Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 1

Aquest full de problemes serà resolt a les sessions del 16 i 23 de setembre.

Exercici 1. L'anell dels *enters de Gauss* es defineix com

$$\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\},$$

on $i = \sqrt{-1}$. Anàlogament, anomenarem

$$\mathbb{Q}(i) = \{a + ib \,|\, a, b \in \mathbb{Q}\}$$

el cos dels *nombres racionals de Gauss*. Definim la *norma* d'un nombre de Gauss $\alpha = a + ib$ com

$$N(\alpha) = \alpha\bar{\alpha} = (a + ib)(a - ib) = a^2 + b^2.$$

i) Demostreu que $\mathbb{Z}[i]$ és un domini euclidià respecte a la norma

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}\,.$$

ii) Demostreu que $N(\alpha\beta) = N(\alpha)N(\beta)$ per tot $\alpha, \beta \in \mathbb{Z}[i]$.

iii) Demostreu que $\alpha \in \mathbb{Z}[i]$ és una unitat si i només si $N(\alpha) = 1$.

iv) Sigui p un primer senar de $\mathbb{Z}$. Demostreu que p no és un element primer de $\mathbb{Z}[i]$ si i només si $p \equiv 1 \pmod 4$.

v) (Fermat $\sim$1750) Sigui p un primer senar de $\mathbb{Z}$. Demostreu que p es pot expressar com la suma dels quadrats de dos nombres enters si si i només si $p \equiv 1 \pmod 4$.

vi) Demostreu que llevat d'associats, els elements primers de $\mathbb{Z}[i]$ són:

   a) $1 + i$.

   b) $a + ib$, on $a, b \in \mathbb{Z}$ són tals que $a^2 + b^2$ és un primer $p \equiv 1 \pmod 4$ de $\mathbb{Z}$ i $a > |b| > 0$.

   c) p, on $p \equiv 3 \pmod 4$ és un primer de $\mathbb{Z}$.

Exercici 2. Ternes pitagòriques. Diem que $(x, y, z) \in \mathbb{Z}^3_{>0}$ és una *terna pitagòrica* si $x^2 + y^2 = z^2$.

i) Demostreu que per $\alpha \in \mathbb{Q}(i)$:

$$N(\alpha) = 1 \quad \text{si i només si} \quad \alpha = \frac{\beta}{\bar{\beta}} \text{ per algun } \beta \in \mathbb{Q}(i) \text{ no nul.}$$

ii) Deduïu de l'apartat anterior que si (x, y, z) és una terna pitagòrica, aleshores existeix un enter positiu d i dos enters relativament primers u i v tals que

$$x = d(v^2 - u^2), \quad y = 2duv, \quad z = d(u^2 + v^2),$$

llevat de permutació de x i y.

iii) Doneu una demostració geomètrica de l'apartat anterior seguint els següents passos. Considereu $C : X^2 + Y^2 = 1$ i $L_m : Y = m(X + 1)$ per $m \in \mathbb{Q}$. Demostreu que existeix una bijecció entre els punts de coordenades racionals de C a l'interior primer quadrant amb els punts d'intersecció de C amb L_m diferents de $(-1, 0)$ amb $0 < m < 1$. Considereu l'aplicació natural del conjunt de ternes pitagòriques a C.

Exercici 3. Equació de Fermat per $n = 3$. Definim l'anell dels *enters d'Eisenstein* com

$$\mathbb{Z}[\rho] = \{a + b\rho \,|\, a, b \in \mathbb{Z}\}, \qquad \text{on } \rho = \frac{1 + \sqrt{-3}}{2}.$$

L'objectiu d'aquest exercici és demostrar que l'equació

$$x^3 + y^3 = z^3$$

no té cap solució amb $x, y, z \in \mathbb{Z}$ tals que $xyz \neq 0$. Més en general, demostrarem que, per a tot $u \in \mathbb{Z}[\rho]^\times$, l'equació

$$x^3 + y^3 = uz^3 \tag{1}$$

no té cap solució amb $x, y, z \in \mathbb{Z}[\rho]$ tals que $xyz \neq 0$. Podeu seguir els següents passos:

i) Demostreu que $\mathbb{Z}[\rho]$ és un anell euclidià i que $\mathbb{Z}[\rho]^\times = \langle \rho \rangle$.

ii) Proveu que $\lambda = 1 + \rho$ és un element primer i que $3 = \rho^{-1}\lambda^2$. Donat $\alpha \in \mathbb{Z}[\rho]$ no nul, denotarem per $\mathrm{ord}_\lambda(\alpha)$ la màxima potència de λ dividint α. Demostreu que donats $\alpha, \beta \in \mathbb{Z}[\rho]$ se satisfà

$$\mathrm{ord}_\lambda(\alpha + \beta) \geq \min\{\mathrm{ord}_\lambda(\alpha), \mathrm{ord}_\lambda(\beta)\}.$$

Mostreu que en la desigualtat de dalt es té igualtat si $\mathrm{ord}_\lambda(\alpha) \neq \mathrm{ord}_\lambda(\beta)$.

iii) Demostreu que l'aplicació

$$\Phi : \mathbb{Z}[\rho] \to \mathbb{Z}/3\mathbb{Z}, \qquad \Phi(a + b\rho) = a - b$$

és un morfisme d'anells i que indueix un isomorfisme $\mathbb{Z}[\rho]/(\lambda) \simeq \mathbb{Z}/3\mathbb{Z}$.

iv) Proveu que no existeixen solucions tals que $\lambda \nmid xyz$.

