat per les desigualtats

$$0 < \prod_{j=1}^{r_1+r_2} |\rho_j|^{e_j} \le \mathrm{N}(\mathfrak{a}), \tag{15.3.4}$$

$$\log|\rho_k| = \frac{1}{n}\log \prod_{j=1}^{r_1+r_2} |\rho_j|^{e_j} + \sum_{j=1}^{r} c_j \log|\sigma_k(u_j)|, \tag{15.3.5}$$

i les variables sotmeses a les condicions següents:

$$0 \le c_j < 1, \quad 1 \le j \le r, \qquad \left.\begin{matrix} 0 \le \theta_k < 2\pi, \\ \rho_{r_1+k} > 0, \end{matrix}\right\} \quad 1 \le k \le r_2, \qquad \rho_k \in \mathbb{R}, \quad 1 \le k \le r_1.$$

Amb aquest canvi, i si denotem el conjunt d'integració per $\overline{B}''(1,\{\alpha_j\})$, obtenim la igualtat

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n = \frac{2^{r_2}}{\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})} \int_{\overline{B}''(1,\{\alpha_j\})} \rho_{r_1+1}\cdots\rho_{r_1+r_2} d\rho_1 \dots d\rho_{r_1+r_2} d\theta_1 \dots d\theta_{r_2}.$$

El càlcul de les integrals que corresponen a les variables θ_k proporciona la nova igualtat

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n = \frac{2^{r_2}(2\pi)^{r_2}}{\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})} \int_{\overline{B}''(1,\{\alpha_j\})} \rho_{r_1+1}\cdots\rho_{r_1+r_2} d\rho_1 \dots d\rho_{r_1+r_2}.$$

En el domini d'integració, les variables ρ_k, $1 \le k \le r_1$, apareixen sempre en valor absolut; i podem considerar-les positives si treiem un factor 2 per a cadascuna d'elles. S'obté que

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \dots dy_n = \frac{2^{r_1+r_2}(2\pi)^{r_2}}{\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})} \int_{\overline{B}''(1,\{\alpha_j\})} \rho_{r_1+1}\cdots\rho_{r_1+r_2} d\rho_1 \dots d\rho_{r_1+r_2},$$

amb les restriccions $\rho_k > 0$, per a tot índex $1 \le k \le r_1 + r_2$.

Es tracta d'anar a cercar el regulador de K. Per a això, encara convé fer el canvi de variable $v_k := \rho_k^{e_k}$, per a $1 \leq k \leq r_1 + r_2 = r + 1$, de manera que $v_k > 0$. Clarament, l'invers del jacobià del canvi és $2^{r_2}\rho_{r_1+1} \cdots \rho_{r_1+r_2}$, i el domini d'integració és el nou conjunt $C(\mathfrak{a})$ format pels vectors $(v_1, \ldots, v_{r+1}) \in \mathbb{R}^{r+1}$ tals que $v_k > 0$, per a $1 \leq k \leq r+1$, $0 < v_1 \cdots v_{r+1} \leq \mathrm{N}(\mathfrak{a})$, i $\log(v_k) = \dfrac{e_k}{n} \log(v_1 \cdots v_{r+1}) + e_k \sum_{j=1}^{r} c_j \log|\sigma_k(\alpha_j)|$, per a $0 \leq c_j < 1$. La integral que cal calcular queda, doncs, en la forma

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \ldots dy_n = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})} \int_{C(\mathfrak{a})} dv_1 \ldots dv_{r+1}.$$

Les darreres igualtats de la definició de $C(\mathfrak{a})$ defineixen un nou canvi de variables; en efecte, podem considerar $t := v_1 \cdots v_{r+1}$, i les c_j, $1 \leq j \leq r$, com a variables noves, de manera que cal calcular el jacobià del canvi i integrar per a $0 \leq c_k < 1$ i $0 < t \leq \mathrm{N}(\mathfrak{a})$. El càlcul del jacobià dóna el determinant

$$\frac{\partial(v_1, \ldots, v_{r+1})}{\partial(t, c_1, \ldots, c_r)} = \frac{v_1, \ldots, v_{r+1}}{t} \det(e_j c_j \log|\sigma_j(u_k)|) = \det(e_j c_j \log|\sigma_j(u_k)|) = \pm R,$$

per definició del regulador de K. Per tant, obtenim el resultat final

$$\int_{\overline{B}(1,\{\alpha_j\})} dy_1 \ldots dy_n = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta|}\mathrm{N}(\mathfrak{a})} \int_0^{\mathrm{N}(\mathfrak{a})} \int_0^1 \cdots \int_0^1 R dc_1 \ldots dc_r dt = \frac{2^{r_1}(2\pi)^{r_2} R}{\sqrt{|\Delta|}},$$

com volíem provar. □

15.4 Residu de la funció zeta de Dedekind en $s = 1$

Donat un cos de nombres K, hem definit la funció zeta de Dedekind associada a aquest cos com la funció donada en el semiplà $\Re(s) > 1$ per la suma de la sèrie $\displaystyle\sum_{\mathfrak{a} \subseteq A} \mathrm{N}(\mathfrak{a})^{-s}$; d'aquesta manera, hem provat que la funció $\zeta_K(s)$ és analítica en el semiplà $\Re(s) > 1$. Podríem demostrar que aquesta funció admet una extensió meromorfa a tot el pla complex, holomorfa llevat d'un únic pol, i simple, en el punt $s = 1$. A més a més, i això també és vàlid per a les funcions zeta de Riemann i L de Dirichlet, la funció zeta de Dedekind admet una equació funcional. No veurem cap d'aquests resultats, però ens interessa fer el càlcul del residu de la funció $\zeta_K(s)$ en $s = 1$. A partir d'aquest resultat, podrem obtenir algunes fórmules tancades per al càlcul del nombre de classes d'alguns cossos de nombres; concretament, dels cossos quadràtics i dels cossos ciclotòmics de les arrels p-èsimes de la unitat, p primer.

Mantindrem les notacions de la secció anterior. El resultat que es tracta d'establir és el següent.

Teorema 15.4.1 (Fórmula del residu)**.** *Siguin K un cos de nombres i $\zeta_K(s)$ la funció zeta de Dedekind associada a K en el semiplà $\Re(s) > 1$. Aleshores, si mantenim $s \in \mathbb{R}$, $s > 1$, se satisfà la igualtat $\displaystyle\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h R}{w\sqrt{|\Delta_K|}}$, on R és el regulador, w el nombre d'arrels de la unitat, r_1 el nombre d'immersions reals, i r_2 el nombre de parelles d'immersions complexes conjugades no reals de K, i Δ_K el discriminant absolut, i h el nombre de classes d'ideals de l'anell dels enters de K.*

Abans de procedir a la demostració d'aquest resultat, convé disposar d'un resultat general per a sèries de Dirichlet.

Lema 15.4.2. *Sigui $F(s) := \sum_{n\geq 1} f(n)n^{-s}$ una sèrie de Dirichlet. Per a tot nombre natural $m \geq 1$, posem $S(m) := f(1) + \cdots + f(m)$, la suma parcial m-èsima de la sèrie $\sum_{n\geq 1} f(n)$. Suposem que existeix el límit $\lim \dfrac{S(m)}{m} =: c \in \mathbb{C}$. Aleshores, la sèrie $F(s)$ és convergent en $\Re(s) > 1$ i $\lim_{s\to 1^+}(s-1)F(s) = c$.*

Demostració: En virtut de les propietats generals de convergència de les sèries de Dirichlet, podem suposar que $s \in \mathbb{R}$. Per a la primera part, només cal veure que, si $s > 1$, aleshores la sèrie $F(s)$ és convergent. Fixem momentàniament dos nombres enters $m, h \geq 1$; podem escriure les sumes parcials de la sèrie $F(s)$ de la manera següent:

$$\begin{aligned}\sum_{n=m}^{m+h} f(n)n^{-s} &= \sum_{n=m}^{m+h}(S(n) - S(n-1))n^{-s}\\ &= \frac{S(m+h)}{(m+h)^s} - \frac{S(m-1)}{m^s} + \sum_{n=m}^{m+h-1} S(n)\left(n^{-s} - (n+1)^{-s}\right)\\ &= \frac{S(m+h)}{(m+h)^s} - \frac{S(m-1)}{m^s} + s\sum_{n=m}^{m+h-1} S(n)\int_n^{n+1} x^{-(s+1)}dx.\end{aligned}$$

Si tenim en compte la hipòtesi sobre el límit, obtenim que existeix una constant $C' > 0$ tal que, per a tot nombre enter $m \geq 1$, se satisfà una desigualtat $\left|\dfrac{S(m)}{m}\right| \leq C'$; o, d'una altra manera, $|S(m)| \leq C'm$. En conseqüència, per a $s > 1$, podem escriure que

$$\begin{aligned}&|S(m+h)(m+h)^{-s} - S(m-1)m^{-s}| \leq |S(m+h)(m+h)^{-s}| + |S(m-1)m^{-s}|\\ &\leq C'(m+h)^{-(s-1)} + C'(m-1)m^{-s} \leq C'(m+h)^{-(s-1)} + C'm^{-(s-1)} \leq 2C'm^{-(s-1)};\end{aligned}$$

similarment, per a la suma d'integrals obtenim que

$$\begin{aligned}&\left|s\sum_{n=m}^{m+h-1} S(n)\int_n^{n+1} x^{-(s+1)}dx\right| \leq s\sum_{n=m}^{m+h-1}|S(n)|\int_n^{n+1} x^{-(s+1)}dx\\ &\leq sC'\sum_{n=m}^{m+h-1}\int_n^{n+1} nx^{-(s+1)}dx \leq sC'\sum_{n=m}^{m+h-1}\int_n^{n+1} x^{-s}dx\\ &= sC'\int_m^{m+h} x^{-s}dx \leq sC'\int_m^{+\infty} x^{-s}dx = sC'(s-1)^{-1}m^{-(s-1)}.\end{aligned}$$

Per tant, per a tot nombre $s > 1$ i tota parella d'enters $m, h \geq 1$, obtenim la desigualtat

$$\left|\sum_{n=m}^{m+h} f(n)n^{-s}\right| \leq 2C'm^{-(s-1)} + sC'(s-1)^{-1}m^{-(s-1)} = C'm^{-(s-1)}\left(2 + \frac{s}{s-1}\right),$$

de manera que la sèrie $F(s)$ és convergent, ja que $\lim m^{-(s-1)} = 0$, quan m creix.

Cal veure que $\lim_{s\to 1^+}(s-1)F(s)=c$. Per a això, compararem la sèrie $F(s)$ amb la sèrie de Riemann. Per a $s>1$, podem escriure les igualtats

$$\begin{aligned}F(s)-c\zeta(s)&=\sum_{n\geq 1}\frac{f(n)-c}{n^s}=\sum_{n\geq 1}\left(\frac{S(n)-cn}{n^s}-\frac{S(n-1)-c(n-1)}{n^s}\right)\\&=\sum_{n\geq 1}\left(\frac{S(n)-cn}{n^s}-\frac{S(n)-cn}{(n+1)^s}\right).\end{aligned}$$

En efecte, la diferència entre les sumes parcials N-èsimes de les dues sèries es pot calcular en la forma

$$\sum_{n=1}^{N}\left(\frac{S(n)-cn}{(n+1)^s}-\frac{S(n-1)-c(n-1)}{n^s}\right)=\frac{S(N)-cN}{N}\frac{N}{N+1}\frac{1}{(N+1)^{s-1}};$$

ara bé, com que $\lim\dfrac{S(n)-cn}{n}=0$, la successió de terme general $\varepsilon_n:=\dfrac{S(n)-cn}{n}$ és fitada per una constant $C>0$, independent de s, i la diferència de les sumes parcials tendeix a zero, de manera que les dues sèries tenen el mateix caràcter de convergència i la mateixa suma.

Si tenim en compte la igualtat de més amunt, podem escriure, per a $s>1$,

$$|F(s)-c\zeta(s)|=s\left|\sum_{n\geq 1}n\varepsilon_n\int_n^{n+1}x^{-(s+1)}dx\right|\leq s\sum_{n\geq 1}|\varepsilon_n|\int_n^{n+1}x^{-s}dx;$$

en multiplicar per $s-1$, i per a tot enter $N\geq 1$, aquesta desigualtat es transforma en

$$|(s-1)F(s)-c(s-1)\zeta(s)|\leq Cs(s-1)\sum_{n=1}^{N}\int_n^{n+1}x^{-1}dx+s(s-1)\sum_{n>N}|\varepsilon_n|\int_n^{n+1}x^{-s}dx.$$

Com que $\lim\varepsilon_n=0$, donat un nombre real $\delta>0$, arbitrari, podem trobar un enter N, que depèn de δ, però no de s, de manera que $|\varepsilon_n|\leq\delta$, sempre que $n>N$; això ens permet escriure que

$$\begin{aligned}|(s-1)F(s)-c(s-1)\zeta(s)|&\leq Cs(s-1)\int_{n=1}^{N+1}x^{-1}dx+\delta s(s-1)\int_{N+1}^{+\infty}x^{-s}dx\\&=Cs(s-1)\log(N+1)+\delta s(N+1)^{1-s},\end{aligned}$$

independentment de s. Si prenem límit quan s tendeix a 1, l'expressió de la dreta tendeix a δ, de manera que $\lim_{s\to 1^+}|(s-1)F(s)-c(s-1)\zeta(s)|\leq\delta$; com que $\delta>0$ és arbitrari, obtenim les igualtats $\lim_{s\to 1^+}(s-1)F(s)=c\lim_{s\to 1^+}(s-1)\zeta(s)=c$, ja que el residu de la funció zeta de Riemann en $s=1$ és 1. Això acaba la prova. □

Ara podem procedir, de manera senzilla, a la prova de la fórmula del residu per a la funció zeta de Dedekind en el punt $s=1$.

Demostració (de la fórmula del residu): De fet, només cal tenir en compte el teorema de Dirichlet-Dedekind provat a la secció anterior, aquest lema, i la definició de la funció. En efecte, com que la sèrie $\sum_{\mathfrak{a}\subseteq A}\mathrm{N}(\mathfrak{a})^{-s}$ és absolutament convergent, podem agrupar els

termes com ens plagui; això ho farem de la manera següent: per a cada nombre enter $n \geq 1$, sigui $f(n)$ el nombre d'ideals enters $\mathfrak{a} \subseteq A$ tals que $\mathrm{N}(\mathfrak{a}) = n$; sabem que això té sentit perquè només hi ha una quantitat finita d'ideals de norma donada. D'aquesta manera, per a $s \in \mathbb{R}$, $s > 1$, podem escriure que $\zeta_K(s) = \sum_{n\geq 1} f(n)n^{-s}$; ara, el lema anterior ens assegura que, si existeix el límit $\lim \frac{S(n)}{n} = \kappa$, on $S(n) := f(1) + \cdots + f(n)$, aleshores el residu de $\zeta_K(s)$ en $s = 1$ és κ. Però el teorema de Dirichlet-Dedekind (de fet el corol·lari), ens permet assegurar que el límit existeix amb $\kappa = \frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|\Delta|}}$, de manera que el teorema queda demostrat. □

15.5 Fórmula analítica del nombre de classes dels cossos quadràtics

La fórmula del residu de la funció zeta de Dedelind associada a un cos de nombres K conté com a factor el nombre de classes d'ideals de l'anell dels enters de K. Aquest fet ens permetrà obtenir una expressió analítica per al càlcul d'aquest nombre de classes en el cas quadràtic i en el cas ciclotòmic. En aquesta secció estudiarem el cas quadràtic.

Sigui, doncs, $K := \mathbb{Q}(\sqrt{D})$ el cos quadràtic de discriminant $\Delta_K = D$; recordem que, en el cas dels cossos quadràtics, el discriminant determina el cos. Considerem, també, el caràcter de Kronecker χ_D associat a K; és a dir, el caràcter quadràtic de conductor D. Recordem que aquest caràcter descriu les lleis de ramificació dels nombres primers en l'anell dels enters de K de la manera següent:

(a) si $p\mathbb{Z}$ és un ideal primer no nul de $\mathbb{Z}$ que descompon com a producte de dos ideals primers diferents de K, aleshores $\chi_D(p) = 1$;

(b) si l'extensió de $p\mathbb{Z}$ a K és primer, aleshores $\chi_D(p) = -1$; i

(c) si $p\mathbb{Z}$ ramifica en K, aleshores $\chi_D(p) = 0$.

Aquest fet fa senzill calcular la funció zeta de Dedekind de K. En efecte, podem establir el resultat següent.

Proposició 15.5.1. *Siguin K un cos quadràtic, D el seu discriminant, i χ_D el caràcter de Kronecker de conductor D. Aleshores, en el semiplà $\Re(s) > 1$, la funció zeta de Dedekind associada al cos K admet l'expressió $\zeta_K(s) = \zeta(s)L(\chi_D, s)$, on $\zeta(s)$ és la funció zeta de Riemann i $L(\chi_D, s)$ la funció L de Dirichlet associada al caràcter χ_D.*

Demostració: En el semiplà $\Re(s) > 1$, podem considerar les expressions com a productes d'Euler de les funcions involucades; s'obtenen les fórmules

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \qquad \zeta_K(s) = \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}, \qquad L(\chi_K, s) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

Ara bé, l'observació anterior sobre la descomposició dels nombres primers en K, afegit al fet que els productes són absolutament convergents i que, per tant, podem calcular-los en

l'ordre que ens plagui, ens permet escriure que, per a tot nombre primer p, se satisfà la igualtat

$$\left(1-\frac{1}{p^s}\right)\left(1-\frac{\chi_D(p)}{p^s}\right)=\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}\right).$$

En efecte, quan $p\mathbb{Z}$ descompon o ramifica, per a tot divisor primer $\mathfrak{p}$ de $p\mathbb{Z}$ és $\mathrm{N}(\mathfrak{p})=p$, mentre que si l'extensió de $p\mathbb{Z}$ a K és un ideal primer $\mathfrak{p}$, aleshores $\mathrm{N}(\mathfrak{p})=p^2$. Per tant, obtenim les igualtats

$$\begin{aligned}\zeta_K(s)&=\prod_p\prod_{\mathfrak{p}|p}(1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}=\prod_p(1-p^{-s})^{-1}(1-\chi_D(p)p^{-s})^{-1}\\&=\prod_p(1-p^{-s})^{-1}\prod_p(1-\chi_D(p)p^{-s})^{-1}=\zeta(s)L(\chi_D,s),\end{aligned}$$

com volíem demostrar. □

Ja hem dit més amunt que la funció zeta de Dedekind d'un cos de nombres s'estén a una funció meromorfa del pla complex amb un únic pol, i simple, en $s=1$, encara que no ho hem demostrat. En el cas quadràtic, ho obtenim fàcilment com a conseqüència del resultat anterior.

Corol·lari 15.5.2. *Sigui K un cos quadràtic. La funció zeta de Dedekind associada al cos K admet una prolongació meromorfa a tot al pla complex amb un únic pol, i simple, en $s=1$. El residu en $s=1$ és $L(\chi_D,1)$, el valor de la funció L de Dirichlet associada al caràcter de Kronecker χ_D de conductor $D:=\Delta_K$.*

Demostració: El producte de les funcions $\zeta(s)$ i $L(\chi,s)$ és una funció que satisfà les condicions de l'enunciat i que coincideix amb la funció $\zeta_K(s)$ en el semiplà $\Re(s)>1$; només cal aplicar el principi de prolongació analítica. □

Com a conseqüència d'aquest resultat obtindrem una fórmula per al càlcul del nombre de classes d'ideals del cos K. En efecte, podem enunciar el resultat següent.

Teorema 15.5.3. *Sigui K un cos quadràtic. Siguin h el nombre de classes d'ideals de K, D el discriminant, i χ_D el caràcter de Kronecker de conductor D. Aleshores,*

$$h=\begin{cases}\dfrac{\sqrt{D}}{2\log(u)}L(\chi_D,1), & \text{si } D>0,\\[2ex] \dfrac{w\sqrt{-D}}{2\pi}L(\chi_D,1), & \text{si } D<0,\end{cases}$$

on u és la unitat fonamental del cos quadràtic real i w designa el nombre d'arrels de la unitat del cos imaginari.

Demostració: El teorema del residu de la funció zeta de Dedekind ens permet escriure, per al cas d'un cos quadràtic de discriminant D, la igualtat

$$L(\chi_D,1)=\lim_{s\to1}(s-1)\zeta(s)L(\chi_D,s)=\lim_{s\to1}\zeta_K(s)=\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|D|}},$$

on R és el regulador, i r_1, r_2, com sempre.