Indicacions: Vegeu que si $x \in \mathbb{Z}[\rho]$ *i* $x \equiv \pm 1 \pmod{\lambda}$, *aleshores* $x^3 \equiv \pm 1 \pmod{\lambda^4}$.

v) Demostreu que tota solució amb $\lambda \nmid xy$ compleix $\lambda^2 \mid z$.

vi) Demostreu que, per a tota solució amb $\lambda \nmid xy$, d'entre els nombres

$$\mathrm{ord}_\lambda(x+y)\,, \qquad \mathrm{ord}_\lambda(\rho^2 x+\rho^4 y)\,, \qquad \mathrm{ord}_\lambda(\rho^4 x+\rho^2 y)$$

n'hi ha exactament dos que valen 1.

Indicacions: Considereu la descomposició

$$(x+y)(\rho^2 x+\rho^4 y)(\rho^4 x+\rho^2 y) = x^3+y^3 = uz^3\,.$$

vii) Diem que una solució de (1) és primitiva si $\gcd(x,y,z)=1$. Proveu que si (x,y,z) és una solució primitiva amb $\lambda \nmid xy$, aleshores n'hi ha una altra (x_1,y_1,z_1) amb $\lambda \nmid x_1y_1$ i amb $\mathrm{ord}_\lambda z_1 < \mathrm{ord}_\lambda(z)$.

viii) Demostreu que (1) no té cap solució amb $x,y,z \in \mathbb{Z}[\rho]$ tals que $xyz \neq 0$.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 2

Presenteu les vostres solucions al Campus Virtual abans del dimecres 28/9/2022 a les 23:59. Recordeu d'esmentar les fonts consultades per a la resolució dels exercicis.

Exercici 1. Sigui D un domini d'integritat i $x \in D \setminus \{0\}$. Demostreu que x és irreductible si i només si (x) és maximal entre tots els ideals principals propis de D. Deduïu que si D és un domini d'ideals principals, aleshores x és irreductible si i només si (x) és maximal. Doneu un exemple d'un domini de factorització única D i d'un element irreductible $x \in D$ tal que (x) no sigui maximal.

Exercici 2. Sigui $D = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ per $m \equiv 1 \pmod 4$ i $m < 0$.

i) Demostreu que $u \in D^\times$ si i només si el valor absolut complex de u és 1.

ii) Demostreu que si $m < -3$, aleshores $D^\times = \{\pm 1\}$.

iii) Demostreu que 2 i 3 són elements irreductibles de $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

Exercici 3. Sigui D un domini d'integritat que no és un cos. Diem que un element $\beta \in D \setminus (D^\times \cup \{0\})$ és un *divisor lateral universal* si per a tot $\alpha \in D$ existeix $\delta \in D^\times \cup \{0\}$ tal que $\alpha - \delta$ és divisible per β.

i) Demostreu que si D no té divisors laterals universals, aleshores D no és domini euclidià respecte a cap funció euclidiana

$$N : D \to \mathbb{Z}_{\geq 0}.$$

Indicació: Suposant que D és un domini euclidià respecte a N, considereu el mínim del conjunt

$$S = \{N(\alpha) \,|\, \alpha \in D \setminus (D^\times \cup \{0\})\}.$$

ii) Demostreu que $D = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ no és un domini euclidià per a cap funció euclidiana.

Indicació: Considerant l'element $\alpha = 2$, vegeu que els únics divisors laterals universals possibles són associats a 2 i 3. Considerant l'element $\alpha = \frac{1+\sqrt{-19}}{2}$, demostreu que 2 i 3 no poden ser divisors laterals universals.

Comentari: En un full de problemes posterior demostrarem, no obstant, que D és un domini d'ideals principals.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 3

Presenteu les vostres solucions al Campus Virtual abans del dimecres 5/10/2022 a les 23:59. Recordeu d'esmentar les fonts consultades per a la resolució dels exercicis.

Exercici 1. Sigui D un domini de factorització única. Sigui x un element del cos de fraccions de D. Demostreu que x és íntegre sobre D si i només si $x \in D$.

Exercici 2. Doneu exemples de:

i) Un anell A, un A-mòdul finitament generat M i un submòdul $N \subseteq M$ que no sigui finitament generat.

ii) Un anell noetherià B i un subanell $A \subseteq B$ que no sigui noetherià.

Exercici 3. Demostreu que $R = \mathbb{Q}[x,y]/(y^2 - x^3)$ és un domini. Demostreu que existeix un element del cos de fraccions de R que no pertany a R i que és íntegre sobre R.

Indicació: Per demostrar que R és un domini, identifiqueu-lo amb un subanell de $\mathbb{Q}[T]$ estudiant el nucli de l'homomorfisme d'anells

$$\Phi : \mathbb{Q}[x,y] \to \mathbb{Q}[T]$$

que envia x a T^2 i y a T^3.

Exercici 4. Sigui B un domini d'integritat i $A \subseteq B$ un subanell tal que B és íntegre sobre A. Demostreu que B és un cos si i només si A és un cos.

Indicació: Supposant que A és un cos, donat $b \in B \setminus \{0\}$, vegeu que l'aplicació

$$\Phi : A[b] \to A[b]\,, \qquad \Phi(y) = by$$

és una aplicació A-lineal injectiva entre espais vectorials de dimensió finita sobre A.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 4

Aquest full serà resolt a la sessió del 17/10/2022.

Exercici 1. Sigui $K = \mathbb{Q}(\sqrt{m})$, on m és un enter lliure de quadrats. Demostreu que l'anell d'enters algebraics de K està donat per

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & \text{si } m \not\equiv 1 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Exercici 2. Sigui $K = \mathbb{Q}(\sqrt{m})$, on m és un enter *negatiu* lliure de quadrats. Demostreu que

$$(\mathcal{O}_K)^\times = \begin{cases} \langle i \rangle & \text{si } m = -1, \\ \langle \rho \rangle & \text{si } m = -3, \\ \langle -1 \rangle & \text{altrament.} \end{cases}$$

Indicació: En virtut de l'exercici anterior, dels exercicis 1 i 3 de FP 1, i de l'exercici 2 de FP 2, només cal considerar el cas $m = -2$ i el cas $m < -3$ i $m \equiv 3 \pmod 4$.

Exercici 3. Sigui $K = \mathbb{Q}(\sqrt{m})$, on $m \neq 1$ és un enter *positiu* lliure de quadrats. L'objectiu d'aquest exercici és demostrar que

$$\#(\mathcal{O}_K)^\times = \infty\,.$$

Sobre $\mathbb{Z} + \mathbb{Z}\sqrt{m} \subseteq \mathcal{O}_K$, definim la següent norma

$$N : \mathbb{Z} + \mathbb{Z}\sqrt{m} \to \mathbb{Z}\,, \qquad N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2\,.$$

Noteu que aquesta no és el quadrat de la norma complexa i que, en particular, pot prendre valors negatius.

i) Sigui $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Demostreu que $\alpha \in (\mathbb{Z} + \mathbb{Z}\sqrt{m})^\times$ si i només si $N(\alpha) = \pm 1$. Doneu un exemple de m i α per als quals $N(\alpha) = -1$.

ii) Demostreu que per a tot $n \in \mathbb{Z}_{\geq 1}$ existeixen $a, b \in \mathbb{Z}$ tals que

$$0 < |a - b\sqrt{m}| < \frac{1}{n} \qquad \text{i} \qquad 0 < b < n.$$

Indicació: Per $i \in \{0, 1, \ldots, n\}$, considereu els elements

$$0 < (\lfloor i\sqrt{m} \rfloor + 1) - i\sqrt{m} \leq 1$$

i llurs diferències.

iii) Demostreu que existeixen infinits parells d'enters (a, b) tals que

$$0 < |N(a + b\sqrt{m})| < 1 + 2\sqrt{m}\,.$$

Indicació: Donada una parella d'enters (a, b) satisfent

$$0 < |a - b\sqrt{m}| < \frac{1}{n} \qquad i \qquad 0 < b < n,$$

apliqueu l'apartat anterior amb $n' \in \mathbb{Z}_{\geq 1}$ tal que $1/n' < |a - b\sqrt{m}|$ per obtenir una parella (a', b') satisfent

$$0 < |a' - b'\sqrt{m}| < \frac{1}{n'} \qquad i \qquad 0 < b' < n',$$

iv) Demostreu que existeix un enter t amb $0 < |t| < 1 + 2\sqrt{m}$ tal que l'equació

$$N(a + b\sqrt{m}) = t$$

té infinites solucions en $a, b \in \mathbb{Z}$ amb $a, b > 0$ i $\gcd(b, t) = 1$.

v) Demostreu que existeix $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, amb $\alpha \neq \pm 1$, tal que $N(\alpha) = 1$.

Indicació: Justifiqueu l'existència de dues solucions diferents (a_1, b_1) i (a_2, b_2) de l'equació de l'apartat anterior satisfent

$$a_1 b_2 \equiv a_2 b_1 \pmod{t}$$

i considereu l'element

$$\alpha := \frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} \in \mathcal{O}_K\,.$$

vi) Deduïu de l'apartat anterior que $\#(\mathcal{O}_K)^\times = \infty$.

Comentari: El resultat d'aquest exercici se segueix de manera immediata del Teorema de les unitats de Dirichlet, que veurem més endavant en aquesta assignatura. En el cas d'un cos quadratic real K, aquest teorema garanteix l'existència d'un element $\eta \in (\mathcal{O}_K)^\times$ tal que

$$(\mathcal{O}_K)^\times = \{\pm\eta^n : n \in \mathbb{Z}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}\,.$$

Exercici 4. Escriviu

$$\alpha = \left(\frac{1 + \sqrt{2}}{9}\right)^{1/3} + \left(\frac{1 - \sqrt{2}}{9}\right)^{1/3}$$

com el quocient d'un enter algebraic per un enter.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 5

Presenteu les vostres solucions al Campus Virtual abans del dimecres 19/10/2022 a les 23:59. Recordeu d'esmentar les fonts consultades per a la resolució dels exercicis.

Exercici 1. Sigui K un cos de nombres de grau $n = [K : \mathbb{Q}]$. Siguin $\sigma_i : K \to \mathbb{C}$, per $i = 1, \dots, n$, les n diferents immersions de K en $\mathbb{C}$ i sigui $\alpha \in K$. Es defineix la *traça de* α com

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)\,.$$

Es defineix la *norma de* α com

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)\,.$$

(Observeu que aquesta definició de norma generalitza les definicions donades a FP 1 Ex. 1 i a FP 4 Ex. 3). Considereu

$$\Phi_{K,\alpha} : K \to K\,, \qquad \Phi_{K,\alpha}(x) = \alpha x\,.$$

Sigui $A_{K,\alpha} \in M_n(\mathbb{Q})$ la matriu de l'aplicació $\mathbb{Q}$-lineal $\Phi_{K,\alpha}$ en una base qualsevol de K com a $\mathbb{Q}$-espai vectorial.

i) Demostreu que

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(A_{K,\alpha})\,, \qquad N_{K/\mathbb{Q}}(\alpha) = \det(A_{K,\alpha})\,.$$

(Això justifica la terminologia de "traça" utilitzada per referir-nos a $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$).