Si K és real, és a dir, si $D > 0$, aleshores $w = 2$, $r_1 = 2$, $r_2 = 0$, $r := r_1 + r_2 - 1 = 1$, i $R = \log(u)$, on u és la més petita de les unitats $u > 1$ de l'anell dels enters de K; la fórmula enunciada en resulta trivialment.

Anàlogament, si K és imaginari, aleshores, $r_1 = 0$, $r_2 = 1$, $r := r_1 + r_2 - 1 = 0$, i $R = 1$, mentre que $w = 2$, excepte quan $K = \mathbb{Q}(i)$, en què $w = 4$, o $K = \mathbb{Q}(\rho)$, ρ una arrel cúbica de la unitat, en què $w = 6$; la igualtat enunciada en resulta, també, trivialment. □

15.6 Fórmula analítica del nombre de classes dels cossos ciclotòmics

En aquesta secció es tracta de donar una fórmula analítica, semblant a la del cas quadràtic, per al càlcul del nombre de classes dels cossos ciclotòmics.

Siguin $m \geq 4$ un nombre enter parell, μ_m el grup de les arrels m-èsimes de la unitat i $K := \mathbb{Q}(\mu_m)$ el cos ciclotòmic de les arrels m-èsimes de la unitat. Observem que prendre m parell no és restrictiu, ja que si m és senar, aleshores $\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{2m})$; en canvi, simplificarà les notacions.

El fet de conèixer les lleis de descomposició dels nombres primers en K ens permet, com en el cas quadràtic, establir el resultat següent.

Teorema 15.6.1. *Sigui $K := \mathbb{Q}(\mu_m)$. La funció zeta de Dedekind associada al cos K admet una prolongació meromorfa a tot el pla complex amb un únic pol, i simple, en $s = 1$. En el semiplà $\Re(s) > 1$ la funció $\zeta_K(s)$ es pot escriure en la forma $\zeta_K(s) = \prod_\chi L(\chi, s)$, on $L(\chi, s)$ és la funció L de Dirichlet associada al caràcter χ, i χ recorre el conjunt dels caràcters primitius de conductor divisor de m, incloent-hi el caràcter trivial.*

Demostració: Per a la demostració d'aquest resultat farem servir de manera decisiva la descomposició explícita dels ideals primers en el cossos ciclotòmics $\mathbb{Q}(\mu_m)$. Comencem per recordar que si p és un nombre primer qualsevol, i si escrivim $m = p^r m'_p$, amb $r \geq 0$, $p \nmid m'_p$, aleshores, l'ideal generat per p en l'anell dels enters del cos K descompon com a producte de g_p ideals primers diferents, tots de grau residual f_p de manera que $f_p g_p = \varphi(m'_p)$ i f_p és el menor nombre enter positiu tal que m'_p divideix $p^{f_p} - 1$.

L'expressió en forma de producte d'Euler de la funció zeta de Dedekind de K en el semiplà $\Re(s) > 1$ es pot escriure, llavors, en la forma

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1} = \prod_p \prod_{\mathfrak{p}|p} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1} = \prod_p (1 - p^{-f_p s})^{-g_p}$$
$$= \prod_p \prod_{\chi \in G(m'_p)\widehat{\ }} (1 - \chi(p)p^{-s})^{-1} = \prod_{p|m} \prod_{\chi \in G(m'_p)\widehat{\ }} (1 - \chi(p)p^{-s})^{-1} \prod_{p \nmid m} \prod_{\chi \in G(m)\widehat{\ }} (1 - \chi(p)p^{-s})^{-1},$$

ja que $m'_p = m$ quan $p \nmid m$.

Ara, per a cada caràcter de Dirichlet $\chi \in G(m)\widehat{\ }$, posarem f_χ per a denotar el seu conductor i $\widetilde{\chi}$ per a denotar el caràcter χ definit mòdul f_χ; d'aquesta manera, χ s'obté com la composició de la projecció $G(m) \longrightarrow G(f_\chi)$ amb $\widetilde{\chi} : G(f_\chi) \longrightarrow \mathbb{C}^*$. Cal observar que, si p és un nombre primer que divideix m però no divideix f_χ, aleshores $\chi(p) = 0$

però $\widetilde{\chi}(p) = \chi(p) \neq 0$. Això fa que les expressions en forma de producte d'Euler de les funcions L associades a χ i a $\widetilde{\chi}$ es puguin escriure en la forma

$$L(\widetilde{\chi}, s) = \prod_{p\nmid f_\chi}(1-\widetilde{\chi}(p)p^{-s})^{-1}, \qquad L(\chi, s) = \prod_{p\nmid m}(1-\chi(p)p^{-s})^{-1},$$

de manera que podem escriure la igualtat

$$L(\chi, s) = L(\widetilde{\chi}, s) \prod_{p|m,\, p\nmid f_\chi} (1-\widetilde{\chi}(p)p^{-s}).$$

Apliquem aquest fet a l'expressió de la funció zeta de Dedekind de K que hem obtingut més amunt; obtenim la nova expressió

$$\begin{aligned}\zeta_K(s) &= \prod_{p|m} \prod_{\chi\in G(m'_p)\widehat{\ }} (1-\chi(p)p^{-s})^{-1} \prod_{\chi\in G(m)\widehat{\ }} \prod_{p\nmid m}(1-\chi(p)p^{-s})^{-1} \\ &= \prod_{p|m} \prod_{\chi\in G(m'_p)\widehat{\ }} (1-\chi(p)p^{-s})^{-1} \prod_{\chi\in G(m)\widehat{\ }} L(\widetilde{\chi}, s) \prod_{p|m,\, p\nmid f_\chi} (1-\widetilde{\chi}(p)p^{-s}).\end{aligned}$$

Es tracta de veure, doncs, que

$$\prod_{p|m} \prod_{\chi\in G(m'_p)\widehat{\ }} (1-\chi(p)p^{-s})^{-1}, \qquad \prod_{\chi\in G(m)\widehat{\ }} \prod_{p|m,\, p\nmid f_\chi} (1-\widetilde{\chi}(p)p^{-s})$$

són inversos l'un de l'altre. Ara bé, podem escriure aquest segon producte en la forma equivalent

$$\prod_{\chi\in G(m)\widehat{\ }} \prod_{p|m,\, p\nmid f_\chi} (1-\widetilde{\chi}(p)p^{-s}) = \prod_{p|m} \prod_{\chi\in G(m)\widehat{\ },\, p\nmid f_\chi} (1-\widetilde{\chi}(p)p^{-s}),$$

mentre que el primer es pot escriure com

$$\prod_{p|m} \prod_{\chi\in G(m'_p)\widehat{\ }} (1-\chi(p)p^{-s})^{-1} = \prod_{p|m} \prod_{\chi\in G(m'_p)\widehat{\ }} (1-\widetilde{\chi}(p)p^{-s})^{-1},$$

ja que p no divideix el conductor dels caràcters $\chi \in G(m'_p)\widehat{\ }$. Per tant, només cal veure que, per a tot nombre primer p que divideix m se satisfà la igualtat

$$\prod_{\chi\in G(m'_p)\widehat{\ }} (1-\widetilde{\chi}(p)p^{-s})^{-1} \prod_{\chi\in G(m)\widehat{\ },\, p\nmid f_\chi} (1-\widetilde{\chi}(p)p^{-s}) = 1.$$

Però qualsevol caràcter de $G(m)$ de conductor no divisible per p, per a un primer p que divideix m, s'obté de manera única a partir d'un caràcter de $G(m'_p)$ per composició amb la projecció $G(m) \longrightarrow G(m'_p)$; per tant, els caràcters sobre els quals es multiplica són els mateixos, de manera que obtenim la igualtat enunciada:

$$\zeta_K(s) = \prod_{\chi\in G(m)\widehat{\ }} L(\widetilde{\chi}, s) = \prod_{d|m} \prod_{\chi\in G(d)\widehat{\ },\, f_\chi = d} L(\chi, s).$$

Això ens permet acabar la prova de manera senzilla. L'extensió meromorfa a tot el pla complex es pot fer tenint en compte que el segon terme de la igualtat anterior és, de fet, un producte finit de funcions meromorfes de tot el pla; per tant, podem utilitzar

aquesta expressió per a definir la funció $\zeta_K(s)$ en els punts s tals que $\Re(s) \leq 1$; com que les funcions $L(\chi, s)$ són meromorfes en tot $\mathbb{C}$, també $\zeta_K(s)$ és una funció meromorfa de tot $\mathbb{C}$; però, a més a més, cada una de les funcions $L(\chi, s)$ que correspon a un caràcter $\chi \neq \chi_1$ és una funció entera que no s'anul·la en $s = 1$; i en canvi, la funció que correspon a $\chi = \chi_1$ és la funció zeta de Riemann. Per tant, $\zeta_K(s)$ té, efectivament, un únic pol en $s = 1$, i simple. □

Aquest resultat ens permet obtenir una fórmula analítica per al nombre de classes del cos ciclotòmic $K := \mathbb{Q}(\mu_m)$.

Corol·lari 15.6.2. *Sigui K el cos ciclotòmic de les arrels m-èsimes de la unitat, per a $m \geq 4$ un enter parell. Siguin R, h, Δ_K, el regulador, el nombre de classes d'ideals i el discriminant absolut del cos K, respectivament. Aleshores, se satisfà la igualtat*

$$h = \frac{m\sqrt{|\Delta_K|}}{R(2\pi)^{\varphi(m)/2}} \prod_{d|m,\, d\neq 1} \prod_{\chi \in G(m)\widehat{},\ f_\chi = d} L(\chi, 1).$$

Demostració: La fórmula del residu de la funció zeta d'un cos de nombres aplicada a aquest cas, dóna la igualtat $\lim_{s\to 1^+}(s-1)\zeta_K(s) = \dfrac{(2\pi)^{\varphi(m)/2}Rh}{m\sqrt{|\Delta_K|}}$, ja que K no té cap immersió real, té $\varphi(m)/2$ parelles d'immersions complexes conjugades no reals, i, com que m és parell, en K hi ha exactament m arrels diferents de la unitat. D'altra banda, la fórmula obtinguda en el teorema anterior ens permet escriure que el residu de la funció $\zeta_K(s)$ en el punt $s = 1$ es pot calcular com el producte del residu de la funció zeta de Riemann en $s = 1$, que és 1, pel valor del producte $\displaystyle\prod_{d|m,\, d\neq 1} \prod_{\chi \in G(m)\widehat{},\, f_\chi = d} L(\chi, s)$ en $s = 1$, ja que aquesta funció és analítica. Per a obtenir la igualtat que cerquem només cal aïllar el nombre de classes en la igualtat que es dedueix trivialment d'aquests càlculs. □

15.7 Avaluació de les funcions L de Dirichlet en $s = 1$

A les dues seccions anteriors hem obtingut fórmules analítiques per a calcular el nombre de classes dels cossos quadràtics o ciclotòmics. En tots dos casos cal avaluar un nombre finit de funcions L associades a caràcters de Dirichlet en el punt $s = 1$. L'objectiu d'aquesta secció és fer aquesta avaluació. Concretament, es tracta de provar el resultat següent.

Teorema 15.7.1. *Siguin χ un caràcter primitiu i no trivial de Dirichlet i f el seu conductor. Aleshores, $L(1, \chi) = \begin{cases} \dfrac{\pi i g(\chi)}{f} B_{1,\overline{\chi}}, & \text{si } \chi \text{ és senar,} \\ -\dfrac{g(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log \operatorname{sin} \dfrac{\pi a}{f}, & \text{si } \chi \text{ és parell,} \end{cases}$ on $\overline{\chi}$ denota el caràcter conjugat de χ i $g(\chi) := \displaystyle\sum_{x=1}^{f} \chi(x) e^{\frac{2\pi i x}{f}}$ la suma de Gauss normalitzada.*

Demostració: Comencem per observar que, pensat com a funció aritmètica, el caràcter χ és una funció periòdica de període f que s'anul·la en els enters que tenen factors comuns no trivials amb f. Per tant, de la definició de la funció L de Dirichlet associada al caràcter

χ, i per a $\Re(s) > 1$, on disposem de convergència absoluta, podem escriure la igualtat

$$L(s,\chi) = \sum_{n\geq 1} \chi(n) n^{-s} = \sum_{x=1}^{f} \chi(x) \sum_{n\equiv x \pmod f} n^{-s}.$$

Prenem, ara, $\zeta := e^{\frac{2\pi i}{f}}$ i no una altra arrel primitiva f-èsima de la unitat en $\mathbb{C}$; aleshores, $\frac{1}{f}\sum_{k=0}^{f-1} \zeta^{xk} = \begin{cases} 1, & \text{si } x \equiv 0 \pmod f, \\ 0, & \text{si } x \not\equiv 0 \pmod f, \end{cases}$ de manera que podem escriure que

$$\begin{aligned} L(s,\chi) &= \sum_{\mathrm{mcd}(x,f)=1} \chi(x) \sum_{n\geq 1} \frac{1}{f} \sum_{k=0}^{f-1} \zeta^{(x-n)k} n^{-s} = \frac{1}{f} \sum_{k=0}^{f-1} \left(\sum_{\mathrm{mcd}(x,f)=1} \chi(x) \zeta^{xk} \right) \sum_{n\geq 1} \zeta^{-nk} n^{-s} \\ &= \frac{1}{f} \sum_{k=0}^{f-1} g(\chi,k) \sum_{n\geq 1} \zeta^{-nk} n^{-s}, \end{aligned}$$

on $g(\chi,k)$ és la k-èsima suma de Gauss associada al caràcter χ (cf. Cap. 1). Com que $g(\chi,0) = 0$, obtenim la igualtat $L(s,\chi) = \frac{1}{f} \sum_{k=1}^{f-1} g(\chi,k) \sum_{n\geq 1} \zeta^{-nk} n^{-s}$.

Ara, per a $1 \leq k \leq f-1$ i en virtut del criteri de Dirichlet per a la convergència de sèries, la sèrie de Dirichlet $\sum_{n\geq 1} \zeta^{-nk} n^{-s}$ és convergent en $\Re(s) > 0$, ja que $\zeta^{-k} \neq 1$; per tant, l'abscissa de convergència de la sèrie és menor o igual que 0 i la funció que defineix és analítica en el semiplà $\Re(s) > 0$. El principi de prolongació analítica ens permet calcular, doncs, el valor de la funció $L(s,\chi)$ en $s = 1$ com la suma d'aquesta sèrie. Obtenim, doncs, que $L(1,\chi) = \frac{1}{f} \sum_{k=1}^{f-1} g(\chi,k) \sum_{n\geq 1} \frac{\zeta^{-kn}}{n}$.

Considerem la sèrie de potències de $z - \log(1-z) = \sum_{n\geq 1} \frac{z^n}{n}$, que té radi de convergència igual a 1. Els valors ζ^{-k}, per a $1 \leq k \leq f-1$, són tots ells de mòdul 1, però la sèrie $-\log(1-\zeta^{-k})$ és convergent i la funció $-\log(1-z)$, que defineix la branca del logaritme que és real quan l'argument $1-z$ és real positiu, és analítica en un entorn de $1-\zeta^{-k}$; per tant, se satisfà la igualtat $\sum_{n\geq 1} \frac{\zeta^{-kn}}{n} = -\log(1-\zeta^{-k})$, de manera que obtenim el valor de la funció $L(s,\chi)$ en $s = 1$ com la suma de la sèrie $L(1,\chi) = -\frac{1}{f} \sum_{k=1}^{f-1} g(\chi,k) \log(1-\zeta^{-k})$. Si tenim en compte els valors de les sumes de Gauss calculats a la proposició **1.6.2**,

$$g(\chi,k) = \begin{cases} 0, & \text{si } \mathrm{mcd}(k,f) > 1, \\ \overline{\chi}(k) g(\chi), & \text{si } \mathrm{mcd}(k,f) = 1, \end{cases}$$

quan el conductor de χ és f, obtenim la nova expressió

$$L(1,\chi) = -\frac{1}{f} g(\chi) \sum_{\mathrm{mcd}(k,f)=1} \overline{\chi}(k) \log(1-\zeta^{-k}).$$

Posem $S(\chi) := \sum_{\mathrm{mcd}(k,f)=1} \overline{\chi}(k)\log(1-\zeta^{-k})$. Cal avaluar $S(\chi)$ i, per a això, distingirem casos segons la paritat del caràcter χ.

Cas χ parell. El caràcter conjugat de χ també és parell; és a dir, $\overline{\chi}(-k) = \overline{\chi}(k)$, de manera que $2S(\chi) = \sum_{\mathrm{mcd}(k,f)=1} \overline{\chi}(k)\left(\log(1-\zeta^{-k}) + \log(1-\zeta^{k})\right)$. Ara bé, se satisfà la igualtat $\log(1-\zeta^{-k}) + \log(1-\zeta^{k}) = 2\log|1-\zeta^{k}|$, ja que l'argument dels nombres complexos $1-\zeta^{-k}$ i $1-\zeta^{k}$ és igual llevat del signe. D'altra banda,

$$|1-\zeta^{k}|^2 = \left|1-\cos\left(\frac{2\pi k}{f}\right) - i\sin\left(\frac{2\pi k}{f}\right)\right|^2 = 2-2\cos\left(\frac{2\pi k}{f}\right) = 4\sin^2\left(\frac{\pi k}{f}\right),$$

de manera que obtenim la igualtat

$$\begin{aligned} L(1,\chi) &= -\frac{g(\chi)}{f}\sum_{\mathrm{mcd}(k,f)=1}\overline{\chi}(k)\log\left(2\sin\left(\frac{\pi k}{f}\right)\right) \\ &= -\frac{g(\chi)}{f}\sum_{k=1}^{f}\overline{\chi}(k)\log\left(2\sin\left(\frac{\pi k}{f}\right)\right) = -\frac{g(\chi)}{f}\sum_{k=1}^{f}\overline{\chi}(k)\log\sin\left(\frac{\pi k}{f}\right), \end{aligned}$$

ja que $\sum_{k=1}^{f}\overline{\chi}(k)\log(2) = 0$ perquè $\chi \neq \chi_1$. Això demostra la fórmula en el cas que el caràcter és parell.

Cas χ senar. Podem aprofitar una part dels càlculs anteriors. Com que $\overline{\chi}(-k) = -\overline{\chi}(k)$, obtenim que

$$\begin{aligned} 2S(\chi) &= \sum_{\mathrm{mcd}(k,f)=1}\overline{\chi}(k)\left(\log(1-\zeta^{-k}) - \log(1-\zeta^{k})\right) = 2\sum_{\mathrm{mcd}(k,f)=1}\overline{\chi}(k)\pi i\left(\frac{1}{2}-\frac{k}{f}\right) \\ &= -2\pi i\sum_{\mathrm{mcd}(k,f)=1}\overline{\chi}(k)\frac{k}{f} = -\frac{2\pi i}{f}\sum_{\mathrm{mcd}(k,f)=1}k\overline{\chi}(k) = -2\pi i B_{1,\overline{\chi}}, \end{aligned}$$

ja que l'argument del nombre complex $1-\zeta^{-k}$ és $\pi\left(\frac{1}{2}-\frac{k}{f}\right)$, i el caràcter χ és no trivial. En conseqüència, podem escriure la fórmula $L(1,\chi) = \frac{\pi i}{f}g(\chi)B_{1,\overline{\chi}}$ que es tractava de demostrar. □

15.8 Nombre de classes dels cossos quadràtics

En aquesta secció es tracta de donar una fórmula més senzilla per al càlcul del nombre de classes dels cossos quadràtics. Cal començar, però, per recordar alguns fets sobre caràcters de Dirichlet quadràtics i sumes de Gauss.

Per a un caràcter quadràtic de Dirichlet de conductor f, χ, hem definit la suma de Gauss normalitzada associada a χ com $g(\chi) := \sum_{k=1}^{f}\chi(k)e^{\frac{2\pi i k}{f}} \in \mathbb{Q}(e^{\frac{2\pi i}{f}})$, i hem demostrat (cf. la proposició **1.6.3**) que $|g(\chi)|^2 = f$. D'altra banda, hem vist que tot caràcter

quadràtic de Dirichlet χ és el producte de caràcters de Legendre $\left(\frac{*}{p}\right)$, p nombre primer senar, potser multiplicats per algun dels caràcters primitius de conductor 4 o 8; recordem, també, que aquests caràcters són els $(-1)^{\varepsilon(*)}$, $(-1)^{\omega(*)}$, i $(-1)^{\omega(*)+\varepsilon(*)}$, on $2\varepsilon(x) := x-1$ i $8\omega(x) := x^2-1$, per a $x \in \mathbb{Z}$, senar. En particular, tot caràcter de Kronecker primitiu és producte de caràcters dels anteriors.