Indicació: Demostreu primer el cas particular en què α és un element primitiu de K. Sigui

$$f_{K,\alpha}(T) = \det(T \cdot I_n - A_{K,\alpha}) \in \mathbb{Q}[T]$$

el polinomi característic de $\Phi_{K,\alpha}$, $\mathrm{Irr}(\alpha;\mathbb{Q})(T)$ el polinomi irreductible de α sobre $\mathbb{Q}$ i $m = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Deduïu el cas general del cas particular emprant el resultat de teoria que diu que

$$f_{K,\alpha}(T) = (\mathrm{Irr}(\alpha;\mathbb{Q})(T))^{n/m}\,.$$

ii) Observeu que si $\alpha \in \mathcal{O}_K$, aleshores $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)\,, N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Exercici 2. Sigui K un cos de nombres de grau $n = [K : \mathbb{Q}]$ i sigui $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$. Denotem per $f(T) := \mathrm{Irr}(\theta;\mathbb{Q})(T) \in \mathbb{Q}[T]$ el polinomi irreductible de θ sobre $\mathbb{Q}$.

i) Demostreu que

$$D(1,\theta,\dots,\theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta))\,.$$

Indicació: Utilitzeu que $D(1,\theta,\dots,\theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\sigma_i(\theta)-\sigma_j(\theta))$.

ii) Calculeu l'expressió de l'apartat anterior en termes de $a, b \in \mathbb{Q}$ en cas que $f(T) = T^n + aT + b$ per $n = 2, 3$.

Indicació: Per $n = 3$*, el resultat és* $-27b^2 - 4a^3$.

Exercici 3. Sigui $\zeta \in \mathbb{C}$ una arrel primitiva cinquena de la unitat. Calculeu

$$\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta+\zeta^{-1}) \qquad \text{i} \qquad N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta+\zeta^{-1})\,.$$

Indicació: Utilitzeu el fet conegut de l'assignatura d'Equacions algebraiques que $\mathrm{Irr}(\zeta;\mathbb{Q})(T) = T^4 + T^3 + T^2 + T + 1$.

Exercici 4.

i) Sigui $K = \mathbb{Q}(\alpha)$, on $\alpha^3 - \alpha - 1 = 0$. Demostreu que l'anell d'enters de K és $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

ii) Sigui $K = \mathbb{Q}(\alpha)$, on $\alpha^3 - d = 0$ amb $d \neq \pm 1$ un enter lliure de quadrats. Demostreu que $[K\colon \mathbb{Q}] = 3$ i que $\mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\alpha]$.

Indicació: Sigui $\theta = u + \alpha v + w\alpha^2$*, amb* $u, v, w \in \mathbb{Q}$*, un element de* $\mathcal{O}_K$*. Calculeu*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\theta) = 3u \in \mathbb{Z}, \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\theta) = 3wd \in \mathbb{Z}, \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2\theta) = 3vd \in \mathbb{Z},$$

$$N_{K/\mathbb{Q}}(\theta) = u^3 + v^3 d + w^3 d^2 - 3uvwd \in \mathbb{Z}\,.$$

Considerant $3^3 \cdot d \cdot N_{K/\mathbb{Q}}(\theta)$ *i* $3^3 \cdot N_{K/\mathbb{Q}}(\theta)$ *deduïu que* $3u, 3v, 3w \in \mathbb{Z}$.

iii) Sigui $K = \mathbb{Q}(\alpha)$, on $\alpha^3 - 17 = 0$. Demostreu que l'anell d'enters de K és

$$\mathcal{O}_K = \mathbb{Z}\left[1, \alpha, \frac{\alpha^2 - \alpha + 1}{3}\right]\,.$$

Indicació: Combinant l'Ex. 2 i l'Ex. 4 ii), primer observeu que el discriminant de K *és o bé* $-3^3 \cdot 17^2$ *o* $-3 \cdot 17^2$*. Demostreu que* $\beta := (\alpha^2 - \alpha + 1)/3$ *satisfà* $\beta^3 - \beta^2 + 6\beta - 12 = 0$*. Per fer-ho, podeu utilitzar que* $\beta = 6/(\alpha+1)$*. Calculeu* $D(1,\alpha,\beta)$ *a partir de* $D(1,\alpha,\alpha^2)$ *per deduir que el discriminant de* K *és* $-3 \cdot 17^2$.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 6

Presenteu les vostres solucions al Campus Virtual abans del dijous 27/10/2022 a les 15:00. Recordeu d'esmentar les fonts consultades.

Exercici 1. Sigui $K = \mathbb{Q}(\sqrt{m})$, on $m \neq 1$ és un enter lliure de quadrats. Demostreu que

$$d(K) = \begin{cases} 4m & \text{si } m \not\equiv 1 \pmod 4, \\ m & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Indicació: Recordeu que, per un cos de nombres F de grau n, definim el seu discriminant $d(F)$ com $D(\alpha_1, \ldots, \alpha_n)$, on $\alpha_1, \ldots, \alpha_n$ és una $\mathbb{Z}$-base de F, és a dir, una base de l'anell d'enters $\mathcal{O}_F$ com a $\mathbb{Z}$-mòdul.

Exercici 2. Sigui p un primer senar i ζ_p una arrel primitiva p-èsima de la unitat a $\overline{\mathbb{Q}}$. Demostreu que

$$D(1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}\,.$$

Indicació: Utilitzeu que $\mathrm{Irr}(\zeta_p, \mathbb{Q})(T) = T^{p-1} + \cdots + T^2 + T + 1$ *i apliqueu Ex. 2 de FP 5.*

Exercici 3. Sigui $K = \mathbb{Q}(\sqrt{-5})$ i considerem l'ideal $\mathfrak{a} = \langle 2, 1+\sqrt{-5}\rangle$. Calculeu la norma $N(\mathfrak{a})$.