Lema 15.8.1. *Sigui χ_D un caràcter de Kronecker. Si $D > 0$, aleshores χ_D és parell i, si $D < 0$, aleshores χ_D és senar.*

Demostració: Cal recordar la definició del caràcter de Kronecker χ_D. Si D' és la part senar i positiva de D, aleshores $\chi_{D'}(*) = (-1)^{\varepsilon(D')\varepsilon(*)}\left(\frac{*}{D'}\right)$, de manera que $\chi_{D'}(-1) = 1$, ja que $\left(\frac{-1}{D'}\right) = (-1)^{\varepsilon(D')}$ i $\varepsilon(-1) = 1$. Si $D = 2D'$, aleshores $\chi_{2D'}(*) = (-1)^{\omega(*)}\chi_{D'}(*)$, de manera que $\chi_{2D'}(-1) = \chi_{D'}(-1) = 1$. En particular, si $D > 0$, aleshores χ_D és parell. D'altra banda, i per definició, $\chi_{-D'}(*) = (-1)^{\varepsilon(*)}\chi_{D'}$, i $\chi_{-2D'}(*) = (-1)^{\varepsilon(*)}\chi_{2D'}$, de manera que si $D < 0$, aleshores χ_D és senar, perquè $(-1)^{\varepsilon(-1)} = -1$. Això acaba la prova. □

Per a fer el càlcul explícit de la suma de Gauss normalitzada corresponent a un caràcter quadràtic primitiu és útil el resultat següent.

Proposició 15.8.2. *Siguin χ_1, χ_2, caràcters quadràtics primitius de conductors f_1, f_2, respectivament. Sigui $\chi := \chi_1\chi_2$, el producte dels dos caràcters definit mòdul el seu conductor. Suposem que f_1 i f_2 són primers entre si. Aleshores, el conductor de χ és $f := f_1f_2$ i la relació entre les sumes de Gauss associades a χ_1, χ_2 i χ és*

$$g(\chi) = g(\chi_1)g(\chi_2)\chi_1(f_2)\chi_2(f_1).$$

Demostració: La qüestió relativa al conductor ja ha estat esmentada en **1.4.9**. D'altra banda, com que $\mathrm{mcd}(f_1, f_2) = 1$, f_1 és un element invertible de $\mathbb{Z}/f_2\mathbb{Z}$, de manera que existeixen enters f_1', f_2' tals que $f_1f_1' + f_2'f_2 = 1$; a més a més, f_2' és invertible en $\mathbb{Z}/f_1\mathbb{Z}$. D'altra banda, donat un enter x tal que $0 \le x \le f_1f_2 - 1$, podem fer la divisió entera de x per f_1 en la forma $x = a + bf_1$, per a $0 \le a \le f_1 - 1$, $0 \le b \le f_2 - 1$, unívocament determinats. Amb aquestes notacions, podem escriure les igualtats següents:

$$g(\chi) = \sum_{x=0}^{f_1f_2-1} \chi(x)e^{\frac{2\pi ix}{f_1f_2}} = \sum_{x=0}^{f_1f_2-1} \chi_1(x)\chi_2(x)e^{\frac{2\pi ix}{f_1f_2}} = \sum_{a=0}^{f_1-1}\sum_{b=0}^{f_2-1} \chi_1(a)\chi_2(a+bf_1)e^{\frac{2\pi ia}{f_1f_2}}e^{\frac{2\pi ib}{f_2}}.$$

Com que els caràcters són quadràtics, de la igualtat $\chi_2(f_1f_1') = \chi_2(1) = 1$ es dedueix que $\chi_2(f_1') = \chi_2(f_1)$; a més a més, f_1 és invertible mòdul f_2, de manera que se satisfà que $\chi_2(a+bf_1) = \chi_2(f_1)\chi_2(af_1' + bf_1f_1') = \chi_2(f_1)\chi_2(af_1' + b)$ i quan b recorre un sistema de representants de $\mathbb{Z}/f_2\mathbb{Z}$, també ho fa $a + bf_1$; per tant, obtenim la nova expressió

$$\begin{aligned} g(\chi) &= \chi_2(f_1)\sum_{a=0}^{f_1-1} \chi_1(a)e^{\frac{2\pi ia}{f_1f_2}}e^{\frac{-2\pi iaf_1'}{f_2}}\sum_{b=0}^{f_2-1} \chi_2(af_1'+b)e^{\frac{2\pi i(af_1'+b)}{f_2}} \\ &= g(\chi_2)\chi_2(f_1)\sum_{a=0}^{f_1-1} \chi_1(a)e^{\frac{2\pi ia}{f_2}(\frac{1}{f_1}-f_1')}. \end{aligned}$$

Ara, la igualtat $\dfrac{2\pi ia}{f_2}\left(\dfrac{1}{f_1}-f_1'\right)=\dfrac{2\pi iaf_2'}{f_1}$ i el fet que quan a recorre un sistema de representants de $\mathbb{Z}/f_1\mathbb{Z}$ també ho fa af_2', ja que f_2' és invertible en $\mathbb{Z}/f_1\mathbb{Z}$, ens permet escriure la igualtat

$$\begin{aligned}g(\chi)&=g(\chi_2)\chi_2(f_1)\sum_{a=0}^{f_1-1}\chi_1(a)e^{\frac{2\pi iaf_2'}{f_1}}=g(\chi_2)\chi_2(f_1)\chi_1(f_2)\sum_{a=0}^{f_1-1}\chi_1(af_2')e^{\frac{2\pi iaf_2'}{f_1}}\\&=g(\chi_1)g(\chi_2)\chi_2(f_1)\chi_1(f_2),\end{aligned}$$

que volíem demostrar. □

Abans d'obtenir el signe de les sumes de Gauss normalitzades, encara convé estudiar les dels caràcters que constitueixen els caràcters quadràtics primitius. El cas de les sumes de Gauss que corresponen als caràcters de Legendre es descriu a la secció següent (cf. més avall, **15.9.1**). Concretament, s'hi demostra que si χ és el caràcter de Legendre que correspon al nombre primer senar p, aleshores

$$g(\chi)=\begin{cases}\sqrt{p}, & \text{si } p\equiv 1 \pmod 4,\\ i\sqrt{p}, & \text{si } p\equiv -1 \pmod 4.\end{cases}$$

Calculem les sumes de Gauss associades als caràcters quadràtics de conductors 4 i 8.

Lema 15.8.3. *Per als caràcters quadràtics de conductors* 4 *o* 8, χ_ε, χ_ω, *i* $\chi_{\varepsilon+\omega}=\chi_\varepsilon\chi_\omega$, *es té que* $g(\chi_\varepsilon)=2i$, $g(\chi_\omega)=2\sqrt{2}$, *i* $g(\chi_{\varepsilon+\omega})=2\sqrt{2}i$.

Demostració: La prova és un exercici senzill; només cal calcular-les:

$$\begin{aligned}g(\chi_\varepsilon)&=\chi_\varepsilon(1)i+\chi_\varepsilon(-1)(-i)=2i;\\ g(\chi_\omega)&=\chi_\omega(1)\zeta_8+\chi_\omega(3)\zeta_8^3+\chi_\omega(5)\zeta_8^5+\chi_\omega(7)\zeta_8^7\\&=\zeta_8-\zeta_8^3-\zeta_8^5+\zeta_8^7=2(\zeta_8+\zeta_8^7)=4\cos\left(\frac{2\pi}{8}\right)=2\sqrt{2};\\ g(\chi_{\omega+\varepsilon})&=\chi_{\omega+\varepsilon}(1)\zeta_8+\chi_{\omega+\varepsilon}(3)\zeta_8^3+\chi_{\omega+\varepsilon}(5)\zeta_8^5+\chi_{\omega+\varepsilon}(7)\zeta_8^7\\&=\zeta_8+\zeta_8^3-\zeta_8^5-\zeta_8^7=2(\zeta_8-\zeta_8^7)=4i\sin\left(\frac{2\pi}{8}\right)=2\sqrt{2}i.\ \square\end{aligned}$$

Proposició 15.8.4. *Sigui* χ *un caràcter quadràtic de Dirichlet primitiu i sigui* f *el seu conductor. Aleshores, la suma de Gauss normalitzada associada al caràcter* χ *admet l'expressió* $g(\chi)=\begin{cases}\sqrt{f}, & \text{si } \chi \text{ és parell,}\\ i\sqrt{f}, & \text{si } \chi \text{ és senar.}\end{cases}$

Demostració: Ja hem fet notar més amunt que tot caràcter quadràtic primitiu és un producte de caràcters de Legendre per, potser, algun dels caràcters primitius de conductor 4 o 8. D'aquesta manera, el problema es redueix al càlcul del signe de la suma de Gauss normalitzada que correspon a un producte de caràcters primitius de conductors primers entre si.

Suposem, doncs, que χ és el caràcter primitiu definit pel producte $\chi=\psi_0\psi_1\cdots\psi_r$, on ψ_0 és el caràcter trivial o bé un dels caràcters primitius de conductor 4 o 8, i ψ_k, per a $1\leq k\leq r$, és el caràcter de Legendre que correspon al nombre primer p_k, on $p_1,\ldots,p_k$

són nombres primers senars diferents. Comencem per considerar el cas en què ψ_0 és el caràcter trivial; en aquest cas, el conductor del caràcter χ és $f = p_1 \cdots p_r$. L'aplicació de la proposició de més amunt ens permet escriure la suma de Gauss $g(\chi)$ en la forma

$$g(\chi) = \psi_1\left(\prod_{k=2}^{r} p_k\right)\prod_{k=2}^{r}\psi_k(p_1)g(\psi_1)g(\psi_2\cdots\psi_r),$$

ja que el conductor del caràcter de Legendre associat al nombre primer p_k és exactament p_k; per inducció, obtenim la igualtat

$$\begin{aligned} g(\chi) &= \prod_{k=1}^{r} g(\psi_k)\prod_{k=1}^{r-1}\left(\left(\frac{\prod_{j=k+1}^{r} p_j}{p_k}\right)\prod_{j=k+1}^{r}\left(\frac{p_k}{p_j}\right)\right) \\ &= \prod_{k=1}^{r} g(\psi_k)\prod_{k=1}^{r-1}\prod_{j=k+1}^{r}\left(\left(\frac{p_j}{p_k}\right)\left(\frac{p_k}{p_j}\right)\right) = \prod_{k=1}^{r} g(\psi_k)\prod_{k=1}^{r-1}\prod_{j=k+1}^{r}(-1)^{\varepsilon(p_k)\varepsilon(p_j)}, \end{aligned}$$

en virtut de la llei de reciprocitat quadràtica. Si tenim en compte les sumes de Gauss associades als caràcters de Legendre, obtenim la nova igualtat

$$g(\chi) = i^s\sqrt{p_1}\cdots\sqrt{p_r}\prod_{1\le k<j\le r}(-1)^{\varepsilon(p_k)\varepsilon(p_j)} = i^s\sqrt{f}\prod_{1\le k<j\le r}(-1)^{\varepsilon(p_k)\varepsilon(p_j)},$$

on s és el nombre d'índexs $1 \le k \le r$ tals que $p_k \equiv -1 \pmod 4$. Ara, si $p_k \equiv 1 \pmod 4$ o si $p_j \equiv 1 \pmod 4$, aleshores $(-1)^{\varepsilon(p_k)\varepsilon(p_j)} = 1$, de manera que el signe que apareix en fer el producte és -1 elevat al nombre de parelles (k, j) d'índexs tals que $1 \le k < j \le r$ i $p_k \equiv p_j \equiv -1 \pmod 4$; aquest nombre és exactament $\binom{s}{2} = \dfrac{s(s-1)}{2}$, de manera que podem escriure que $g(\chi) = (-1)^{\frac{s(s-1)}{2}} i^s\sqrt{f} = i^{s(s-1)}i^s\sqrt{f} = i^{s^2}\sqrt{f}$. Ara bé, com que $s^2 \equiv 0, 1 \pmod 4$, obtenim que $i^{s^2} = \begin{cases} 1, & \text{si } s \text{ és parell,} \\ i, & \text{si } s \text{ és senar,} \end{cases}$ mentre que el caràcter χ també és parell o senar segons la paritat de s; això acaba la prova en el cas que el conductor de χ sigui senar.

Suposem, ara, que $\psi_0 = \chi_\varepsilon$ i escrivim $\psi := \psi_1\cdots\psi_r$. A l'expressió anterior de la suma de Gauss de ψ cal afegir els factors que corresponen al caràcter χ_ε; és a dir, disposem de la nova expressió $g(\chi) = g(\chi_\varepsilon)g(\psi)\chi_\varepsilon(p_1\cdots p_k)$, ja que $\psi(4) = 1$. Ara bé, tenim les igualtats

$$g(\psi) = \begin{cases} \sqrt{p_1\cdots p_r}, & \text{si } \psi \text{ és parell,} \\ i\sqrt{p_1\cdots p_r}, & \text{si } \psi \text{ és senar,} \end{cases} \qquad g(\chi_\varepsilon) = 2i, \qquad \chi_\varepsilon(p_1\cdots p_k) = (-1)^{\varepsilon(p_1\cdots p_r)},$$

mentre que ψ té la mateixa paritat que $\varepsilon(p_1\cdots p_r)$. Com que χ i ψ tenen paritat diferent, ja que χ_ε és senar, la prova s'acaba immediatament per multiplicació.

Els casos $\psi_0 = \chi_\omega$ i $\psi_0 = \chi_{\varepsilon+\omega}$ s'acaben de la mateixa manera que l'anterior. Els detalls finals es deixen com a exercici. □

Per a acabar el capítol, podem donar ja una fórmula per al càlcul del nombre de classes d'ideals de l'anell dels enters d'un cos quadràtic. Recordem que si K és un cos quadràtic i D el seu discriminant, aleshores $K = \mathbb{Q}(\sqrt{D})$.

Teorema 15.8.5. *Sigui $K := \mathbb{Q}(\sqrt{D})$ un cos quadràtic, on D és el discriminant. El nombre de classes d'ideals de K, $h := h_K$ és donat per les expressions*

$$h = \begin{cases} \dfrac{1}{D} \displaystyle\sum_{0<x<|D|,\, \mathrm{mcd}(x,D)=1} \chi_D(x)x, & \text{si } D < -4, \\ 1, \text{ si } D = -4,\, -3, & \\ \dfrac{-1}{\log(u)} \displaystyle\sum_{0<x<\frac{D}{2},\ \mathrm{mcd}(x,D)=1} \chi_D(x) \log \sin\left(\dfrac{\pi x}{D}\right), & \text{si } D > 0, \end{cases}$$

on u designa la unitat fonamental del cos quadràtic real K, és a dir, la menor de les unitats de l'anell dels enters de K tal que $u > 1$.

Demostració: Els casos $D = -4, -3$, corresponen a $\mathbb{Q}(i)$, $\mathbb{Q}(\rho)$, on ρ és una arrel cúbica primitiva de la unitat i són ben coneguts, ja que els anells d'enters són euclidians. En el cas $D < -4$, el nombre d'arrels de la unitat de K és $w = 2$, i el caràcter de Kronecker χ_D és senar; per tant, els teoremes **15.5.3** i **15.7.1** i el càlcul dels nombres generalitzats de Bernoulli associats a caràcters de Dirichlet (cf. el corol·lari **14.4.7**) ens permeten escriure la igualtat

$$h = \frac{w\sqrt{-D}}{2\pi} \frac{\pi i g(\chi_D)}{-D} B_{1,\chi_D} = \frac{2\sqrt{-D}}{2\pi} \frac{\pi i\, i\, \sqrt{-D}}{-D} \frac{1}{-D} \sum_{k=1}^{-D} \chi_D(k)k = \frac{1}{D} \sum_{k=1}^{-D} \chi_D(k)k$$

que volíem provar.

D'altra banda, en el cas $D > 0$ el caràcter de Kronecker χ_D és parell i els teoremes **15.5.3** i **15.7.1** ens permeten escriure que

$$\begin{aligned} h &= \frac{\sqrt{D}}{2\log(u)} \frac{-g(\chi_D}{D} \sum_{k=1}^{D} \overline{\chi}_D(k) \log \sin\left(\frac{\pi k}{D}\right) = \frac{\sqrt{D}}{2\log(u)} \frac{-\sqrt{D}}{D} \sum_{k=1}^{D} \chi_D(k) \log \sin\left(\frac{\pi k}{D}\right) \\ &= \frac{-1}{\log(u)} \sum_{k=1}^{D/2} \chi_D(k) \log \sin\left(\frac{\pi k}{D}\right), \end{aligned}$$

ja que, per ser χ_D parell, és $\chi_D(D-k) = \chi_D(-k) = \chi_D(k)$ i $\sin(\pi - \alpha) = \sin(\alpha)$, per a tot nombre real α, en particular, per a $\alpha = \dfrac{\pi k}{D}$. Això acaba la prova. □

15.9 El signe de les sumes de Gauss per als caràcters de Legendre

En aquesta secció es tracta de fer el càlcul del signe de la suma de Gauss normalitzada per als caràcters de Legendre. Concretament, es tracta de provar el resultat següent.

Teorema 15.9.1 (Signe de les sumes de Gauss per als caràcters de Legendre)**.** *Siguin p un nombre primer senar, $\zeta := e^{2\pi i/p} \in \mathbb{C}$, i $S(p) := \displaystyle\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\zeta^a$ la suma de Gauss normalitzada per al caràcter de Legendre. Llavors, si $\sqrt{p}$ indica l'arrel quadrada positiva de p, se satisfà que $S(p) = \begin{cases} \sqrt{p}, & \text{si } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{si } p \equiv -1 \pmod 4. \end{cases}$*

Donarem dues demostracions d'aquest resultat. Les dues es basen en el valor del quadrat de la suma de Gauss, $S(p)^2 = \left(\frac{-1}{p}\right)p$ (cf. la proposició **1.7.1**). La primera, és una demostració de Kronecker (cf. [I-R 82, cap. 6, secció 4]). Proposem com a exercici la demostració d'un resultat elemental sobre coeficients de sèries que utilitzarem més avall.

Exercici 15.9.2. Siguin $f(X) := \sum_{n\geq 0} a(n)\frac{X^n}{n!}$, $g(X) := \sum_{n\geq 0} b(n)\frac{X^n}{n!} \in \mathbb{Q}[[X]]$ sèries de potències tals que els coeficients $a(n)$, $b(n) \in \mathbb{Z}$. Llavors, per a la sèrie producte es té que $f(X)g(X) = \sum_{n\geq 0} c(n)\frac{X^n}{n!}$, on $c(n) = \sum_{m=0}^{n} \binom{n}{m} a(m)b(n-m) \in \mathbb{Z}$. A més a més, si suposem que p és un nombre natural primer tal que $p|a(n)$, per a $0 \leq n \leq p-1$, aleshores també $p|c(n)$, per a $0 \leq n \leq p-1$.

Per inducció, s'obté una expressió senzilla per als coeficients d'un producte.

Corol·lari 15.9.3. *Siguin $f_i(X) := \sum_{n\geq 0} a_i(n)\frac{X^n}{n!}$, $1 \leq i \leq m$, sèries de potències tals que els coeficients $a_i(n)$ pertanyin a qualsevol subanell $A \subseteq \mathbb{C}$. Per a la sèrie producte es té que $f_1(X)\cdots f_m(X) = \sum_{n\geq 0} c(n)\frac{X^n}{n!}$, i $c(n) = \sum_{n_1+\cdots+n_m=n} \binom{n}{n_1,\ldots,n_m} a_1(n_1)\cdots a_m(n_m) \in A$, i $\binom{n}{n_1,\ldots,n_m} = \frac{n!}{n_1!\cdots n_m!}$ són els nombres multinomials.* □

Demostració (del teorema **15.9.1**, Kronecker): Si $\Phi_p(X)$ és el p-èsim polinomi ciclotòmic, llavors $p = \Phi_p(1) = \prod_{r=1}^{p-1}(1-\zeta^r)$. D'altra banda, els nombres enters $\pm(4k-2)$, per a $1 \leq k \leq \frac{p-1}{2}$, formen un sistema reduït de residus mòdul p. Per tant, se satisfà que

$$\prod_{k=1}^{p-1}(1-\zeta^r) = \prod_{k=1}^{\frac{p-1}{2}}\left((1-\zeta^{4k-2})(1-\zeta^{-(4k-2)})\right) = \prod_{k=1}^{\frac{p-1}{2}}(\zeta^{-(2k-1)}-\zeta^{2k-1})\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}-\zeta^{-(2k-1)});$$

i, en tenir en compte que hi ha $\frac{p-1}{2}$ factors repetits llevat del signe, que

$$\prod_{k=1}^{p-1}(1-\zeta^r) = (-1)^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)^2.$$

O sigui, hem obtingut que $\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)^2 = (-1)^{\frac{p-1}{2}}p = S(p)^2$. Com a conseqüència, existeix $\varepsilon = \pm 1$ tal que $S(p) = \varepsilon\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right)$. I si ara demostrem que

$$\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta^{2k-1}-\zeta^{-(2k-1)}\right) = \begin{cases}\sqrt{p}, & \text{si } p\equiv 1 \pmod 4,\\ i\sqrt{p}, & \text{si } p\equiv -1 \pmod 4,\end{cases}$$ només caldrà veure que $\varepsilon = 1$.

Ara bé, se satisfà que $\zeta^{2k-1}-\zeta^{-(2k-1)}=2i\sin\left(\frac{2(2k-1)\pi}{p}\right)$; per tant, el producte val $i^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}2\sin\left(\frac{(4k-2)\pi}{p}\right)$, i serà suficient calcular-ne el signe. Com que $1\leq k\leq\frac{p-1}{2}$, resulta que $0<\frac{(4k-2)\pi}{p}<2\pi$, i que $\sin\left(\frac{(4k-2)\pi}{p}\right)\begin{cases}>0, & \text{si } \frac{4k-2}{p}<1,\\ <0, & \text{si } \frac{4k-2}{p}>1.\end{cases}$

Distingim casos. Si $p\equiv 1 \pmod 4$, resulta que hi ha exactament $\frac{p-1}{2}-\frac{p-1}{4}=\frac{p-1}{4}$ valors de k per als quals el sinus és negatiu, i també $i^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{4}}$, de manera que el producte és positiu. I si $p\equiv -1 \pmod 4$, hi ha exactament $\frac{p-1}{2}-\frac{p+1}{4}=\frac{p-3}{4}$ valors de k per als quals el sinus és negatiu, però $i^{\frac{p-1}{2}}=i(-1)^{\frac{p-3}{4}}$, de manera que el producte és exactament i vegades un nombre positiu, com calia veure.

Ara resta la tasca més complicada: demostrar que $\varepsilon=1$. Per a veure això, considerem el polinomi

$$f(X):=\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)X^r-\varepsilon\prod_{k=1}^{\frac{p-1}{2}}\left(X^{2k-1}-X^{p-(2k-1)}\right)\in\mathbb{Z}[X].$$

Com que $f(\zeta)=0$, el polinomi ciclotòmic $\Phi_p(X)$ divideix $f(X)$; i com que $f(1)=0$, també $X-1$ divideix $f(X)$. Per tant, X^p-1 divideix $f(X)$ i, en conseqüència, existeix un polinomi $h(X)\in\mathbb{Z}[X]$ tal que $f(X)=(X^p-1)h(X)$. Si canviem X per e^z, obtenim la igualtat, de sèries de potències de z,

$$f(e^z)=\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)e^{rz}-\varepsilon\prod_{k=1}^{\frac{p-1}{2}}\left(e^{(2k-1)z}-e^{(p-2k+1)z}\right)=(e^{pz}-1)h(e^z).$$

Tant $f(e^z)$ com $(e^{pz}-1)h(e^z)$ són sèries de la forma $\sum_{n\geq 0}a(n)\frac{z^n}{n!}$, amb $a(n)\in\mathbb{Z}$. El càlcul del coeficient de $\frac{z^{\frac{p-1}{2}}}{(\frac{p-1}{2})!}$; o sigui, de $a\left(\frac{p-1}{2}\right)$, ens proporcionarà el valor $\varepsilon=1$ que volem.

Clarament, per a la suma $\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)e^{rz}$, el coeficient és $\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)r^{\frac{p-1}{2}}$. I, per aplicació del corol·lari **15.9.3**, el coeficient que correspon al producte $\varepsilon\prod_{k=1}^{\frac{p-1}{2}}\left(e^{(2k-1)z}-e^{(p-2k+1)z}\right)$ és $\left(\frac{p-1}{2}\right)!\prod_{k=1}^{\frac{p-1}{2}}(4k-p-2)$.

En efecte, notem que multipliquem les $\frac{p-1}{2}$ sèries, per a $1\leq k\leq\frac{p-1}{2}$,

$$e^{(2k-1)z}-e^{(p-2k+1)z}=\sum_{n\geq 0}\left((2k-1)^n-(p-(2k-1))^n\right)\frac{z^n}{n!}.$$

Per tant, el coeficient que correspon a $n = \dfrac{p-1}{2}$ és

$$\sum_{m_1+\cdots+m_{\frac{p-1}{2}}=\frac{p-1}{2}} \binom{\frac{p-1}{2}}{m_1,\ldots,m_{\frac{p-1}{2}}} \prod_{j=1}^{\frac{p-1}{2}} \left((2k-1)^{m_j} - (p-(2k-1))^{m_j}\right).$$

Fixem-nos que si algun dels índexs és $m_j = 0$, aleshores el corresponent factor del producte és $1-1=0$ i el sumand s'anul·la. Per tant, només resta el sumand que correspon a $m_1 = \cdots = m_{\frac{p-1}{2}} = 1$, el valor del qual és $\left(\dfrac{p-1}{2}\right)! \displaystyle\prod_{j=1}^{\frac{p-1}{2}} (4k-2-p)$, com calia veure.

Així, doncs, $a\left(\dfrac{p-1}{2}\right) = \displaystyle\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r^{\frac{p-1}{2}} - \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} (4k-p-2)$.

Si calculem aquest coeficient de nou, però a partir de l'expressió $(e^{pz}-1)h(e^z)$, obtenim, a partir del corol·lari **15.9.3**, que p divideix $a\left(\dfrac{p-1}{2}\right)$, perquè, de fet, p divideix tots els coeficients de $e^{pz}-1$ (que són p^n, per a $n \geq 1$). Això ens diu que $a\left(\dfrac{p-1}{2}\right) \equiv 0 \pmod{p}$; o sigui, obtenim la congruència $\displaystyle\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r^{\frac{p-1}{2}} \equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} (4k-p-2) \pmod{p}$.

Apliquem el criteri d'Euler per al càlcul del símbol de Legendre; podem escriure que $\left(\dfrac{r}{p}\right) \equiv r^{\frac{p-1}{2}} \pmod{p}$, de manera que $\displaystyle\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r^{\frac{p-1}{2}} \equiv \sum_{r=1}^{p-1} 1 = p-1 \equiv -1 \pmod{p}$. I, d'altra banda, en virtut del teorema de Wilson,

$$\varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} (4k-p-2) \equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} 2(2k-1) = \varepsilon(p-1)! \equiv -\varepsilon \pmod{p}.$$

Finalment, el fet que sigui $\varepsilon = \pm 1$ i, alhora, $-1 \equiv -\varepsilon \pmod{p}$, amb p primer senar, permet dir que $\varepsilon = 1$, com restava provar. □

Observació 15.9.4. Notem que en aquesta demostració, essencialment de Kronecker, només es fa servir aritmètica sobre l'anell $\mathbb{Z}$ dels nombres enters. D'altra banda, les sèries de potències que hi intervenen són de coeficients enters, llevat dels denominadors $n!$, i només ho fan com a sèries formals, sense necessitat de convergència en cap punt, encara que les sèries siguin convergents en tot el pla complex, perquè són polinomis en la sèrie exponencial.

Observació 15.9.5. Una altra demostració, també de Kronecker (cf. [B-S 66, cap.5, exercicis 13 al 16]), fa ús dels mateixos principis. La variació principal respecte de l'anterior és que, en lloc de fer servir només aritmètica sobre l'anell dels nombres enters, utilitza aritmètica en l'anell dels enters, $\mathbb{Z}[\zeta]$, del p-èsim cos ciclotòmic, i reducció mòdul l'ideal primer que divideix p, en lloc de reducció mòdul p en $\mathbb{Z}$. En aquest cas, s'estalvia l'ús de les sèries exponencials, a canvi d'introduir els nombres algebraics de $\mathbb{Z}[\zeta]$.

La segona demostració que presentem del càlcul del signe de la suma de Gauss per al caràcter de Legendre és de Schur (cf. [B-S 66, cap.5, secció 4.3]).

DEMOSTRACIÓ (del teorema **15.9.1**, Schur): Aquesta prova parteix, de nou, de la igualtat $S(p)^2 = \left(\frac{-1}{p}\right)p$, de manera que $S(p) = \begin{cases} \pm\sqrt{p}, & \text{si } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p}, & \text{si } p \equiv -1 \pmod 4. \end{cases}$ Es tracta de veure que val el signe més en tots dos casos.

Notem que podem permutar els sumands i escriure la suma de Gauss en la forma $S(p) = \sum_r \zeta^r - \sum_s \zeta^s$, on r recorre els residus quadràtics no nuls mòdul p, i s recorre els no-residus quadràtics no nuls mòdul p. I, si tenim en compte que el polinomi ciclotòmic $\Phi_p(X)$ s'anul·la en ζ, és $\sum_r \zeta^r + \sum_s \zeta^s + 1 = 0$, de manera que obtenim la igualtat que $S(p) = 1 + 2\sum_r \zeta^r = \sum_{k=0}^{p-1} \zeta^{k^2}$, la darrera expressió perquè els quadrats no nuls ho són exactament de dos valors. Així, la suma de Gauss coincideix amb la traça de la matriu de Vandermonde

$$V := \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \dots & \zeta^{(p-1)^2} \end{bmatrix};$$

o sigui, amb la suma dels valors propis de la matriu, comptats cadascun amb la seva multiplicitat. Siguin $v_1, \dots, v_p$ aquests valors propis. Cal calcular, doncs, la suma $S(p) = v_1 + \cdots + v_p$.

Els valors propis de la matriu V^2 són $v_1^2, \dots, v_p^2$. A més a més, la matriu V^2 es pot calcular de manera senzilla; com que $\sum_{k=0}^{p-1} \zeta^{ik}\zeta^{kj} = \sum_{k=0}^{p-1} \zeta^{k(i+j)} = \begin{cases} p, & \text{si } i+j \equiv 0 \pmod p, \\ 0, & \text{si } i+j \not\equiv 0 \pmod p, \end{cases}$ resulta que

$$V^2 = \begin{bmatrix} p & 0 & \dots & 0 \\ 0 & 0 & \dots & p \\ \vdots & \vdots & \dots & \vdots \\ 0 & p & \dots & 0 \end{bmatrix}.$$

Ara bé, el polinomi característic de la matriu V^2 es calcula immediatament, i s'obté que és $(X-p)^{\frac{p+1}{2}}(X+p)^{\frac{p-1}{2}}$, de manera que hi ha $\dfrac{p+1}{2}$ arrels iguals a p i $\dfrac{p-1}{2}$ arrels iguals a $-p$. Notem que, en particular, el determinant de V^2 és $\det V^2 = (-1)^{\frac{p(p-1)}{2}} p^p$.

Siguin n^+, n^-, m^+ i m^-, respctivament, els nombres de valors propis $\sqrt{p}$, $-\sqrt{p}$, $i\sqrt{p}$, $-i\sqrt{p}$. Tenim, doncs, que $n^+ + n^- = \dfrac{p+1}{2}$, i que $m^+ + m^- = \dfrac{p-1}{2}$. I, a més a més, la suma de Gauss es pot reescriure en la forma $S(p) = \big((n^+ - n^-) + (m^+ - m^-)i\big)\sqrt{p}$. Per tant, en tenir en compte la primera expressió, obtenim que per a $p \equiv 1 \pmod 4$ ha de ser $m^+ = m^-$ i $n^+ - n^- = \pm 1$; i per a $p \equiv -1 \pmod 4$ ha de ser $n^+ = n^-$ i $m^+ - m^- = \pm 1$.

Obtindrem una segona relació que permeti determinar completament els valors n^+, n^-, m^+, m^-, a partir del càlcul del determinant de la matriu de Vandermonde, V. D'entrada, com que hem calculat el determinant de V^2, el determinant de V és una arrel quadrada de l'anterior; per tant, tenim que $\det V = \pm i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}$. Però cal determinar-ne el signe.

I podem treballar de manera semblant a la demostració de Kronecker. Tal com hem escrit la matriu V, l'expressió usual del determinant és $\det V = \prod_{0\le i<j\le p-1} (\zeta^j - \zeta^i)$.

Posem $\xi := e^{\frac{2\pi i}{2p}} = \cos\frac{2\pi}{2p} + i\sin\frac{2\pi}{2p}$ l'arrel primitiva $2p$-èsima de la unitat usual, per a la qual és $\zeta = \xi^2$. Aquest canvi permet reescriure l'expressió anterior en la forma

$$\begin{aligned}\det V &= \prod_{0\le i<j\le p-1} (\xi^{2j} - \xi^{2i}) = \prod_{0\le i<j\le p-1} \xi^{j+i}(\xi^{j-i} - \xi^{-(j-i)}) \\ &= \prod_{0\le i<j\le p-1} \xi^{j+i} \prod_{0\le i<j\le p-1} \left(2i\sin\frac{2(j-i)\pi}{2p}\right) = i^{\frac{p(p-1)}{2}} 2^{\frac{p(p-1)}{2}} \prod_{0\le i<j\le p-1} \sin\frac{2(j-i)\pi}{2p},\end{aligned}$$

ja que $\sum_{0\le i<j\le p-1} (j+i) = 2p\left(\frac{p-1}{2}\right)^2$ és un nombre enter múltiple de $2p$ i, per tant, $\prod_{0\le i<j\le p-1} \xi^{j+i} = \xi^{2p(\frac{p-1}{2})^2} = 1$. A més a més, com abans, per a tots els valors de la parella (i,j) que considerem, tenim que $\sin\frac{2(j-i)\pi}{2p} > 0$, perquè $0 < \frac{2(j-i)\pi}{2p} < \pi$. Així, obtenim que el determinant de V admet l'expressió $\det V = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}$, amb el signe positiu.

D'altra banda, el determinant de la matriu V és el producte dels seus valors propis; és a dir, $\prod_{k=1}^{p} v_k = \sqrt{p}^{n^+}(-\sqrt{p})^{n^-}(i\sqrt{p})^{m^+}(-i\sqrt{p})^{m^-} = i^{2n^- + m^+ - m^-} p^{\frac{p}{2}}$. Si ara comparem els dos valors del determinant, obtenim la relació $2n^- + m^+ - m^- \equiv \frac{p(p-1)}{2} \pmod 4$.

Finalment, per a $p \equiv 1 \pmod 4$, els fets que siguin $m^+ = m^-$ i $n^+ + n^- = \frac{p+1}{2}$, impliquen que $n^+ - n^- \equiv 1 \pmod 4$ i, per tant, que $n^+ - n^- = 1$ i $S(p) = \sqrt{p}$. I, anàlogament, per a $p \equiv -1 \pmod 4$, els fets que siguin $n^+ = n^-$ i $m^+ + m^- = \frac{p-1}{2}$, impliquen que també $m^+ - m^- \equiv 1 \pmod 4$ i, per tant, que $m^+ - m^- = 1$ i $S(p) = i\sqrt{p}$. □

Capítol 16

Aplicacions a la conjectura de Fermat

En el capítol **8** hem demostrat el primer cas de la conjectura de Fermat per a exponents regulars (cf. **8.5.3**). En aquest capítol, i com a aplicació d'alguns dels resultats que s'han demostrat en els anteriors, i d'alguns de nous que demostrarem en aquest mateix, es tracta de fer la prova del segon cas de la conjectura de Fermat per a exponents primers regulars. D'aquesta manera, la conjectura de Fermat restarà provada per a tot exponent $n > 2$ divisible per algun primer regular.

16.1 Factors del nombre de classes d'un cos ciclotòmic

Abans de provar el segon cas del teorema de Fermat per a exponents regulars, donarem algun criteri per a decidir quan un cert nombre primer senar p és un primer regular. I per a això, cal estudiar una certa descomposició del nombre de classes d'ideals de l'anell dels enters del cos ciclotòmic de les arrels p-èsimes de la unitat.

A partir d'aquest moment, i si no es diu res en contra, p denotarà un nombre primer senar, $\zeta := \zeta_p$ una arrel primitiva p-èsima de la unitat, $K := \mathbb{Q}(\zeta)$ el cos ciclotòmic de les arrels p-èsimes de la unitat, $A := \mathbb{Z}[\zeta]$ l'anell dels enters de K, i h_p el nombre de classes d'ideals de A. Com és habitual, escriurem $K^+ = \mathbb{Q}(\zeta)^+ := \mathbb{Q}(\zeta + \zeta^{-1})$, el subcòs real maximal de K, A^+ l'anell dels enters de K^+, i h_p^+ el nombre de classes d'ideals de A^+. El primer resultat que demostrarem, més general que per a arrels p-èsimes, és el següent.

Lema 16.1.1. *Siguin $n \geq 3$ un enter qualsevol i ζ_n una arrel primitiva n-èsima de la unitat. L'anell dels enters del cos $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ és l'anell $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

Demostració: Ja sabem que l'anell dels enters de $\mathbb{Q}(\zeta_n)$ és $\mathbb{Z}[\zeta_n]$ (cf. el teorema **3.9.9**); per tant, les potències $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}$ formen una $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_n]$. Aprofitarem aquest fet per a deduir el resultat que desitgem. Clarament, com que $\zeta_n + \zeta_n^{-1}$ és un enter algebraic de $\mathbb{Q}(\zeta_n)^+$, l'anell dels enters d'aquest cos conté $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$; es tracta de veure la inclusió contrària. Suposem que $\alpha \in \mathbb{Q}(\zeta_n)^+$ és un enter algebraic; aleshores, existeixen nombres $a_0, a_1, \ldots, a_k \in \mathbb{Q}$, $0 \leq k \leq \dfrac{\varphi(n)}{2} - 1$, tals que $\alpha = \displaystyle\sum_{j=0}^{k} a_j(\zeta_n + \zeta_n^{-1})^j$,

ja que $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \dfrac{\varphi(n)}{2}$. Restem els sumands tals que $a_j \in \mathbb{Z}$, que són elements de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$; volem veure que, per al nou α, és $a_j = 0$, per a tot índex j. Si no fos així, podríem suposar que $k \geq 0$ i que $a_k \neq 0$; si multipliquem la igualtat de més amunt per ζ_n^k, obtenim una igualtat de la forma $\zeta_n^k \alpha = \sum_{i=0}^{2k} b_i \zeta_n^i$, on els coeficients b_i són combinacions lineals, de coeficients enters, dels nombres a_j; i, en particular, $b_{2k} = a_k$. Ara bé, $\zeta_n^k \alpha$ és un enter algebraic i pertany al cos ciclotòmic $\mathbb{Q}(\zeta_n)$, de manera que és un element de $\mathbb{Z}[\zeta_n]$; com que $2k \leq \varphi(n) - 2 \leq \varphi(n) - 1$, i les potències $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}$ són una $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_n]$, tots els nombres b_j han de ser enters. En particular, $a_k \in \mathbb{Z}$, contràriament a la suposició que havíem fet. Això prova el resultat. □

Hem vist en el capítol anterior (cf. la proposició **15.5.1**) que la funció zeta de Dedekind associada al cos quadràtic de discriminant D es pot escriure, en el semiplà $\Re(s) > 1$, en la forma $\zeta_{\mathbb{Q}(\sqrt{D})}(s) = \zeta(s) L(\chi_D, s)$, on χ_D és el caràcter de Kronecker associat a D; si tenim en compte que $\zeta(s)$ és la funció L associada al caràcter trivial, la funció zeta de Dedekind és producte de funcions L associades a caràcters primitius. Un resultat semblant també ha estat provat per al cos de les arrels $2m$-èsimes de la unitat; la funció zeta és el producte de les funcions L associades a tots els caràcters de Dirichlet primitius de conductor divisor de $2m$ (cf. el teorema **15.6.1**). Aquest resultat no és anecdòtic, ni de bon tros; de fet, és vàlid per a totes les extensions abelianes de $\mathbb{Q}$. Encara que no ho provarem en general, sí que ho farem en el cas del cos K^+. Concretament, demostrarem el resultat següent.

Proposició 16.1.2. *Siguin p un nombre primer senar, $K := \mathbb{Q}(\mu_p)$ el cos de les arrels p-èsimes de la unitat, i $K^+ := \mathbb{Q}(\mu_p)^+$ el subcòs real maximal de K. Aleshores, en el semiplà $\Re(s) > 1$ se satisfà la igualtat* $\zeta_{K^+}(s) = \zeta(s) \prod_{\chi \in G(p)\widehat{},\ \chi \text{ parell i primitiu}} L(\chi, s)$.