Indicació: Recordeu que si $\mathfrak{b}$ és un ideal de l'anell d'enters $\mathcal{O}_F$ d'un cos de nombres F de grau n, la seva norma es defineix com

$$N(\mathfrak{b}) = \sqrt{\frac{D(\beta_1, \ldots, \beta_n)}{d(F)}}\,,$$

on $\beta_1, \ldots, \beta_n$ és una base de $\mathfrak{b}$ com a $\mathbb{Z}$-mòdul.

Exercici 4. Sigui K un cos de nombres de grau n. Mostreu que si $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, aleshores

$$D(\alpha_1, \ldots, \alpha_n) \equiv 0 \pmod 4 \quad \text{o} \quad D(\alpha_1, \ldots, \alpha_n) \equiv 1 \pmod 4\,.$$

Indicació: Sigui $\mathfrak{A}_n$ el grup alternat, és a dir, el subgrup del grup simètric $\mathfrak{S}_n$ format per permutacions de signe positiu. Siguin $\sigma_1, \ldots, \sigma_n$ les immersions de K a $\overline{\mathbb{Q}}$. Mostreu que si escrivim

$$P = \sum_{\pi \in \mathfrak{A}_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}), \qquad N = \sum_{\pi \in \mathfrak{S}_n \setminus \mathfrak{A}_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}),$$

aleshores $PN, P+N \in \mathbb{Z}$. Expresseu el discriminant en termes de P i N.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 7

Presenteu les vostres solucions al Campus Virtual abans del dijous 3/11/2022 a les 15:00. Recordeu d'esmentar les fonts consultades.

Exercici 1. Sigui L/K una extensió de cossos de nombres de grau relatiu $n = [L : K]$. Siguin σ_i, per $i = 1, \dots, n$, les n immersions de L en $\mathbb{C}$ que fixen K, i sigui $\alpha \in L$. Es defineix la *traça relativa de* α com

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)\,.$$

Es defineix la *norma relativa de* α com

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)\,.$$

(Observeu que aquestes definicions de traça i norma generalitzen les definicions donades a FP 5 Ex. 1).

i) Observeu que si $\alpha \in \mathcal{O}_L$, aleshores $\mathrm{Tr}_{L/K}(\alpha)\,, N_{L/K}(\alpha) \in \mathcal{O}_K$.

ii) Demostreu que si L/K és quadràtica, aleshores per $\alpha \in L$ tenim que $\alpha \in \mathcal{O}_L$ si i només si $\mathrm{Tr}_{L/K}(\alpha)\,, N_{L/K}(\alpha) \in \mathcal{O}_K$.

Indicació: Utilitzeu el resultat de teoria que diu que si tenim dominis d'integritat $A \subseteq B \subseteq C$ tals que C és íntegre sobre B i B és íntegre sobre A, aleshores C és íntegre sobre A.

Exercici 2. Sigui $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, on $m, n \neq 1$ són enters lliures de quadrats. Observeu que K conté $\mathbb{Q}(\sqrt{k})$, on $k = mn/\gcd(m,n)^2$. Suposeu que $m \equiv 3 \pmod 4$ i que $n \equiv k \equiv 2 \pmod 4$.

i) Demostreu que els elements

$$1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}$$

formen una $\mathbb{Z}$-base de $\mathcal{O}_K$.

ii) Calculeu el discriminant de $\mathbb{Q}(\sqrt{3}, \sqrt{2})$.

Indicació: Per fer el primer apartat, el primer pas és veure que tot element $\alpha \in \mathcal{O}_K$ es pot escriure de la forma

$$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}\,, \qquad \textit{on } a, b, c, d \in \mathbb{Z}.$$

Per veure això, escriviu α com una combinació lineal amb coefficients racionals de $1, \sqrt{m}, \sqrt{n}, \sqrt{k}$, calculeu les traces relatives $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$, $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{n})}(\alpha)$, $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{k})}(\alpha)$ i utilitzeu FP 4 Ex 1. Després vegeu que $a \equiv b \equiv 0 \pmod 2$ i que $c \equiv d \pmod 2$ tot calculant $N_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$.

Exercici 3. Demostreu que:

i) Si k és un cos, aleshores $k[X_1, X_2, \dots]$ és un domini de factorització única, però no és un anell de Dedekind.

ii) $\mathbb{Z}[X]$ és un domini de factorització única, però no és un anell de Dedekind.

Exercici 4. Sigui R un anell de Dedekind. Demostreu que R és un domini de factorització única si i només si R és un domini d'ideals principals.

Indicació: Per la 'només si' part de la implicació, us caldrà utilitzar un resultat fonamental de l'assignatura, que aviat veureu a teoria. És el següent: En un anell de Dedekind, tot ideal factoritza com a producte d'ideals primers. Deduïu-ne que n'hi ha prou amb veure que tot ideal primer $\mathfrak{p}$ és principal. Per demostrar això, prengueu un element no nul de $\mathfrak{p}$ i considereu la seva factorització en producte d'elements primers de R.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 8

Presenteu les vostres solucions al Campus Virtual abans del dijous 24/11/2022 a les 15:00. Recordeu d'esmentar les fonts consultades.

Exercici 1. Sigui K un cos de nombres i $\mathfrak{a} \subseteq \mathcal{O}_K$ un ideal. Recordeu que la norma de l'ideal $\mathfrak{a}$ es defineix com

$$N(\mathfrak{a}) = \sqrt{\frac{D(\alpha_1, \alpha_2, \ldots, \alpha_n)}{d(K)}}\,,$$

on $\alpha_1, \ldots, \alpha_n$ formen una $\mathbb{Z}$-base de $\mathfrak{a}$. Demostreu que si $\alpha \in \mathcal{O}_K$, aleshores

$$N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|\,,$$

on $N_{K/\mathbb{Q}}$ és la norma definida a Ex. 1 de FP 5.

Exercici 2. Sigui K un cos de nombres i $\mathfrak{p} \subseteq \mathcal{O}_K$ un ideal primer. De teoria sabem que tot ideal fraccionari no nul $\mathfrak{a}$ es pot escriure com

$$\mathfrak{a} = \mathfrak{p}^r \cdot \mathfrak{q}\,, \qquad \text{on } r \in \mathbb{Z} \text{ i } \mathfrak{q} \text{ és un ideal fraccionari no divisible per } \mathfrak{p}.$$

Definim la valoració $\mathfrak{p}$-àdica de $\mathfrak{a}$ com $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = r$. Noteu que $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ està ben definit, perquè tot ideal fraccionari no nul factoritza de manera única com a producte de potències d'exponent enter d'ideals primers. Sigui $\alpha \in K$ no nul. Definim

$$\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}((\alpha))\,.$$

Demostreu que:

i) Donats ideals fraccionaris no nuls $\mathfrak{a}$ i $\mathfrak{b}$, se satisfà

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} \cdot \mathfrak{b}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\,,$$

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\}\,.$$

ii) Donats $\alpha, \beta \in K$ tals que $\alpha, \beta, \alpha + \beta$ són no nuls, se satisfà

$$\mathrm{ord}_{\mathfrak{p}}(\alpha \cdot \beta) = \mathrm{ord}_{\mathfrak{p}}(\alpha) + \mathrm{ord}_{\mathfrak{p}}(\beta)\,,$$

$$\mathrm{ord}_{\mathfrak{p}}(\alpha + \beta) \geq \min\{\mathrm{ord}_{\mathfrak{p}}(\alpha), \mathrm{ord}_{\mathfrak{p}}(\beta)\}\,.$$

La desigualtat anterior és una igualtat si $\mathrm{ord}_{\mathfrak{p}}(\alpha) \neq \mathrm{ord}_{\mathfrak{p}}(\beta)$.

Exercici 3. Sigui p un primer senar, ζ una arrel p-èsima primitiva de la unitat i $K = \mathbb{Q}(\zeta)$. Sigui $\mathfrak{p} \subseteq \mathcal{O}_K$ l'ideal generat per $1 - \zeta$. L'objectiu d'aquest exercici és demostrar que $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

i) Siguin r i s enters tals que $\gcd(p, rs) = 1$. Demostreu que

$$\frac{\zeta^r - 1}{\zeta^s - 1} \in \mathbb{Z}[\zeta]^\times .$$

ii) Demostreu que $\mathfrak{p}$ és un ideal primer i que $(p) = \mathfrak{p}^{p-1}$.

Indicació: Utilitzeu que el polinomi ciclotòmic p-èsim es pot escriure de la forma

$$\Phi_p(T) = T^{p-1} + \cdots + T + 1 = (T - \zeta)(T - \zeta^2) \cdots (T - \zeta^{p-1}) .$$

iii) Sigui $a \in \mathbb{Q} \subseteq K$ no nul. Demostreu que $\mathrm{ord}_{\mathfrak{p}}(a) \equiv 0 \pmod{p-1}$.

Indicació: Observeu que per l'apartat anterior és suficient demostrar que $\mathrm{ord}_{\mathfrak{p}}(q) = 0$ si $q \in \mathbb{Z}$ és un primer diferent de p.

iv) Justifiqueu que $1, 1 - \zeta, (1 - \zeta)^2, \ldots, (1 - \zeta)^{p-2}$ és una $\mathbb{Q}$-base de K. Demostreu que si $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Q}$ són els coeficients d'un element $\alpha \in \mathcal{O}_K$ en aquesta base

$$\alpha = a_0 + a_1(1 - \zeta) + \cdots + a_{p-2}(1 - \zeta)^{p-2},$$

aleshores $\mathrm{ord}_{\mathfrak{p}}(a_i) \geq 0$ per tot $a_i \neq 0$.

v) Demostreu que tot $\alpha \in \mathcal{O}_K$ és pot escriure de la forma

$$\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} ,$$

on $b_i \in \mathbb{Z}$.

Indicació: Per $i = 1, \ldots, p-1$, sigui

$$\sigma_i : K \to K \subseteq \mathbb{C} , \qquad \sigma_i(\zeta) = \zeta^i .$$

Observeu que

$$\begin{pmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \sigma_3(\alpha) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & \zeta & \zeta^2 & \ldots \\ 1 & \zeta^2 & \zeta^4 & \ldots \\ 1 & \zeta^3 & \zeta^6 & \ldots \\ \vdots & \vdots & \vdots & \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \end{pmatrix}$$

Utilitzant la fórmula del determinant de Vandermonde, deduïu que cada b_i és un enter algebraic dividit per una potència de $1 - \zeta$. Deduïu que b_i és enter combinant la caracterització anterior amb el fet que p no divideix el denominador de b_i, com es pot veure a partir de l'apartat anterior.

Exercici 4.

i) Sigui K un cos de nombres i $\alpha \in \mathcal{O}_K$. Demostreu que $\alpha \in \mathcal{O}_K^\times$ si i només si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

ii) Sigui $K = \mathbb{Q}(\alpha)$, on $\alpha^3 - 2 = 0$. Determineu la factorització en producte d'ideals primers de $(2) \subseteq \mathcal{O}_K$ i de $(3) \subseteq \mathcal{O}_K$.

Indicació: Noteu que $3 = (\alpha - 1)(\alpha + 1)^3$.