Demostració: Comencem per observar que el caràcter de Teichmüller (ciclotòmic) de K és, per definició, l'isomorfisme de grups abelians $\omega : \mathrm{Gal}\,(K|\mathbb{Q}) \longrightarrow G(p) = {\mathbb{F}_p}^*$ que assigna a cada automorfisme $\sigma \in \mathrm{Gal}\,(K|\mathbb{Q})$ l'element $\omega(\sigma) \in G(p)$ tal que $\sigma(\zeta) = \zeta^{\omega(\sigma)}$, per a tota arrel primitiva p-èsima de la unitat, ζ. Considerem la successió exacta de grups de Galois

$$1 \longrightarrow \mathrm{Gal}\left(K|K^+\right) \longrightarrow \mathrm{Gal}\,(K|\mathbb{Q}) \longrightarrow \mathrm{Gal}\left(K^+|\mathbb{Q}\right) \longrightarrow 1.$$

La conjugació complexa, donada per $c(\zeta) := \zeta^{-1}$, és l'únic element d'ordre 2 de $\mathrm{Gal}\,(K|\mathbb{Q})$, ja que aquest grup és cíclic, i genera $\mathrm{Gal}\,(K|K^+)$. Per tant, si identifiquem $\mathrm{Gal}\,(K|\mathbb{Q})$ amb el grup $G(p)$ dels elements invertibles de $\mathbb{Z}/p\mathbb{Z}$, la conjugació complexa c s'identifica amb l'element $-1 \in G(p)$. Amb aquesta identificació, la successió exacta de grups de Galois es pot escriure en la forma

$$1 \longrightarrow \{\pm 1\} \longrightarrow G(p) \longrightarrow G(p)/\{\pm 1\} \longrightarrow 1.$$

En dualitzar, el grup de Galois $\mathrm{Gal}\,(K^+|\mathbb{Q})$ correspon al subgrup format pels caràcters $\chi \in \mathrm{Gal}\,(K|\mathbb{Q})$ tals que $\chi(c) = 1$; és a dir, el grup de caràcters $\chi \in G(p)\widehat{}$ tals que $\chi(-1) = 1$; o sigui, el grup dels caràcters parells de Dirichlet definits mòdul p. Observem que, via aquesta identificació entre els grups de Galois i els grups de caràcters, K^+ és el subcòs de K fix per la intersecció de tots els nuclis dels caràcters parells.

Calculem, ara, la funció zeta de Dirichlet del cos K^+. Anàlogament a com hem fet en el cas dels cossos quadràtics o ciclotòmics, utilitzarem la descomposició en producte d'Euler

de la funció zeta en el semiplà $\Re(s) > 1$. Podem escriure el factor d'Euler que correspon a un nombre primer $\ell \neq p$ en la forma $E_\ell(s, K^+) := \prod_{\mathfrak{l}|\ell}(1 - \mathrm{N}(\mathfrak{l})^{-s})^{-1} = (1 - \ell^{-sf_\ell})^{-g_\ell}$, on f_ℓ és el grau residual de cada un dels ideals primers $\mathfrak{l}$ de A^+ que divideixen ℓA, i g_ℓ el nombre d'aquests ideals primers.

Siguin G el subgrup del grup de caràcters parells de $G(p)$ format per tots els caràcters de Dirichlet (parells) $\chi : G(p) \longrightarrow \mathbb{C}^*$ tals que $\chi(\ell) \neq 0$, i H el subgrup de G format pels caràcters χ tals que $\chi(\ell) = 1$. Com que $\ell \neq p$, aleshores ℓ no ramifica en K^+ i se satisfà que el grup G coincideix amb tot el grup de caràcters parells; en efecte, si χ és un caràcter qualsevol de $G(p)$, aleshores $\chi(\ell) \neq 0$ ja que ℓ no divideix el conductor de χ, que només pot ser 1 o p. D'altra banda, l'ordre del grup H és el nombre d'ideals primers diferents en A^+ que divideixen ℓ.

Per a veure això, comencem per observar que el caràcter de Teichmüller identifica l'automorfisme de Frobenius associat a un primer $\mathfrak{l}$ de A que divideix ℓ amb l'element $\ell \in G(p)$; en efecte, l'automorfisme de Frobenius $F_\mathfrak{l}$ està definit unívocament per la condició que $F_\mathfrak{l}(b) - b^\ell \in \mathfrak{l}$, per a tot element $b \in A$; en particular, se satisfà la condició que $F_\mathfrak{l}(\zeta) - \zeta^\ell \in \mathfrak{l}$; però tot automorfisme de K envia ζ a una potència de ζ, de manera que existeix un nombre enter k, definit mòdul p, tal que $F_\mathfrak{l}(\zeta) = \zeta^k$; ara, dels fets que $\zeta^k - \zeta^\ell \in \mathfrak{l}$, que $\mathfrak{l} \neq \mathfrak{p}$, i que ζ és un element invertible de A, s'obté que $k \equiv \ell \pmod p$, de manera que $F_\mathfrak{l}$ és l'automorfisme definit per la condició que $\omega(F_\mathfrak{l}) = \ell$; és a dir, $F_\mathfrak{l}$ s'identifica amb ℓ en $G(p)$.

D'altra banda, l'automorfisme de Frobenius de $F_\mathfrak{l}$ restringeix a l'automorfisme de Frobenius de la contracció de $\mathfrak{l}$ a A^+, de manera que per a tot ideal primer $\mathfrak{l}$ de A^+, la identificació de $\mathrm{Gal}\,(K^+|\mathbb{Q})$ amb el grup dels caràcter parells de $G(p)$ transforma l'automorfisme de Frobenius associat a $\mathfrak{l}$ en l'element ℓ de $G(p)$. En conseqüència, dir que un caràcter actua trivialment sobre ℓ equival a dir que actua trivialment sobre l'automorfisme de Frobenius associat a ℓ. Per tant, H és el grup de caràcters de $\mathrm{Gal}\,(K^+|\mathbb{Q})$ que actuen trivialment sobre l'automorfisme de Frobenius associat a ℓ; si es vol, H és l'ortogonal en $\widehat{G(p)}$ del subgrup generat per l'automorfisme de Frobenius associat a ℓ. Dit d'una altra manera, el cos fix per la intersecció dels nuclis dels caràcters de H és el cos de descomposició de ℓ, en virtut de la caracterització dels ideals que descomponen completament en una extensió com aquells que tenen automorfisme de Frobenius trivial (cf. el corol·lari **5.5.5**). Per tant, H té ordre exactament el nombre d'ideals primers que divideixen ℓ, ja que aquest és el grau sobre $\mathbb{Q}$ del cos de descomposició de ℓ.

Aquestes consideracions ens permeten escriure d'una altra manera el factor d'Euler $(1-\ell^{-sf_\ell})^{-g_\ell}$. En efecte, quan χ recorre un sistema de representants de les classes laterals de G mòdul H, $\chi(\ell)$ recorre totes les arrels f_ℓ-èsimes de la unitat una vegada, i només una, ja que el quocient G/H és un grup cíclic d'ordre f_ℓ, isomorf al quocient entre el grup de descomposició i el grup d'inèrcia de qualsevol ideal primer $\mathfrak{l}$ que divideix ℓ. Per tant, el producte $\displaystyle\prod_{\chi\in\widehat{G(p)},\ \chi,\ \text{parell}} (1 - \chi(\ell)\ell^{-s})^{-1}$ coincideix amb el factor d'Euler $(1 - \ell^{-sf_\ell})^{-g_\ell}$.

A més a més, com que p és totalment ramificat, el factor d'Euler $\displaystyle\prod_{\mathfrak{p}|p}(1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}$ és exactament el factor $(1-p^{-s})^{-1}$, ja que només hi ha un ideal primer que divideix p i és de grau residual 1; d'altra banda, tots els caràcters que considerem, llevat del caràcter trivial, s'anul·len en p, ja que el conductor és un divisor de p, de manera que el producte dels

factors $(1-\chi(p)p^{-s})^{-1}$ és el factor $(1-p^{-s})^{-1}$ que correspon al caràcter trivial. Per tant, en el semiplà $\Re(s)>1$, se satisfà la igualtat $\zeta_{K^+}(s)=\zeta(s)\prod_{\chi\in G(p)\widehat{},\,\chi \text{ parell i primitiu}} L(\chi,s)$, que volíem provar; només cal tenir en compte que $\zeta(s)$ és la funció L associada al caràcter trivial. □

Aquest resultat ens permet obtenir una fórmula analítica per al nombre de classes d'ideals de A^+. En efecte, anàlogament als casos dels cossos quadràtics o ciclotòmics, obtenim la fórmula següent.

Corol·lari 16.1.3. *Siguin p un nombre primer senar, ζ una arrel primitiva p-èsima de la unitat, $K^+:=\mathbb{Q}(\zeta+\zeta^{-1})$, A^+ l'anell dels enters de K^+, Δ^+ el discriminant de A^+, R_p^+ el regulador, i h_p^+ el nombre de classes d'ideals. Aleshores,*

$$\frac{2^{\frac{p-1}{2}}h_p^+R_p^+}{2|\Delta_p^+|^{\frac{1}{2}}}=\prod_{\chi\in G(p)\widehat{},\,\chi\neq\chi_1,\chi\ parell} L(\chi,1).\ \square$$

Podem comparar aquesta fórmula amb la que hem obtingut per al cos ciclotòmic $\mathbb{Q}(\zeta)$ (cf. el corol·lari **15.6.2**):

$$\frac{(2\pi)^{\frac{p-1}{2}}h_pR_p}{2p|\Delta_p|^{\frac{1}{2}}}=\prod_{\chi\in G(p)\widehat{},\,\chi\neq\chi_1} L(\chi,1).$$

Per a fer aquesta comparació més precisa, convé calcular el quocient $\dfrac{R_p}{R_p^+}$ i els discriminants. De fet, no costa gens, si tenim en compte que el discriminant de A ja ha estat calculat com $\Delta_p=(-1)^{\frac{p-1}{2}}p^{p-2}$ (cf. el corol·lari **3.9.10**), deduir que $\Delta_p^+=p^{\frac{p-3}{2}}$. D'altra banda, la relació entre els reguladors és donada pel resultat següent.

Proposició 16.1.4. *Amb les mateixes notacions, se satisfà la igualtat $R_p=2^{\frac{p-3}{2}}R_p^+$.*

Demostració: El rang de la part lliure dels grups de les unitats de A i de A^+ és el mateix i val $\dfrac{p-3}{2}$; a més a més, podem elegir un sistema fonamental d'unitats de A format per unitats de A^+, de manera que aquestes unitats també formen un sistema fonamental d'unitats de A^+. D'aquesta manera, només cal comparar els determinants que tenen entrades $e_i\log|\sigma_i(\varepsilon_j)|$, $1\leq i,j\leq\dfrac{p-3}{2}$, on σ_i són les diferents immersions reals o representants de les parelles d'immersions complexes conjugades no reals, i $e_i=1,2$, segons que σ_i sigui real o no. Ara bé, cada una de les immersions de K^+ és real, i cada una dóna lloc a dues immersions complexes conjugades no reals de K, de manera que els dos determinants coincideixen llevat d'un factor $2^{\frac{p-3}{2}}$, que és el producte dels factors e_i. Això acaba la prova. □

Definició 16.1.5. S'anomena primer factor del nombre de classes h_p de K, el nombre de classes h_p^+ de K^+. El quocient, $h_p^-:=\dfrac{h_p}{h_p^+}$ s'anomena el segon factor.

16.2 Càlcul del segon factor del nombre de classes

En aquesta secció es tracta de donar una expressió per al càlcul del segon factor del nombre de classes d'ideals de l'anell dels enters dels cossos ciclotòmics de les arrels p-èsimes de la unitat, p primer senar. De fet, hem definit h_p^- com el quocient entre els nombres de classes h_p i h_p^+, però això només garanteix que $h_p^- \in \mathbb{Q}$. De fet, h_p^- és un nombre enter positiu i es tracta de donar-ne una expressió adient per a obtenir-ne alguna conseqüència.

Comencem per calcular els valors en $s = 1$ de les funcions L associades als caràcters de $G(p)$. Per a això, observem que $\widehat{G(p)}$ és cíclic i generat pel caràcter de Teichmüller $\omega : \mathrm{Gal}\,(K|\mathbb{Q}) \longrightarrow G(p)$, definit per $\sigma(\zeta) = \zeta^{\omega(\sigma)}$. De fet, això és així a partir de la identificació de $G(p)$ amb $\mathrm{Gal}\,(K|\mathbb{Q})$ que proporciona aquest mateix caràcter i la identificació de $G(p)$ amb el grup de les arrels $(p-1)$-èsimes de la unitat de $\mathbb{C}$.

Observem, també, que el caràcter de Teichmüller és de conductor p i és senar, de manera que podem escriure $\widehat{G(p)} = \{\omega, \omega^2, \ldots, \omega^{p-1} = \omega^0\}$, que, per a $1 \leq k \leq p-2$, ω^k és de conductor p, i que ω^k és parell si, i només si, k és parell. Amb aquestes notacions, podem reescriure les fórmules dels nombres de classes de K i de K^+ en la forma

$$\frac{(2\pi)^{\frac{p-1}{2}} h_p R_p}{2p|\Delta_p|^{\frac{1}{2}}} = \prod_{k=0}^{p-2} L(\omega^k, 1), \qquad \frac{2^{\frac{p-1}{2}} h_p^+ R_p^+}{2|\Delta_p^+|^{\frac{1}{2}}} = \prod_{k=0}^{\frac{p-3}{2}} L(\omega^{2k}, 1).$$

Se satisfan les propietats següents.

Lema 16.2.1. *Siguin ω^k, $0 \leq k \leq p-2$, els caràcters de $G(p)$. Aleshores:*

(a) $|\Delta_p| = \prod_{k=0}^{p-2} f_{\omega^k}, \qquad |\Delta_p^+| = \prod_{k=0}^{\frac{p-3}{2}} f_{\omega^{2k}},$

(b) $\prod_{k=1}^{p-2} g(\omega^k) = i^{\frac{p-1}{2}} |\Delta_p|^{\frac{1}{2}}, \qquad i \quad \prod_{k=1}^{\frac{p-3}{2}} g(\omega^{2k}) = |\Delta_p^+|^{\frac{1}{2}},$

on $g(\omega^k)$ és la suma de Gauss normalitzada associada al caràcter ω^k i f_{ω^k} el conductor.

Observació 16.2.2. Les fórmules (a) són les *Führerdiskriminantenproductformeln*, és a dir, les fórmules del producte dels conductors i discriminant.

Demostració: Les dues primeres propietats són immediates, ja que tots els caràcters no trivials dels productes són de conductor p, el caràcter trivial és de conductor 1, i els discriminants són $|\Delta_p| = p^{p-2}$, i $|\Delta_p^+| = p^{\frac{p-3}{2}}$. Anem, doncs, a fer l'estudi de les sumes de Gauss.

Comencem per adonar-nos del fet que, per a $1 \leq k \leq p-1$, és $\omega^k \omega^{(p-1)-k} = \omega^0$, el caràcter trivial, de manera que $\omega^{(p-1)-k}$ és l'invers del caràcter ω^k. Per tant, podem escriure les igualtats $\prod_{k=1}^{p-2} g(\omega^k) = g(\omega^{\frac{p-1}{2}}) \prod_{k=1}^{\frac{p-3}{2}} \big(g(\omega^k) g(\omega^{-k})\big) = g(\omega^{\frac{p-1}{2}}) \prod_{k=1}^{\frac{p-3}{2}} \big|g(\omega^k)\big|^2$, ja que $g(\omega^{-k}) = \omega^k(-1)\overline{g(\omega^k)}$, i $\omega^k(-1) = \pm 1$. Per tant, si tenim en compte el valor absolut de les sumes de Gauss, obtenim que $\prod_{k=1}^{p-2} g(\omega^k) = g(\omega^{\frac{p-1}{2}}) p^{\frac{p-3}{2}} = i^{\frac{p-1}{2}} p^{\frac{1}{2}} p^{\frac{p-3}{2}} = i^{\frac{p-1}{2}} |\Delta_p|^{\frac{1}{2}}$, ja

que el caràcter $\omega^{\frac{p-1}{2}}$ és l'unic caràcter quadràtic de Dirichlet mòdul p, de manera que és el caràcter de Kronecker que correspon al cos quadràtic inclòs en K; i, per tant, ja coneixem la seva suma de Gauss. Això demostra la primera de les fórmules (b).

Per a la darrera fórmula, distingim els casos $p \equiv \pm 1 \pmod 4$. Si $p \equiv 3 \pmod 4$, aleshores $\dfrac{p-1}{2}$ és senar i tenim que $\displaystyle\prod_{k=1}^{\frac{p-3}{2}} g(\omega^{2k}) = \prod_{k=1}^{\frac{p-3}{4}} \left(g(\omega^{2k})\overline{g(\omega^{2k})}\right) = p^{\frac{p-3}{4}} = |\Delta_p^+|^{\frac{1}{2}}$, per les mateixes raons que abans. I si $p \equiv 1 \pmod 4$, aleshores $\dfrac{p-1}{2}$ és parell i podem escriure, anàlogament, que $\displaystyle\prod_{k=1}^{\frac{p-3}{2}} g(\omega^{2k}) = p^{\frac{1}{2}} \prod_{k=1}^{\frac{p-5}{4}} \left(g(\omega^{2k})\overline{g(\omega^{2k})}\right) = |\Delta_p^+|^{\frac{1}{2}}$. □

Aquestes fórmules ens permeten obtenir una fórmula per al càlcul del segon factor del nombre de classes del cos ciclotòmic $\mathbb{Q}(\zeta_p)$. En efecte, podem provar el resultat següent.

Teorema 16.2.3. *Siguin p un nombre primer senar, ω el caràcter de Teichmüller de $G(p)$, i h_p^- el segon factor del nombre de classes d'ideals de l'anell dels enters del cos ciclotòmic de les arrels p-èsimes de la unitat. Aleshores, $h_p^- = 2p \displaystyle\prod_{k=1,\, k \text{ senar}}^{p-2} \left(\frac{-1}{2} B_{1,\omega^k}\right)$, on B_{1,ω^k} és el nombre de Bernoulli generalitzat que correspon al caràcter ω^k.*

Demostració: Les fórmules dels nombres de classes que hem provat més amunt ens permeten escriure immediatament el quocient:

$$h_p^- = \frac{h_p}{h_p^+} = \frac{2p|\Delta_p|^{\frac{1}{2}}}{2|\Delta_p^+|^{\frac{1}{2}}} \frac{2^{\frac{p-1}{2}} R_p^+}{(2\pi)^{\frac{p-1}{2}} R_p} \prod_{k=1,\, k \text{ senar}}^{p-2} L(\omega^k, 1) = \frac{p|\Delta_p|^{\frac{1}{2}}}{\pi^{\frac{p-1}{2}} |\Delta_p^+|^{\frac{1}{2}} 2^{\frac{p-3}{2}}} \prod_{k=1,\, k \text{ senar}}^{p-2} L(\omega^k, 1),$$

en virtut de la relació entre els reguladors. D'altra banda, el càlcul de les funcions L associades a caràcters de Dirichlet en el punt $s = 1$ ens permet escriure les noves igualtats

$$\begin{aligned}
h_p^- &= \frac{p|\Delta_p|^{\frac{1}{2}}}{\pi^{\frac{p-1}{2}} |\Delta_p^+|^{\frac{1}{2}} 2^{\frac{p-3}{2}}} \prod_{k=1,\, k \text{ senar}}^{p-2} \frac{\pi i}{p} g(\omega^k) B_{1,\overline{\omega^k}} \\
&= \frac{p|\Delta_p|^{\frac{1}{2}}}{\pi^{\frac{p-1}{2}} |\Delta_p^+|^{\frac{1}{2}} 2^{\frac{p-3}{2}}} \frac{\pi^{\frac{p-1}{2}} i^{\frac{p-1}{2}}}{p^{\frac{p-1}{2}}} \prod_{k=1,\, k \text{ senar}}^{p-2} g(\omega^k) \prod_{k=1,\, k \text{ senar}}^{p-2} B_{1,\overline{\omega^k}} \\
&= \frac{p|\Delta_p|^{\frac{1}{2}} i^{\frac{p-1}{2}}}{|\Delta_p^+|^{\frac{1}{2}} 2^{\frac{p-3}{2}} p^{\frac{p-1}{2}}} \prod_{k=1}^{p-2} g(\omega^k) \prod_{k=1}^{\frac{p-3}{2}} g(\omega^{2k})^{-1} \prod_{k=1,\, k \text{ senar}}^{p-2} B_{1,\overline{\omega^k}} \\
&= \frac{p|\Delta_p|^{\frac{1}{2}} i^{\frac{p-1}{2}}}{|\Delta_p^+|^{\frac{1}{2}} 2^{\frac{p-3}{2}} p^{\frac{p-1}{2}}} \frac{i^{\frac{p-1}{2}} |\Delta_p|^{\frac{1}{2}}}{|\Delta_p^+|^{\frac{1}{2}}} \prod_{k=1,\, k \text{ senar}}^{p-2} B_{1,\overline{\omega^k}} \\
&= \frac{p(-1)^{\frac{p-1}{2}}}{2^{\frac{p-3}{2}}} \prod_{k=1,\, k \text{ senar}}^{p-2} B_{1,\overline{\omega^k}} \\
&= 2p \prod_{k=1,\, k \text{ senar}}^{p-2} \left(\frac{-1}{2} B_{1,\overline{\omega^k}}\right),
\end{aligned}$$

en virtut del lema anterior. Finalment, només cal fer notar que el caràcter $\overline{\omega^k}$ és el caràcter $\omega^{-k} = \omega^{(p-1)-k}$ i que k i $(p-1)-k$ són alhora parells o senars, de manera que el darrer producte és el de l'enunciat. □

Aquesta expressió per al nombre h_p^- ens permet demostrar elementalment que aquest nombre és enter, sense utilitzar resultats de teoria de cossos de classes.

Proposició 16.2.4. *El segon factor, h_p^-, del nombre de classes h_p és enter.*

DEMOSTRACIÓ: Com que el primer factor és el nombre de classes del cos K^+, el quocient h_p^- és un nombre racional positiu. D'altra banda, si tenim en compte la fórmula anterior i l'expressió dels nombres generalitzats de Bernoulli, $B_{1,\omega^k} = \frac{1}{p}\sum_{a=1}^{p-1}\omega^k(a)a$, obtenim l'expressió $h_p^- = 2p\prod_{k=1,\,k\text{ senar}}^{p-2}\frac{-1}{2p}\sum_{a=1}^{p-1}\omega^k(a)a = \frac{1}{(2p)^{\frac{p-3}{2}}}\prod_{k=1,\,k\text{ senar}}^{p-2}\sum_{a=1}^{p-1}\omega^k(a)a$, per al segon factor.

Com que ω és un caràcter del grup $G(p)$, els seus valors no nuls són arrels $(p-1)$-èsimes de la unitat, de manera que les sumes $\sum_{a=1}^{p-1}\omega^k(a)a$ són elements del cos ciclotòmic $\mathbb{Q}(\theta)$, on θ és una arrel primitiva $(p-1)$-èsima de la unitat; no només això, sinó que els valors són enters algebraics d'aquest cos. Per tant, per a demostrar el resultat que volem, és suficient veure que el producte $\prod_{k=1,\,k\text{ senar}}^{p-2}\sum_{a=1}^{p-1}\omega^k(a)a$ és divisible per $(2p)^{\frac{p-3}{2}}$.

Triem un representant qualsevol $g \in \mathbb{Z}$ d'un generador de $G(p)$ i sigui $\theta := \omega(g)$; d'aquesta manera, podem escriure que $F_k := \sum_{a=1}^{p-1}\omega^k(a)a = \sum_{j=0}^{p-2}\omega^k(g^j)g_j = \sum_{j=0}^{p-2}\theta^{jk}g_j$, on $g_j \in \mathbb{Z}$ és el representant de g^j elegit en el conjunt $\{1,2,\ldots,p-1\}$. Se satisfà la relació $g_{\frac{p-1}{2}+j} + g_j \equiv g^{\frac{p-1}{2}+j} + g^j = g^j(g^{\frac{p-1}{2}}+1) \equiv 0 \pmod p$, ja que $g^{\frac{p-1}{2}} \equiv -1 \pmod p$. Per definició dels g_j, obtenim la igualtat $g_{\frac{p-1}{2}+j}+g_j = p$; com que p és senar, també $g_{\frac{p-1}{2}+j}-g_j$ és senar. D'altra banda, $\theta^{\frac{p-1}{2}} = -1$, ja que θ és una arrel primitiva $(p-1)$-èsima de la unitat, de manera que, a l'anell dels enters de $\mathbb{Q}(\theta)$ i per a k senar, podem escriure que

$$F_k = \sum_{j=0}^{\frac{p-3}{2}}\left(\theta^{jk}g_j + \theta^{k\frac{p-1}{2}+kj}g_{\frac{p-1}{2}+j}\right) = \sum_{j=0}^{\frac{p-3}{2}}\left(g_j - g_{\frac{p-1}{2}+j}\right)\theta^{kj} \equiv \sum_{j=0}^{\frac{p-3}{2}}\theta^{kj} \pmod 2,$$

de manera que, en sumar la sèrie geomètrica i multiplicar per $1-\theta^k$, s'obté la nova relació $(1-\theta^k)F_k \equiv 0 \pmod 2$. Per tant, si multipliquem els factors per a $1 \le k \le p-2$, k senar, obtenim la nova relació $\prod_{k=1,\,k\text{ senar}}^{p-2}(1-\theta^k)F_k \equiv 0 \pmod{2^{\frac{p-1}{2}}}$. Ara, en tenir en compte que se satisfà la igualtat de polinomis $\prod_{k=1}^{p-2}(X-\theta^k) = \frac{X^{p-1}-1}{X-1} = 1 + X + \cdots + X^{p-2}$, i substituir X per 1, obtenim la relació $\prod_{k=1}^{p-2}(1-\theta^k) = p-1$.

Anàlogament, com que θ^2 és una arrel primitiva $\dfrac{p-1}{2}$-èsima de la unitat, obtenim la igualtat $\displaystyle\prod_{k=1}^{\frac{p-3}{2}}(1-\theta^{2k})=\frac{p-1}{2}$, de manera que $\displaystyle\prod_{k=1,\,k\text{ senar}}^{p-2}(1-\theta^k)=2$; i, en conseqüència, obtenim que $\displaystyle\prod_{k=1,\,k\text{ senar}}^{p-2}F_k$ és divisible per $2^{\frac{p-3}{2}}$. Resta veure que aquest mateix producte és divisible per $p^{\frac{p-3}{2}}$.

Per a això, prenem $g\in\mathbb{Z}$ de manera que $g^{p-1}\not\equiv 1 \pmod{p^2}$, cosa que es pot fer, si cal, canviant g per $g+p$. D'aquesta manera ens assegurem que la valoració p-àdica de $g^{p-1}-1$ sigui exactament 1. Ara bé, de la relació $\displaystyle\prod_{k=0}^{p-2}(1-\theta^k g)=1-g^{p-1}$, obtenim que la valoració p-àdica del producte és exactament 1. D'altra banda, podem escriure que

$$\begin{aligned}(1-\theta^k g)F_k &\equiv (1-\theta^k g)\sum_{j=0}^{p-2} g^j\theta^{jk}=(1-\theta^k g)\sum_{j=0}^{p-2}(g\theta^k)^j\\ &=(1-\theta^k g)\frac{1-(g\theta^k)^{p-1}}{1-g\theta^k}=1-(g\theta^k)^{p-1}=1-g^{p-1}\equiv 0 \pmod{p},\end{aligned}$$

en sumar la sèrie geomètrica. Per tant, cada un dels factors $F_k(1-g\theta^k)$ és divisible per p, de manera que el producte $\displaystyle\prod_{k=1,\,k\text{ senar}}^{p-2}F_k(1-g\theta^k)$ és divisible per $p^{\frac{p-1}{2}}$. Com que el producte dels factors $(1-g\theta^k)$ és divisible, com a màxim, per p, ja que només multipliquem els factors que corresponen a k senar, obtenim que el producte dels factors F_k és divisible per $p^{\frac{p-3}{2}}$, com calia demostrar. □

16.3 El regulador p-àdic

Ens cal parlar del regulador p-àdic en el cas del cos K^+. Per tant, anem a procedir a la seva introducció.

Recordem que si $\varepsilon_1,\ldots,\varepsilon_{\frac{p-3}{2}}$ és una $\mathbb{Z}$-base del grup de les unitats de A^+ mòdul ±1, hem definit el regulador de K^+ com el valor absolut del determinant que té entrades $\log|\sigma_i(\varepsilon_j)|$, per a $1\le i,j\le\dfrac{p-3}{2}$, on σ_i són les diferents immersions reals de K^+.

Observem que les imatges per les immersions σ_i de les unitats ε_j són elements algebraics; per tant, si prenem una immersió de $\overline{\mathbb{Q}}$ en $\mathbb{C}_p$, podem considerar-los com a elements de $\mathbb{C}_p$. En particular, i com que cada un dels elements $\sigma_i(\varepsilon_j)$ és no nul, podem prendre també logaritmes p-àdics i formar la matriu de coeficients $\log_p(\sigma_i(\varepsilon_j))$, per a $1\le i\le\dfrac{p-1}{2}$, i $1\le j\le\dfrac{p-3}{2}$. Anàlogament com hem vist que els menors d'ordre $\dfrac{p-3}{2}$ de la matriu real són iguals, es demostra que els de la matriu p-àdica també són iguals: per a demostrar-ho només hem fet un càlcul formal sobre les files i columnes d'un determinant (cf. la proposició **15.2.1**).

Aquest procés es pot fer per a qualsevol sistema de $\frac{p-3}{2}$ unitats ε_j que siguin linealment independents, i no cal que siguin una $\mathbb{Z}$-base del grup de les unitats mòdul torsió. Qualsevol dels menors d'ordre $\frac{p-3}{2}$ de la matriu defineix un element de $\mathbb{C}_p$, independent del menor, que es denota per $R_p(\{\varepsilon_j\}_j)$ i s'anomena el regulador p-àdic del sistema $\{\varepsilon_j\}_j$; quan aquest sistema és una base, s'anomena el regulador p-àdic de K, i està definit a menys d'un factor ± 1. En efecte, disposem del resultat següent que relaciona els reguladors de dos sistemes linealment independents d'unitats.

Lema 16.3.1. *Sigui $\{\eta_j\}_j$ el sistema d'unitats donat (multiplicativament) a partir de $\{\varepsilon_j\}_j$ per una matriu $(a_{i,j})$ de coeficients enters. Llavors, $R_p(\{\eta_j\}_j) = \det(a_{i,j})R_p(\{\varepsilon_j\}_j)$.*

Demostració: Efectivament, la matriu $(a_{i,j})$ és, aleshores, la matriu que expressa els vectors (additius) formats pels logaritmes p-àdics dels elements η_j com a combinació lineal dels vectors formats pels logaritmes dels elements ε_j; per tant, estem només en una situació de canvi de base. □

Observació 16.3.2. En particular, el valor absolut (real) del determinant de la matriu $(a_{i,j})$ és l'índex del subgrup generat pels elements η_j en el grup generat pels elements ε_j. Aquest fet s'usarà més endavant.

Lema 16.3.3. *Sigui ε_1 una unitat de A^+. Suposem que existeix un nombre enter $a \in \mathbb{Z}$ tal que $\varepsilon_1 \equiv a \pmod{pA^+}$. Aleshores, $\log_p(\varepsilon_1) \equiv 0 \pmod{pA_p^+}$, on A_p^+ és l'anell dels enters de la compleció de A^+ en l'únic ideal primer de A^+ que divideix p.*

Demostració: Com que $a\varepsilon_1^{-1} \equiv 1 \pmod{pA_p^+}$, el valor absolut p-àdic de la diferència $a\varepsilon_1^{-1} - 1$ és menor o igual que $p^{-\frac{1}{p-1}}$, de manera que $\log_p(a\varepsilon_1^{-1}) \equiv 0 \pmod{pA_p^+}$; és a dir, $\log_p(\varepsilon_1) \equiv \log_p(a) \pmod{pA_p^+}$. Si prenem normes, de la igualtat $\mathrm{N}(\varepsilon) = \pm 1$ obtenim que $\pm 1 \equiv \mathrm{N}(a) = a^{\frac{p-1}{2}} \pmod{pA_p^+}$, i $\log_p(\varepsilon_1) \equiv \log_p(a) \equiv \dfrac{2}{p-1}\log_p(\pm 1) = 0 \pmod{pA_p^+}$, com volíem demostrar. □

Lema 16.3.4. *Sigui $\varepsilon_1, \ldots, \varepsilon_{\frac{p-3}{2}}$ un sistema linealment independent d'unitats de A^+. Suposem que existeix $a \in \mathbb{Z}$ tal que $\varepsilon_1 \equiv a \pmod{pA_p^+}$. Posem $\beta_1 := \dfrac{1}{p}\log_p(\varepsilon_1)$, $\beta_j := \log_p(\varepsilon_j)$, per a $2 \le j \le \dfrac{p-3}{2}$, i $\beta_{\frac{p-1}{2}} = 1$. Aleshores,*

$$\det(\sigma_i(\beta_j)) = \frac{p-1}{2p} R_p(\{\varepsilon_j\}_j), \qquad i \qquad \left| \frac{\det(\sigma_i(\beta_j))}{\Delta_{K^+}^{\frac{1}{2}}} \right|_p \le 1, \text{ en } \mathbb{C}_p.$$

Demostració: En primer lloc, observem que si $x \in K_p^+$, la compleció de K^+ en l'ideal primer que divideix p, aleshores $\log_p(x) \in A_p^+$, en virtut de l'extensió del logaritme p-àdic a tot $\mathbb{C}_p$. D'altra banda, per a $2 \le j \le \dfrac{p-1}{2}$, és $\beta_j \in A_p^+$, i el lema anterior ens permet assegurar que $\beta_1 \in A_p^+$. Per tant, podem considerar el A_p^+-mòdul generat pels elements β_j, $1 \le j \le \dfrac{p-1}{2}$. Sigui $\alpha_1, \ldots, \alpha_{\frac{p-1}{2}}$ una $\mathbb{Z}_p$-base de A_p^+; existeix una matriu $(a_{i,j})$ d'elements $a_{i,j} \in \mathbb{Z}_p$ de manera que $\beta_j = \displaystyle\sum_{k=1}^{\frac{p-1}{2}} a_{k,j}\alpha_k$. Com que $a_{i,j} \in \mathbb{Z}_p$,

per a cada automorfisme de K_p^+ sobre $\mathbb{Q}_p$, σ_i, resulta que $\sigma_i(\beta_j) = \sum_{k=1}^{\frac{p-1}{2}} a_{k,j}\sigma_i(\alpha_k)$. Per tant, també que $\det(\sigma_i(\beta_j)) = \det(a_{k,j})\det(\sigma_i(\alpha_k))$. Ara bé, el discriminant de l'extensió $A_p^+|\mathbb{Z}_p$ coincideix amb el de l'extensió $A^+|\mathbb{Z}$ i és exactament el quadrat del determinant $\det(\sigma_i(\alpha_k))$; per tant, obtenim que $|\Delta_{K^+}^{\frac{1}{2}}|_p = |\det(\sigma_i(\alpha_k))|_p$. D'altra banda, el càlcul del regulador a partir de la matriu dels logaritmes orlada amb una fila de coeficients 1, ens ensenya que $\det(\sigma_i(\beta_j)) = \dfrac{p-1}{2p}R_p(\{\varepsilon_j\}_j)$, ja que el grau de K_p^+ sobre $\mathbb{Q}_p$ és $\dfrac{p-1}{2}$. Això demostra la primera propietat.

Per a acabar, només cal tenir en compte que $p-1$ no és divisible per p, de manera que $\left|\dfrac{\det(\sigma_i(\beta_j))}{\Delta_{K^+}^{\frac{1}{2}}}\right|_p = \left|\dfrac{\det(\sigma_i(\beta_j))}{|\det(\sigma_i(\alpha_k))|_p}\right|_p = |\det(a_{i,j})|_p \leq 1$, ja que $a_{i,j} \in \mathbb{Z}_p$. I això acaba la prova. □

Per a acabar aquesta secció, enunciarem la fórmula p-àdica del nombre de classes del cos K^+. De fet, igual que el regulador p-àdic, aquesta fórmula és més general, però només la utilitzarem en aquest cas. No en donarem la demostració, que es pot seguir, per exemple, en [Wa 82, thm. 5.24, i §8.2] i fa ús de les unitats ciclotòmiques.

Afirmació 16.3.5 (fórmula p-àdica del nombre de classes)**.** Sigui p un nombre primer senar. Aleshores, se satisfà la igualtat $\dfrac{2^{\frac{p-3}{2}}h_p^+R_p(K_p^+)}{\Delta_{K^+}^{\frac{1}{2}}} = \prod_{k=1,\,k\text{ parell}}^{p-3} L_p(\omega^k,1)$, on ω és el caràcter de Teichmüller i $R_p(K^+)$ el regulador p-àdic de K^+.

16.4 El criteri de regularitat de Kummer

Recordem que un nombre primer senar p s'anomena regular quan p no divideix el nombre de classes d'ideals del cos ciclotòmic de les arrels p-èsimes de la unitat. D'altra banda, hem provat que si p és un primer regular, aleshores el primer cas del teorema de Fermat és cert (cf. el teorema **8.5.3**). En aquesta secció es tracta de donar un criteri per a saber quan un nombre primer senar és regular. Comencem per establir el resultat següent.

Proposició 16.4.1. *Sigui p un nombre primer senar qualsevol. Aleshores, en l'anell $\mathbb{Z}_p$ dels nombres enters p-àdics, se satisfà la congruència* $h_p^- \equiv \prod_{k=1}^{\frac{p-3}{2}} \dfrac{-1}{2}\dfrac{B_{2k}}{2k} \pmod{p\mathbb{Z}_p}$.

Demostració: Hem provat (cf. **16.2.3**) que $h_p^- = 2p\prod_{k=1,\,k\text{ senar}}^{p-2}\left(\dfrac{-1}{2}B_{1,\omega^k}\right)$, on ω és el caràcter de Teichmüller de $G(p)$ i B_{1,ω^k} el nombre generalitzat de Bernoulli associat al caràcter ω^k. El càlcul d'aquests nombres (cf. **14.4.7**) ens permet escriure les igualtats $B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} = \dfrac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a)$; i com que $a\omega^{-1}(a) \equiv 1 \pmod{p\mathbb{Z}_p}$, obtenim la congruència $2p\left(\dfrac{-1}{2}B_{1,\omega^{p-2}}\right) = -\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv -(p-1) \equiv 1 \pmod{p\mathbb{Z}_p}$. I les congruències

de Kummer (cf. **14.6.2**), proven que $\prod_{k=1,\, k \text{ senar}}^{p-4} B_{1,\omega^k} \equiv \prod_{k=1,\, k \text{ senar}}^{p-4} \frac{B_{k+1}}{k+1} \pmod{p\mathbb{Z}_p}$, ja que $p-1$ no divideix cap dels nombres $k+1$ que apareixen en el producte. El resultat es dedueix immediatament per multiplicació, tenint en compte que 2 és invertible en $\mathbb{Z}_p$. □

Com a conseqüència immediata d'aquest resultat, obtenim una forma feble del criteri de regularitat de Kummer.

Corol·lari 16.4.2. *Sigui $p \geq 3$ un nombre primer senar. Condició necessària i suficient perquè p no divideixi el segon factor, h_p^-, del nombre de classes de $\mathbb{Q}(\zeta_p)$ és que p no divideixi el numerador de cap dels nombres de Bernoulli B_k, per a $2 \leq k \leq p-3$, k parell.* □

El criteri de regularitat de Kummer afirma que aquesta condició sobre els nombres de Bernoulli és suficient perquè p sigui regular. Per a això, és suficient demostrar el resultat següent.

Proposició 16.4.3. *Sigui p un nombre primer senar. Si p no divideix h_p^-, aleshores p tampoc no divideix h_p^+.*

Demostració: Farem servir la fórmula p-àdica per al nombre de classes del cos K^+. Una petita modificació de la prova del lema **16.3.4** ens ensenya que $\left| \frac{R_p(K^+)}{\Delta_{K^+}^{\frac{1}{2}}} \right|_p \leq 1$. Només cal canviar el sistema $\{\varepsilon_j\}_j$ per un sistema fonamental d'unitats, i substituir β_1 per $\log_p(\varepsilon_1)$, de manera que no calgui la hipòtesi restrictiva sobre ε_1.

Suposem que $p|h_p^+$; cal veure que $p|h_p^-$. La fórmula p-àdica del nombre de classes ens permet assegurar que existeix un enter parell k, $2 \leq k \leq p-3$, tal que p divideix $L_p(\omega^k, 1)$. Ara bé, com que el conductor de ω^k és p i pq no divideix p, el corol·lari anterior a les congruències de Kummer (cf. **14.6.1**) diu que $L_p(\omega^k, 1) \equiv L_p(\omega^k, 0) \pmod{p\mathbb{Z}_p}$. D'altra banda, la interpolació p-àdica de la funció L de Dirichlet associada al caràcter ω^k proporciona, en particular, que $L_p(\omega^k, 0) = -(1-\omega^{k-1}(p))B_{1,\omega^{k-1}} = -B_{1,\omega^{k-1}}$, ja que ω^{k-1} és de conductor p. Per tant, obtenim que $B_{1,\omega^{k-1}}$ és divisible per p en $\mathbb{Z}_p$ per a algun exponent $k-1$ senar. Però ja hem observat que $B_{1,\omega^{k-1}} \equiv \frac{B_k}{k} \pmod{p}$, de manera que p divideix el producte $\prod_{k=1}^{\frac{p-3}{2}} \frac{-1}{2}\frac{B_{2k}}{2k} \equiv h_p^- \pmod{p\mathbb{Z}_p}$, com volíem demostrar. □

Per a acabar aquesta secció, donarem un resultat que farem servir per a la demostració del lema de Kummer.