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 9

Presenteu les vostres solucions al Campus Virtual abans del dijous 1/12/2022 a les 15:00. Recordeu d'esmentar les fonts consultades.

Exercici 1. Sigui $q = p^r$ la potència d'un primer p i sigui $\mathbb{F}_q$ el cos finit de q elements. La norma de $x \in \mathbb{F}_q$ es defineix com

$$N_{\mathbb{F}_q/\mathbb{F}_p}(x) = \prod_{i=0}^{r-1} \sigma^i(x)\,,$$

on $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ denota l'automorfisme de Frobenius. Observeu que $N_{\mathbb{F}_q/\mathbb{F}_p}(x) \in \mathbb{F}_p$. Considereu el cos finit $\mathbb{F}_{7^3} = \mathbb{F}_7(\alpha)$, on $\alpha^3 = 2$. Demostreu que si $x = x_0 + x_1\alpha + x_2\alpha^2 \in \mathbb{F}_{7^3}$, on $x_0, x_1, x_2 \in \mathbb{F}_p$, aleshores

$$N_{\mathbb{F}_{7^3}/\mathbb{F}_7}(x) = x_0^3 + 2x_1^3 + 4x_2^3 + x_0x_1x_2\,.$$

Exercici 2. Sigui $K = \mathbb{Q}(\sqrt{-23})$.

i) Determineu ideals primers $\mathfrak{p}, \overline{\mathfrak{p}} \subseteq \mathcal{O}_K$ tals que $\mathfrak{p}\overline{\mathfrak{p}} = (2) \subset \mathcal{O}_K$. Deduïu que $\mathfrak{p}$ no és un ideal principal.

ii) Demostreu que $\mathfrak{p}^3$ és un ideal principal.

Indicació: Considereu la factorització en producte d'ideals primers de

$$\left(\frac{3+\sqrt{-23}}{2}\right) \subseteq \mathcal{O}_K\,.$$

Exercici 3. (Teorema xinès del residu per anells). Sigui A un anell commutatiu i siguin $\mathfrak{a}_1 \ldots, \mathfrak{a}_n \subseteq A$ ideals tals que $\mathfrak{a}_i + \mathfrak{a}_j = A$ per tot $i \neq j$.

i) Demostreu que, donats $x_1 \ldots, x_n \in A$, existeix $x \in A$ tal que $x \equiv x_i \pmod{\mathfrak{a}_i}$ per tot i.

ii) Deduïu que

$$A \Big/ \prod_{i=1}^n \mathfrak{a}_i \simeq A \Big/ \bigcap_{i=1}^n \mathfrak{a}_i \simeq A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n\,.$$

Exercici 4. Sigui D un anell de Dedekind.

i) Demostreu que si $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq D$ són ideals primers diferents, aleshores $\mathfrak{p}_1^{a_1} + \mathfrak{p}_2^{a_2} = D$ per tot $a_1, a_2 \in \mathbb{Z}_{\geq 1}$.

ii) Demostreu que si D té només un nombre finit d'ideals primers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, aleshores D és un domini d'ideals principals.

Indicació: Noteu que n'hi ha prou amb veure que cadascun dels $\mathfrak{p}_i$ és un ideal principal. Per $i = 1, \ldots, r$, considereu $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Utilitzeu el Teorema xinès del residu per trobar $z_i \in D$ tal que $z_i \equiv \pi_i \pmod{\mathfrak{p}_i^2}$ i $z_i \equiv 1 \pmod{\mathfrak{p}_j}$ per tot $j \neq i$. Determineu la factorització en producte d'ideals primers de (z_i).

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 10

Presenteu les vostres solucions al Campus Virtual abans del dijous 8/12/2022 a les 15:00. Recordeu d'esmentar les fonts consultades. L'exercici 4 és opcional.

A les properes sessions de teoria veureu les següents nocions i resultats:

Sigui K un cos de nombres de grau $n = [K : \mathbb{Q}]$ i anell d'enters $\mathcal{O}_K$. Sigui r_1 el nombre d'immersions reals de K i $2r_2$ el nombre d'immersions complexes (i no reals) de K, de manera que $r_1 + 2r_2 = n$. Denotarem per $I(K)$ el grup d'ideals fraccionaris de K no nuls. Sigui $P(K) \subseteq I(K)$ el subgrup d'ideals principals fraccionaris de K. El *grup de classes* (d'ideals) de K es defineix com el quocient $H(K) := I(K)/P(K)$. El cardinal de $H(K)$ s'anomena *nombre de classes*. Es té:

Teorema (finitud del nombre de classes). $H(K)$ és un grup finit.

Proposició (fita de Minkowski). Tota classe d'ideals de $H(K)$ conté un ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ tal que

$$N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}(K)|}\,.$$

Exercici 1.

i) Noteu que si K és un cos quadràtic, aleshores la fita de Minkowski és $\sqrt{|\mathrm{disc}(K)|}/2$ si K és real i $2\sqrt{|\mathrm{disc}(K)|}/\pi$ si K és imaginari.

ii) Demostreu que els cossos quadràtics següents

$$\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{13}),\ \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7})$$

tenen nombre de classes 1.

iii) Calculeu el nombre de classes de $K = \mathbb{Q}(\alpha)$, on $\alpha^3 + \alpha + 1 = 0$.

Exercici 2.

i) Mostreu que $K = \mathbb{Q}(\sqrt{-19})$ té nombre de classes 1.

Indicació: Demostreu que $H(K)$ està generat per l'ideal primer dividint $2\mathcal{O}_K$. Mostreu que aquest ideal és principal.