Corol·lari 16.4.4. *Sigui p un primer regular. Si k és un enter parell no divisible per $p-1$, aleshores $L_p(\omega^k, 1) \not\equiv 0 \pmod{p}$. En particular, $L_p(\omega^k, 1) \neq 0$.*

Demostració: De nou per les propietats de la interpolació p-àdica de la funció L associada a ω^k (cf. **14.5.1**), i si tenim en compte que k no és divisible per $p-1$, de manera que podem utilitzar la congruència $B_{1,\omega^{k-1}} \equiv \frac{B_k}{k} \pmod{p}$ (cf.**14.6.3**), resulta que podem escriure que $L_p(\omega^k, 1) \equiv L_p(\omega^k, 1-k) = -(1-p^{k-1})\frac{B_{k,\chi_1}}{k} \pmod{p\mathbb{Z}_p}$. Però els nombres de Bernoulli associats al caràcter trivial són els nombres de Bernoulli ordinaris, de manera que el resultat queda provat, ja que p no divideix B_k perquè p és regular. □

16.5 El lema de Kummer

L'objectiu d'aquesta secció és de proveir del resultat més fort que es fa servir en la prova del segon cas del teorema de Fermat per a exponents regulars. Concretament, es tracta de demostrar el teorema següent.

Teorema 16.5.1 (Lema de Kummer)**.** *Siguin p un nombre primer, ζ una arrel primitiva p-èsima de la unitat, $K := \mathbb{Q}(\zeta)$, $A := \mathbb{Z}[\zeta]$ l'anell dels enters, i $\varepsilon \in A^*$, un element invertible. Suposem que p és regular i que ε difereix d'un enter en un element de pA. Aleshores, ε és la potència p-èsima d'una unitat de A.*

Demostració: El primer pas de la prova consisteix a demostrar que ε és una unitat real; és a dir, una unitat de l'anell dels enters de $K^+ := \mathbb{Q}(\zeta)^+$. En efecte, ja sabem que tota unitat de A es pot escriure en la forma $\varepsilon = \pm\zeta^k\varepsilon_1$, amb $0 \leq k \leq p-1$ i ε_1 una unitat de A^+. Ara bé, també sabem que $A^+ = \mathbb{Z}[\zeta + \zeta^{-1}]$, de manera que tot element de A^+ satisfà una congruència de la forma $\varepsilon_1 \equiv a \pmod{\mathfrak{p}^+}$, per a un cert nombre enter $a \in \mathbb{Z}$, on $\mathfrak{p}^+$ designa l'únic ideal primer de A^+ que divideix $p\mathbb{Z}$.

En efecte, $\mathfrak{p}^+$ està generat per l'element $(1-\zeta)(1-\zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$, de manera que podem substituir $\zeta + \zeta^{-1}$ per 2 en l'expressió $\varepsilon_1 = \sum_{k=0}^{\frac{p-3}{2}} b_k(\zeta + \zeta^{-1})^k$, $b_k \in \mathbb{Z}$, a fi d'obtenir la congruència $\varepsilon_1 \equiv \sum_{k=0}^{\frac{p-3}{2}} b_k 2^k =: a_1 \in \mathbb{Z} \pmod{\mathfrak{p}^+}$. D'altra banda, també podem escriure que $\zeta^k = (1-(1-\zeta))^k \equiv 1 - k(1-\zeta) \pmod{(1-\zeta)^2}$, de manera que, a partir de la congruència $\varepsilon_1 \equiv a_1 \pmod{\mathfrak{p}^+}$, i per multiplicació, obtenim que se satisfà la nova congruència $\varepsilon = \pm\zeta^k\varepsilon_1 \equiv \pm\big(1 - k(1-\zeta)\big)a_1 \pmod{(1-\zeta)^2}$, en A. Per hipòtesi, existeix $a \in \mathbb{Z}$ tal que $\varepsilon \equiv a \pmod{pA}$; com que $pA = (1-\zeta)^{p-1}A$, obtenim que $a \equiv \pm\big(1 - k(1-\zeta)\big)a_1 \pmod{(1-\zeta)^2}$, de manera que $k \equiv 0 \pmod{(1-\zeta)}$ en A; com que $k \in \mathbb{Z}$, això fa que k sigui divisible per p i $\zeta^k = 1$, de manera que $\varepsilon = \pm\varepsilon_1 \in A^{+*}$ i, per tant, ε és real.

Suposem, ara, que ε no és una potència p-èsima en A. Recordem que el rang del grup de les unitats de A^+ és $\dfrac{p-3}{2}$, de manera que podem trobar unitats $\varepsilon_2, \ldots, \varepsilon_{\frac{p-3}{2}} \in A^+$ de manera que el grup generat per $-1, \varepsilon, \varepsilon_2, \ldots, \varepsilon_{\frac{p-3}{2}}$ és un subgrup d'índex finit i no divisible per p del grup de les unitats de A^+; en efecte, n'hi ha prou d'expressar ε en una $\mathbb{Z}$-base del grup de les unitats i adonar-se que algun dels exponents no és divisible per p, de manera que es pot canviar aquell element de la base per ε per a obtenir el que s'acaba d'enunciar. En particular, com que l'índex del subgrup generat per aquestes unitats en el grup de totes les unitats de K^+ mòdul torsió no és divisible per p, el valor absolut p-àdic del regulador de K^+ coincideix amb el valor absolut p-àdic del sistema $\{\varepsilon, \varepsilon_2, \ldots, \varepsilon_{\frac{p-3}{2}}\}$.

D'altra banda, i per hipòtesi, $\log_p(\varepsilon) \equiv 0 \pmod{pA_p^+}$, de manera que podem aplicar el lema **16.3.4**; obtenim que $\left|\dfrac{R_p(K^+)}{\Delta_{K^+}^{\frac{1}{2}}}\right|_p \leq |p|_p < 1$, de manera que el nombre p-àdic $\dfrac{2^{\frac{p-3}{2}} h_p^+ R_p(K^+)}{\Delta_{K^+}^{\frac{1}{2}}}$ és divisible per p. Si ara apliquem la fórmula p-àdica del nombre de

classes (cf. **16.3.5**), obtenim que el producte $\prod_{k=1,\,k\text{ parell}}^{p-3} L_p(\omega^k,1)$ és divisible per p, i això contradiu el darrer corol·lari de la secció anterior. Per tant, ε ha de ser una potència p-èsima d'una unitat de K, com volíem demostrar. □

16.6 El segon cas del teorema de Fermat per a exponents regulars

El punt final d'aquest curs és la prova del segon cas del teorema de Fermat per a exponents regulars. Recordem que, en el capítol **8**, hem anomenat així un enunciat que ara precisem per al cas d'exponent un nombre primer regular.

Teorema 16.6.1 (Kummer)**.** *Sigui p un nombre primer senar. Suposem que p no divideix el nombre de classes d'ideals, h_p, de l'anell dels enters del cos ciclotòmic de les arrels p-èsimes de la unitat. Llavors, l'equació diofantina $x^p + y^p = z^p$ no té solucions enteres $x, y, z \in \mathbb{Z}$ tals que*

(a) *p no divideix el producte xy,*

(b) *$z \neq 0$ és divisible per p, i*

(c) *x, y, z són primers entre si.*

Demostració: Considerem una arrel primitiva p-èsima de la unitat $\zeta := \zeta_p$, i siguin $K := \mathbb{Q}(\zeta)$, $A := \mathbb{Z}[\zeta]$ l'anell dels enters de K, i $\mathfrak{p} := (1-\zeta)A$. Suposem que existeixen nombres enters x, y, z per als quals se satisfan les condicions (a), (b) i (c), i tals que $x^p + y^p = z^p$. Podem considerar, llavors, els elements de A definits de la manera següent: si v és la valoració p-àdica de z, de manera que $zp^{-v} \in \mathbb{Z}$, posem $\xi := x$, $\eta := y$, $\theta := zp^{-v}$, i $m := v(p-1) \in \mathbb{N}$. Com que $pA = (1-\zeta)^{p-1}A$, existeix una unitat $u \in A^*$ de manera que $p = (1-\zeta)^{p-1}u \in A$. Aleshores, en A se satisfà la igualtat $\xi^p + \eta^p = \omega(1-\zeta)^{pm}\theta^p$, on $\xi, \eta, \theta \in A$, $m := v(p-1) \geq p-1 > 1$, $\omega := u^{vp} \in A^*$, i $\xi, \eta, \theta, 1-\zeta$ són elements primers entre si de A.

Però el resultat següent, una mica més general, ens ensenya que això no pot ser quan p no divideix h_p, i això acabala prova. □

Proposició 16.6.2. *Amb les mateixes notacions, i si p no divideix h_p, aleshores l'equació*

$$\xi^p + \eta^p = \omega(1-\zeta)^{pm}\theta^p \tag{16.6.1}$$

no té solucions en A tals que

(a) *$\xi, \eta, \theta \in A$ siguin no divisibles per $1-\zeta$, (i, en particular, no nuls),*

(b) *$m \in \mathbb{N}$, $m \geq 1$, i*

(c) *$\omega \in A^*$.

DEMOSTRACIÓ: Farem la prova per reducció a l'absurd a partir del lema de Kummer i d'un procés de descens. Suposem que l'equació (16.6.1) té alguna solució per a la qual se satisfan les condicions (a), (b) i (c) de l'enunciat, i triem-ne una de manera que m sigui tant petit com és possible. Podem escriure la igualtat d'elements de A

$$\omega(1-\zeta)^{pm}\theta^p = \xi^p + \eta^p = \prod_{k=0}^{p-1}(\xi+\zeta^k\eta), \tag{16.6.2}$$

igualtat que ens mirarem com a igualtat d'ideals.

Observem, en primer lloc, que $\mathfrak{p} = (1-\zeta)A$ divideix aquest producte d'ideals; per tant, $\mathfrak{p}$ ha de dividir algun dels ideals $(\xi+\zeta^k\eta)$. Com que η no és divisible per $\mathfrak{p}$, per a $j \not\equiv k \pmod p$, la diferència $(\xi+\zeta^k\eta)-(\xi+\zeta^j\eta) = \eta\zeta^k(1-\zeta^{j-k})$ és divisible exactament per $\mathfrak{p}$ i, en conseqüència, tots els ideals $(\xi+\zeta^k\eta)$ són divisibles per $\mathfrak{p}$ i només un d'ells pot ser divisible per potències més altes de $\mathfrak{p}$. Ara bé, com que els p nombres $\xi+\zeta^k\eta$ són diferents mòdul $\mathfrak{p}^2$, i tots són nuls mòdul $\mathfrak{p}$, algun d'ells ha de ser divisible per $\mathfrak{p}^2$. Si convé, canviem η per $\zeta^k\eta$, i podem suposar que $(\xi+\eta)$ és l'únic dels ideals $(\xi+\zeta^k\eta)$ que és divisible per $\mathfrak{p}^2$; i com que tots els altres $p-1$ ideals són divisibles per $\mathfrak{p}$, l'exponent m de la igualtat (16.6.1) ha de ser, obligatòriament, estrictament més gran que 1.

Sigui $\mathfrak{m}$ l'ideal màxim divisor comú dels ideals ξA, ηA; podem escriure igualtats d'ideals

$$(\xi+\eta)A = \mathfrak{p}^{mp-p+1}\mathfrak{m}\mathfrak{a}_0, \qquad (\xi+\zeta^k\eta)A = \mathfrak{p}\mathfrak{m}\mathfrak{a}_k, \quad 1\le k\le p-1,$$

que serveixen de definició dels ideals $\mathfrak{a}_k$, per a $0\le k\le p-1$. Assegurem que els ideals $\mathfrak{a}_k$ són primers entre si dos a dos. En efecte, suposem que $\mathfrak{q}$ és un ideal primer de A que divideix $\mathfrak{a}_k$ i $\mathfrak{a}_j$, per a $j\ne k$; aleshores, els ideals $(\xi+\zeta^k\eta)A$ i $(\xi+\zeta^j\eta)A$ serien divisibles per $\mathfrak{p}\mathfrak{m}\mathfrak{q}$, de manera que també ho serien els ideals

$$\big((\xi+\zeta^k\eta)-(\xi+\zeta^j\eta)\big)A = \zeta^k\eta(1-\zeta^{j-k})A = \eta\mathfrak{p},$$
$$\big((\xi+\zeta^k\eta)-\zeta^{k-j}(\xi+\zeta^j\eta)\big)A = \xi(1-\zeta^{k-j})A = \xi\mathfrak{p},$$

i $\mathfrak{m}\mathfrak{q}$ dividiria els ideals ξA, ηA, contra l'elecció de $\mathfrak{m}$.

Si substituïm en (16.6.2) cada ideal $(\xi+\zeta^k\eta)$, $1\le k\le p-1$, per $\mathfrak{p}\mathfrak{m}\mathfrak{a}_k$ i $(\xi+\eta)$ per $\mathfrak{p}^{mp-p-+1}\mathfrak{m}\mathfrak{a}_0$, i després simplifiquem els factors $\mathfrak{p}^{mp}$ dels dos membres de la igualtat que resulta, obtenim la nova igualtat d'ideals $\mathfrak{m}^p\mathfrak{a}_0\mathfrak{a}_1\cdots\mathfrak{a}_{p-1} = \theta^pA$, de manera que els ideals $\mathfrak{a}_k$ són potències p-èsimes d'ideals de A, ja que són primers entre si i el seu producte és la potència p-èsima d'un ideal. Per tant, podem escriure $\mathfrak{a}_k =: \mathfrak{b}_k^p$, per a $0\le k\le p-1$, on $\mathfrak{b}_k$ és un cert ideal de A. Dit d'una altra manera, podem escriure igualtats d'ideals

$$(\xi+\eta)A = \mathfrak{p}^{pm-p+1}\mathfrak{m}\mathfrak{b}_0^p, \qquad (\xi+\zeta^k\eta)A = \mathfrak{p}\mathfrak{m}\mathfrak{b}_k^p, \quad 1\le k\le p-1.$$

En particular, obtenim expressions en ideals fraccionaris

$$(\xi+\zeta^k\eta)\mathfrak{p}^{pm-p} = \mathfrak{p}^{pm-p+1}\mathfrak{m}\mathfrak{b}_k^p = (\xi+\eta)\mathfrak{b}_k^p\mathfrak{b}_0^{-p}, \qquad 1\le k\le p-1, \tag{16.6.3}$$

de manera que, per ser $\mathfrak{p}$ principal, els ideals fraccionaris $(\mathfrak{b}_k\mathfrak{b}_0^{-1})^p$ també són principals.

Ara aplicarem la hipòtesi que p és un primer regular, és a dir, que p no divideix h_p. Com que p no divideix h_p i les potències p-èsimes dels ideals fraccionaris $\mathfrak{b}_k\mathfrak{b}_0^{-1}$ són principals, també són principals els ideals fraccionaris $\mathfrak{b}_k\mathfrak{b}_0^{-1}$; per tant, existeixen elements

$\alpha_k, \beta_k \in A$, $1 \leq k \leq p-1$, tals que $\mathfrak{b}_k \mathfrak{b}_0^{-1} = \alpha_k \beta_k^{-1} A$; i, com que $\mathfrak{p}$ és un ideal principal, podem suposar que cap dels elements α_k, β_k no és divisible per $\mathfrak{p}$.

Transformem les igualtats d'ideals (16.6.3) en igualtats numèriques. Podem dir que, per a $1 \leq k \leq p-1$, existeixen elements invertibles $\omega_k \in A^*$ tals que

$$(\xi + \zeta^k \eta)(1-\zeta)^{pm-p} = (\xi + \eta)(\alpha_k \beta_k^{-1})^p \omega_k. \tag{16.6.4}$$

D'altra banda, de la identitat

$$(1-\zeta)^{pm-p}(\xi + \zeta\eta)(1+\zeta) - (1-\zeta)^{pm-p}(\xi + \zeta^2\eta) = \zeta(1-\zeta)^{pm-p}(\xi + \eta),$$

que s'obté en multiplicar per $(1-\zeta)^{pm-p}$ la identitat òbvia

$$(\xi + \zeta\eta)(1+\zeta) - (\xi + \zeta^2\eta) = \zeta(\xi + \eta),$$

i de les igualtats (4) per a $k = 1, 2$ (que podem usar ja que $p - 1 \geq 2$), obtenim una igualtat

$$(\xi + \eta)\left(\frac{\alpha_1}{\beta_1}\right)^p \omega_1(1+\zeta) - (\xi + \eta)\left(\frac{\alpha_2}{\beta_2}\right)^p \omega_2 = (\xi + \eta)\zeta(1-\zeta)^{pm-p};$$

com que $\xi + \eta$ és no nul, i com que ω_1 i $1 + \zeta$ són unitats de A, podem dividir i obtenim la igualtat

$$(\alpha_1\beta_2)^p - \frac{\omega_2}{\omega_1(1+\zeta)}(\alpha_2\beta_1)^p = \frac{\zeta}{\omega_1(1+\zeta)}(1-\zeta)^{pm-p}(\beta_1\beta_2)^p. \tag{16.6.5}$$

Observem que aquesta igualtat en enters de K és de la mateixa forma que en l'enunciat, llevat d'un factor unitari que acompanya el segon factor, però que ara m ha estat canviat per $m-1$. Si no hi hagués aquesta unitat, $-\dfrac{\omega_2}{\omega_1(1+\zeta)}$, hauríem arribat a contradicció, ja que els enters de A, $\alpha_1\beta_2$, $\alpha_2\beta_1$, $\beta_1\beta_2$ són no nuls i no divisibles per $\mathfrak{p}$. Cal, doncs, treure aquesta unitat. Per a això usarem el lema de Kummer (**16.5.1**). De fet, aquest lema ens permetrà deduir que la unitat $\dfrac{\omega_2}{\omega_1(1+\zeta)}$ és la potència p-èsima d'una unitat de A, de manera que podrem incloure la seva arrel p-èsima en el factor $-\alpha_2\beta_1$ i haurem acabat.

Com que $m > 1$, i com hem vist més amunt, la igualtat 16.6.5 dóna la congruència $\alpha^p - \omega_0\beta^p \equiv 0 \pmod{\mathfrak{p}^p}$, on $\alpha := \alpha_1\beta_2$, $\beta := \alpha_2\beta_1$, i $\omega_0 := \dfrac{\omega_2}{\omega_1(1+\zeta)}$. Com que β no és divisible per $\mathfrak{p}$, podem trobar un element $\gamma \in A$ tal que $\beta\gamma \equiv 1 \pmod{\mathfrak{p}^p}$, de manera que $\omega_0 \equiv \omega_0\beta^p\gamma^p \equiv (\alpha\gamma)^p \pmod{\mathfrak{p}^p}$. Ara bé, com que tot element de A és congru a un nombre enter mòdul $\mathfrak{p}$, existeixen $n \in \mathbb{Z}$, $\delta \in A$ tals que $\alpha\gamma = n + \delta(1-\zeta)$; aleshores, $(\alpha\gamma)^p \equiv n^p \pmod{(1-\zeta)^p}$, de manera que $\omega_0 \equiv n^p \pmod{\mathfrak{p}^p}$ i $n^p \in \mathbb{Z}$. En virtut del lema de Kummer, ω_0 és la potència p-èsima d'una unitat de A, com calia veure per a acabar la prova. □

Apèndix A

Taules

A.1 Nombres de Bernoulli

La llista següent ho és d'alguns nombres de Bernoulli. $B_0 = 1$, $B_1 = \frac{-1}{2}$, $B_2 = \frac{1}{6}$,

$$
\begin{aligned}
B_4 &= \frac{-1}{30} \\
B_6 &= \frac{1}{42} \\
B_8 &= \frac{-1}{30} \\
B_{10} &= \frac{5}{66} \\
B_{12} &= \frac{-691}{2730} \\
B_{14} &= \frac{7}{6} \\
B_{16} &= \frac{-3617}{510} \\
B_{18} &= \frac{43867}{798} \\
B_{20} &= \frac{-174611}{330} \\
B_{22} &= \frac{854513}{138} \\
B_{24} &= \frac{-236364091}{2730} \\
B_{26} &= \frac{8553103}{6} \\
B_{28} &= \frac{-23749461029}{870} \\
B_{30} &= \frac{8615841276005}{14322} \\
B_{32} &= \frac{-7709321041217}{510}
\end{aligned}
$$

$$B_{34} = \frac{2577687858367}{6}$$
$$B_{36} = \frac{-26315271553053477373}{1919190}$$
$$B_{38} = \frac{2929993913841559}{6}$$
$$B_{40} = \frac{-261082718496449122051}{13530}$$
$$B_{42} = \frac{1520097643918070802691}{1806}$$
$$B_{44} = \frac{-27833269579301024235023}{690}$$
$$B_{46} = \frac{59645111159391216327 7961}{282}$$
$$B_{48} = \frac{-560940336899781768624 9127547}{46410}$$
$$B_{50} = \frac{49505720524107964821 2477525}{66}$$
$$B_{52} = \frac{-80116571813548995734 7924991853}{1590}$$
$$B_{54} = \frac{29149963634884862421418123812691}{798}$$
$$B_{56} = \frac{-24793929293132267536854157396632 29}{870}$$
$$B_{58} = \frac{84483613348880041862046775994036021}{354}$$
$$B_{60} = \frac{-12152331404837555720403049940798202460414 91}{56786730}$$
$$B_{62} = \frac{12300585434086858541953039857403386151}{6}$$
$$B_{64} = \frac{-10678383014786652988638544497914264794 2017}{510}$$
$$B_{66} = \frac{14726000221263356540516194285519323422418991 01}{64722}$$
$$B_{68} = \frac{-78773130858718728141909149208474606244347001}{30}$$
$$B_{70} = \frac{15053813473333670038030765673778572085114381602 35}{4686}$$
$$B_{72} = \frac{-58279549616699441104382772446410673652824883018442 60429}{140100870}$$
$$B_{74} = \frac{34152417289221168014330073731472635186688307783087}{6}$$
$$B_{76} = \frac{-24655088825935372707687196040585199904365267828865801}{30}$$
$$B_{78} = \frac{41484636557540082829517903554954207349219937537240048 3487}{3318}$$
$$B_{80} = \frac{-46037842994794576469355749690190468497942578727512889196568 67}{230010}$$

A.2 Polinomis de Bernoulli

La llista següent ho és d'alguns polinomis de Bernoulli.

$$
\begin{aligned}
B_0(x) &= 1 \\
B_1(x) &= x + \frac{1}{2} \\
B_2(x) &= x^2 - x + \frac{1}{6} \\
B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \\
B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30} \\
B_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x \\
B_6(x) &= x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42} \\
B_7(x) &= x^7 - \frac{7}{2}x^6 + \frac{7}{2}x^5 - \frac{7}{6}x^3 + \frac{1}{6}x \\
B_8(x) &= x^8 - 4x^7 + \frac{14}{3}x^6 - \frac{7}{3}x^4 + \frac{2}{3}x^2 - \frac{1}{30} \\
B_9(x) &= x^9 - \frac{9}{2}x^8 + 6X^7 - \frac{21}{5}x^5 + 2x^3 - \frac{3}{10}x \\
B_{10}(x) &= x^{10} - 5x^9 + \frac{15}{2}x^8 - 7x^6 + 5x^4 - \frac{3}{2}x^2 + \frac{5}{66} \\
B_{11}(x) &= x^{11} - \frac{11}{2}x^{10} + \frac{55}{6}x^9 - 11x^7 + 11x^5 - \frac{11}{2}x^3 + \frac{5}{6}x \\
B_{12}(x) &= x^{12} - 6X^{11} + 11x^{10} - \frac{33}{2}x^8 + 22x^6 - \frac{33}{2}x^4 + 5x^2 - \frac{691}{2730}
\end{aligned}
$$

Referències

[Ap 84] **Apostol**, Tom Mike: *Introduction to Analytic Number Theory*. UTM, Springer Verlag, New York, 1976, segona impressió, 1984. ISBN: 0-387-90163-9.

[At-McD 73] **Atiyah**, Michael Francis; **Macdonald**, Ian Grant: *Introducción al Álgebra conmutativa*. Ed. Reverté, Barcelona, 1973. ISBN: 84-291-5008-0. Edició original: *Introduction to Commutative Algebra*, Addison Wesley, Massachussets, 1969. Traducció: Griselda **Pascual** Xufré.

[B-G-T 12] **Bayer**, Pilar; **Guàrdia**, Jordi; **Travesa**, Artur: *Arrels germàniques de la matemàtica contemporània. Amb una antologia de textos matemàtics de* 1850 *a* 1950. Institut d'Estudis Catalans, Barcelona, 2012. ISBN: 978-84-9965-119-4.

[B-M-T 90] **Bayer**, Pilar; **Montes**, Jesús; **Travesa**, Artur: *Problemes d'Àlgebra*. Publicacions de la Universitat de Barcelona; Materials docents, n. 7. Barcelona, 1990. ISBN: 84-7875-361-3.

[B-S 66] **Borevich**, Zenon Ivanovich; **Shafarevich**, Igor Rostislavovich: *Number Theory*. Pure and Applied Mathematics 20, Academic Press, London, 1966. ISBN: 0-12-117850-1. Edició original: *Teoriya Čisel*, Moscow, 1964. Traducció: Newcomb **Greenleaf**.

[Cor 80] **Coromines**, Joan: *Diccionari etimològic i complementari de la llengua catalana*. Curial, edicions catalanes, Barcelona, 1980. ISBN: 84-7256-173-9.

[I-R 82] **Ireland**, Kenneth Frederick; **Rosen**, Michael Ira: *A Classical Introduction to Modern Number Theory*. GTM 84, Springer Verlag, New York, 1982. ISBN: 0-387-90625-8. Edició ampliada de l'obra dels mateixos autors: *Elements of Number Theory*, Bogden and Quigley Inc. Pub., 1972.

[Ja 73] **Janusz**, Gerald J.: *Algebraic Number Fields*. Pure and Applied Mathematics 55, Academic Press, London, 1973. ISBN: 0-12-380250-4.

[La 70] **Lang**, Serge: *Algebraic Number Theory*. Addison Wesley, Reading, Massachussets, 1970. ISBN: 0-201-04201-0.

[Neu 86] **Neukirch**, Jürgen; *Class Field Theory*. GMW 280, Springer Verlag, Berlin, 1986. ISBN: 3-540-15251-2.

[Ri 72] **Ribenboim**, Paulo: *L'arithmétique des corps*. Méthodes, Hermann, París, 1972. ISBN: 2-7056-5665-0.

[Rie 1859] **Riemann**, Georg Friedrich Bernhard; Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie*, November, 1859, p. 145–153.

[Sa 72] **Samuel**, Pierre: *Teoría algebraica de números*. Métodos, Omega, Barcelona, 1972. Edició original: *Théorie algébrique des nombres*, Hermann, Paris, 1967. Traducció: Manuel **Udina** Abelló i María José **Castello** Esnal

[Se 70] **Serre**, Jean-Pierre: *Cours d'Arithmétique*. Le Mathématicien 2, Presses Universitaires de France, segona edició, Paris, 1977. Primera edició, 1970.

[Se 79] **Serre**, Jean-Pierre: *Local Fields*. GTM 67, Springer Verlag, New York, 1979. ISBN: 0-387-90424-7, 3-540-90424-7. Edició original: *Corps locaux*, Ed. Hermann, Paris, 1962. Traducció: Marvin Jay **Greenberg**.

[Tra 1998] **Travesa**, Artur: *Aritmètica*, Edicions de la Universitat de Barcelona, Col·lecció Materials docents, n. 25, Barcelona, 1998. ISBN: 84-8338-031-5.

[Tra 2020] **Travesa**, Artur: *Equacions algebraiques*, Barcelona, 2020. Disponible en format pdf a la pàgina https://travesa.cat/notes.html

[vdW 70] **van der Waerden**, Bartel Leendert: *Algebra*, vol. 1 i 2. Frederick Ungar Pub. Co. New York, 1970. ISBN: 0-8044-4950-3, 0-8044-4951-1. Edició original, en alemany: *Moderne Algebra*, Springer Verlag, Berlin, 1930, 1931. Traducció de la setena edició (1966), vol. 1; i de la cinquena edició (1967), vol. 2: John R. **Schulenberger**.

[Wa 82] **Washington**, Lawrence Clinton: *Introduction to cyclotomic fields*, GTM 83, Springer Verlag, New York, 1982. ISBN: 0-387-90622-3, 3-540-90622-3

[W-W 70] **Whittaker**, Edmund. Taylor; **Watson**, George Neville: *A course of Modern Analysis*, Cambridge University Press, Cambridge, 2005. Reimpressió de la quarta edició (1927); edició original de 1902. ISBN: 0-521-58807-3.

[Wi 1995] **Wiles**, Andrew John: Modular elliptic curves and Fermat's last theorem, *Annals of Mathematics* **141** (1995), p. 443-551.

Índex terminològic

p-grup, 95
índex
    de ramificació, 36, 96
àlgebra
    de quaternions, 161

Abel, 194
abscissa
    de convergència, 195
    de convergència absoluta, 188
acció
    contínua, 57
    transitiva, 40
adherència, 104
anàlisi
    p-àdica, 1
    complexa, 1
anell
    íntegrament tancat, 24
    commutatiu, 23
    compacte, 146
    complet, 133
    d'enters, 139
    de Dedekind, 27
    de valoració, 121, 122
      discreta, 123, 132
    dels enters d'un cos de nombres, 25
    euclidià, 255
    localitzat, 24, 31
aproximació diofantina, 1
aritmètica, 1
arrel
    de la unitat, 188
    primitiva de la unitat, 4, 50
automorfisme de Frobenius, 85, 104, 263

base
    d'entorns, 103, 126
    dual respecte d'una forma bilineal no degenerada, 27
    ortogonal, 156
Bernoulli, 209, 227, 230

cadena normal, 87
caràcter
    ciclotòmic, 4, 262
    d'un grup abelià, 6
    de Dirichlet, 7, 188, 219, 227, 230
    de Kronecker, 18, 49, 262
    de Legendre, 8, 12
    de Teichmüller, 262, 263
    parell, 229
    primitiu de Dirichlet, 8
    quadràtic de Dirichlet, 8
    senar, 228
    trivial, 8, 262
característica, 14, 60
Cauchy, 195
Clausen, 212
clausura
    algebraica, 4
    entera, 24
    separable, 35
codiferent, 75
commutador, 88
compleció, 128
    profinita, 104
conductor, 227
    d'un anell en un subanell, 78
    d'un caràcter de Dirichlet, 8
    d'una extensió abeliana, 100
congruències de Kummer, 231
conjugació complexa, 8
conjugat, 34
conjunt
    fonamental d'unitats, 69
    mesurable Lebesgue, 59
convolució de Dirichlet, 185
corba el·líptica, 1, 57, 58
cos
    ciclotòmic, 23, 50, 96, 233, 261
    complet, 128, 133
    d'inèrcia, 83
    de descomposició, 83
    de nombres, 1, 23, 25, 233
    global, 1
    local, 1

quadràtic, 233
residual, 36
topològic, 126, 133
criteri
d'Euler, 9
de regularitat de Kummer, 271

Dedekind, 233, 236, 242, 244, 245, 262
densitat, 236
de Dirichlet, 218, 222
Descartes, 72
desigualtat
de la mitjana geomètrica, 64
triangular, 124
ultramètrica, 124
diferent, 75, 76, 98
dimensió d'un espai quadràtic, 154
Dirichlet, 64, 67, 185, 187, 188, 199, 217, 236, 243, 244
disc de convergència absoluta, 190
discriminant, 12, 42, 44, 75
absolut, 63
d'una forma quadràtica, 154
distància, 126, 128
domini
euclidià, 26
factorial, 24
fonamental, 57
noetherià, 26
principal, 24

element
enter sobre un anell, 24
idempotent, 141
primitiu, 5, 34
elements
associats, 51
conjugats, 6
endomorfisme nilpotent, 47
enter
algebraic, 25
de Gauss, 23, 25
equació
de Fermat, 110
diofantina, 1
espai
dual, 155
mètric, 128
quadràtic, 153
topològic, 57
vectorial
normat, 134
topològic, 134
Euler, 9, 193, 199, 234, 263
exponencial, 148
exponent
d'un grup abelià finit, 6
diferencial, 76
extensió
abeliana, 3, 4, 95
algebraica, 24
cíclica, 3, 95
ciclotòmica, 4
composició, 3
de Galois, 3, 40
entera, 24
finita, 3, 26
intersecció, 3
moderadament ramificada, 89, 101
nilpotent, 3
no ramificada, 38, 96
normal, 3
purament inseparable, 35
quadràtica, 6, 11, 49
ramificada, 38, 95
resoluble, 3
salvatgement ramificada, 90
separable, 3, 26, 60
totalment ramificada, 54, 96
extensions linealment disjuntes, 4, 95

fórmula
analítica del nombre de classes, 233, 264
d'Hadamard, 148
d'inversió de Möbius, 186
de sumació d'Abel, 194
del producte, 128, 175
del residu, 242, 245
factor d'Euler, 193, 263
família
absolutament sumable, 233
uniformement sumable, 233
Fermat, 110, 115, 230, 261, 273
fita de Minkowski, 62
forma
bilineal, 153
diferencial algebraica, 1
modular, 1, 57
quadràtica, 153
no degenerada, 155
no singular, 155
Frobenius, 104, 263
frontera, 57
funció

Γ d'Euler, 199
L, 1, 188, 262
L de Dirichlet, 199, 242
abeliana, 1
analítica, 1
  p-àdica, 215, 227
aritmètica, 185
  completament multiplicativa, 185
  multiplicativa, 185
d'Euler, 50
de classe C^1, 194
de Möbius, 45, 186
el·líptica, 1
esglaonada, 194
holomorfa p-àdica, 227
integrable Lebesgue, 202
meromorfa p-àdica, 227
zeta, 1
  de Dedekind, 221, 233, 236, 242, 245, 262
  de Hurwitz, 199, 202
  de Riemann, 188, 199, 202, 233, 242

gènere, 58
Galois, 82, 103
Gauss, 23, 253
generador topològic, 108
geometria aritmètica, 1
grau
  d'inseparabilitat, 34, 83
  de separabilitat, 34, 60, 83
  residual, 37
grup
  abelià lliure, 58
  d'ideals, 30
  d'inèrcia, 42, 81, 96, 105, 107
    moderada, 90
  d'isotropia, 41
  de classes d'ideals, 30, 57
  de descomposició, 41, 81, 105
  de Galois, 3
    absolut, 104
  de ramificació superior, 87, 96
  de valors d'una valoració, 131
  discret, 57, 58
  dual, 6
  procíclic, 108
  profinit, 103
  resoluble, 90
  topològic, 57
    compacte, 103
    discret, 57
    finitament generat, 108
    Hausdorff, 103
  totalment ordenat, 121

Haar, 60
Hadamard, 148
Hasse, 168, 178, 182, 217
Hausdorff, 103, 133
Hensel, 141, 142
Hermite, 65, 97
Hilbert, 164
hipòtesi de Riemann, 212
homeomorfisme, 57
Hurwitz, 199, 202

ideal
  de valoració, 122
  discriminant, 43, 46
  enter, 28
  extensió, 36
  fraccionari, 28
    principal, 28
  primer, 36
idempotent, 141
idempotents ortogonals, 141
immersió, 34, 235
  canònica, 61, 67
  logarítmica, 67, 235
integral de Riemann-Stieltjes, 194
interpolació p-àdica, 212
invariant de Hasse-Witt, 168
isometria, 129

Jacobi, 16

Krasner, 143, 147
Kronecker, 75, 95
Kummer, 117, 230, 231, 271, 272

límit, 128
  inductiu, 103
  projectiu, 103, 132, 133
Laurent, 133, 211
Lebesgue, 59, 202
Legendre, 12, 179
lema
  d'aproximació, 176
  de Gauss, 23
  de Hensel, 141, 142, 146, 165, 178
  de Krasner, 143, 147
  de Kummer, 271, 272
  de Nakayama, 39
Levi, 202
llei de reciprocitat quadràtica, 14, 16, 54

logaritme, 149
  p-àdic, 149
  real, 148

Möbius, 186
mètode
  de Gauss, 157
  del descens, 115
malla, 235
  d'una xarxa, 59
matriu
  de Vandermonde, 35
  transposada, 35
mesura de Haar, 60
Minkowski, 59, 62, 68, 97, 178, 182, 217
multiplicació complexa, 1

nombre
  algebraic, 227
  de Bernoulli, 209, 227, 229, 230
  de classes, 245, 261
  generalitzat de Bernoulli, 224, 228
norma, 33, 44, 134
  d'un ideal, 233
  d'un quaternió, 162
  del suprem, 134

operació transitiva, 40
Ostrowski, 129

paral·lelepípede fonamental, 58, 59
paral·lelogram fonamental, 57
període (de Gauss), 5
pla hiperbòlic, 155
polinomi
  ciclotòmic, 45, 51
  de Bernoulli, 209
  de Newton, 6
  derivat, 44
  simètric, 6
    elemental, 6
primer
  descompost totalment, 48
  factor del nombre de classes, 264
  inert, 48
  moderadament ramificat, 89
  no ramificat, 107
  regular, 117, 261, 270, 271, 273
  salvatgement ramificat, 90
  totalment ramificat, 107
principi de Hasse, 182
producte
  d'Euler, 193, 234
  de Dirichlet, 185
  infinit, 192
progressió geomètrica, 11

quaternió conjugat, 162

radi de convergència, 148
radical, 156
  d'un espai quadràtic, 155
rang d'una forma quadràtica, 154
recobriment, 60
regla
  de Descartes, 72
  de l'Höpital, 225
regulador, 234, 236
  p-àdic, 269
relacions d'ortogonalitat de caràcters, 7
residu quadràtic, 49
resultant, 144
Riemann, 188, 194, 199, 202, 212, 233

sèrie
  L de Dirichlet, 219
  de Dirichlet, 185, 187, 190, 243
  de Laurent, 133, 211
  de potències, 190
  exponencial, 148
  funcional, 187
  invertible, 209
  logaritme, 149
  zeta
    de Dedekind, 233
    de Riemann, 188
símbol
  de Hilbert, 164, 168, 175
  de Jacobi, 16
  de Kronecker, 18
  de Legendre, 8, 165
segon cas del teorema de Fermat, 261, 273
segon factor del nombre de classes, 264
semiplà
  de convergència, 195
  de convergència absoluta, 187, 190
  de Poincaré, 58
signatura, 176
signe de les sumes de Gauss, 253
sistema
  cofinal, 103
  fonamental d'unitats, 69, 235
Stieltjes, 194
subanell topològic, 133
subcòs real maximal, 261

subespai
  isòtrop, 155
  ortogonal, 155
subgrup
  obert, 103
  tancat, 103
successió
  coherent, 133
  convergent, 128
  de Cauchy, 128
suma
  de Gauss, 9, 253
  normalitzada de Gauss, 10
  ortogonal, 156
superfície de Riemann, 58

Teichmüller, 262, 263
teorema
  d'Hermite, 65
  d'Hermite-Minkowski, 64, 97
  d'Ostrowski, 129, 130, 135
  de Clausen-von Staudt, 212, 213
  de Dirichlet, 64, 67, 69, 177, 217, 218, 222
    de la progressió aritmètica, 217
  de Dirichlet-Dedekind, 236
  de Fermat, 2, 261, 273
  de Hasse-Minkowski, 153, 178, 182, 217
  de Kronecker-Weber, 1, 4, 11, 75, 95
  de la progressió aritmètica, 217, 222
  de Legendre, 179
  de Levi, 202
  de Minkowski, 59, 64, 68
  de Wilson, 258
  de Witt, 157, 158
  fonamental de la teoria de Galois, 3, 103
  xinès del residu, 13, 31
teoria
  de cossos de classes, 267
  de Galois, 1, 82, 103
  de la ramificació, 1
  de nombres, 1
terna pitagòrica, 110
topologia, 126
tor, 58
torsió, 58
traça, 27, 33

unitat, 57
  fonamental, 70, 235

valor
  absolut, 124
    p-àdic, 125
    arquimedià, 124, 125
    no arquimedià, 124, 125
    no ultramètric, 124
    trivial, 124
    ultramètric, 124
    usual, 125
  propi, 47
valoració, 121
  $\mathfrak{p}$-àdica, 123
  p-àdica, 123
  discreta, 123
  real, 123
  trivial, 122
Vandermonde, 35
varietat abeliana, 1
vector
  isòtrop, 155
  totalment isòtrop, 155
von Staudt, 212

Weber, 75, 95
Wilson, 258
Witt, 168

xarxa, 57, 59

zero trivial de la funció zeta, 212