Comentari: Hem complert doncs la promesa feta a FP 2 Ex. 3 apartat ii).

ii) Mostreu que $K = \mathbb{Q}(\sqrt{-5})$ té grup de classes isomorf a $\mathbb{Z}/2\mathbb{Z}$.

Indicació: Demostreu que $H(K)$ està generat per l'ideal primer dividint $2\mathcal{O}_K$. Mostreu que aquest ideal no és principal.

iii) Mostreu que $K = \mathbb{Q}(\sqrt{-23})$ té grup de classes isomorf a $\mathbb{Z}/3\mathbb{Z}$.

Indicació: Demostreu que $H(K)$ està generat pels ideals primers dividint $2\mathcal{O}_K$ o $3\mathcal{O}_K$, trobeu relacions entre ells estudiant la decomposició en ideals primers de $\left(\frac{1+\sqrt{-23}}{2}\right)\mathcal{O}_K$, i concloeu utilitzant FP 9 Ex. 2.

Exercici 3. Demostreu que, per tot cos de nombres K, existeix una extensió de cossos L/K finita tal que, per tot ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, l'ideal $\mathfrak{a}\mathcal{O}_L$ de $\mathcal{O}_L$ és principal.

Indicació: Utilitzeu la finitud del grup de classes.

Exercici 4. (Teorema de Warning-Chevalley) Sigui $\mathbb{F}_q$ un cos finit de característica p. Sigui $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomi homogeni de grau d i sigui

$$V := \{\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n : F(\mathbf{a}) = 0\}.$$

Per $\mathbf{a} \in \mathbb{F}_q^n$, definim $G(\mathbf{a}) := F(\mathbf{a})^{q-1}$. Demostreu que:

i) $\#(\mathbb{F}_q^n \setminus V) \equiv \sum_{\mathbf{a}\in\mathbb{F}_q^n} G(\mathbf{a}) \pmod{p}$.

ii) Per $\alpha \in \mathbb{Z}_{\geq 0}$, es té
$$\sum_{a\in\mathbb{F}_q} a^\alpha \equiv 0 \pmod{p}$$
llevat que α sigui un múltiple no nul de $q-1$.

iii) Per $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$, escrivim $\mathbf{a}^\alpha = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$. Es té:
$$\sum_{\mathbf{a}\in\mathbb{F}_q^n} \mathbf{a}^\alpha \equiv 0 \pmod{p}$$
llevat que $\alpha_1 + \cdots + \alpha_n \geq n(q-1)$.

iv) Si $n > d$, aleshores
$$\sum_{\mathbf{a}\in\mathbb{F}_q^n} G(\mathbf{a}) \equiv 0 \pmod{p}, \quad \#(\mathbb{F}_q^n \setminus V) \equiv 0 \pmod{p}, \quad \#V \equiv 0 \pmod{p}.$$

Indicació: Per ii), expresseu la suma en termes d'un generador de $\mathbb{F}_q^\times$. Per iii), observeu que

$$\sum_{\mathbf{a}\in\mathbb{F}_q^n} \mathbf{a}^\alpha = \left(\sum_{a_1\in\mathbb{F}_q} a_1^{\alpha_1}\right) \cdots \left(\sum_{a_n\in\mathbb{F}_q} a_n^{\alpha_n}\right)$$

i apliqueu ii).

Francesc Fité

Semestre de tardor 2022

Mètodes algebraics en teoria de nombres

Full de problemes 11

Presenteu les vostres solucions al Campus Virtual abans del dijous 15/12/2022 a les 15:00. Recordeu d'esmentar les fonts consultades.

Sigui K un cos de nombres de grau $n = [K : \mathbb{Q}]$ i anell d'enters $\mathcal{O}_K$. Sigui r_1 el nombre d'immersions reals de K i $2r_2$ el nombre d'immersions complexes (i no reals) de K, de manera que $r_1 + 2r_2 = n$. Sigui μ_K el grup d'arrels de la unitat contingudes a K. A la darrera sessió de teoria veureu:

Teorema de les unitats de Dirichlet. Es té un isomorfisme de grups

$$(\mathcal{O}_K)^\times \simeq \mu_K \times \mathbb{Z}^{r_1+r_2-1}.$$

Exercici 1.

i) Demostreu que $K = \mathbb{Q}(\sqrt{-14})$ té grup de classes isomorf a $\mathbb{Z}/4\mathbb{Z}$.

Indicació: Demostreu que $H(K)$ està generat pels ideals primers dividint $2\mathcal{O}_K$ i $3\mathcal{O}_K$, que aquests no són principals, i trobeu relacions entre ells calculant la descomposició en producte d'ideals primers de $(2+\sqrt{-14})\mathcal{O}_K$.

ii) Demostreu que $K = \mathbb{Q}(\sqrt{-30})$ té grup de classes isomorf a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Indicació: Demostreu que $H(K)$ està generat pels ideals primers dividint $2\mathcal{O}_K$, $3\mathcal{O}_K$, i $5\mathcal{O}_K$, que aquests no són principals, i trobeu relacions entre ells considerant un ideal principal de norma 30.

iii) Demostreu que $K = \mathbb{Q}(\sqrt{-26})$ té grup de classes isomorf a $\mathbb{Z}/6\mathbb{Z}$.

Exercici 2. Sigui α un enter algebraic i siguin $\alpha_1, \ldots, \alpha_n$ els seus conjugats. Demostreu que si $|\alpha_i| = 1$ per tot i, on $|\cdot|$ denota la norma complexa, aleshores α és una arrel de la unitat.

Indicació: Fitant els seus coeficients, vegeu que només hi ha un nombre finit de polinomis de $\mathbb{Z}[x]$ dels quals α^r en pot ser arrel, per a qualsevol $r \in \mathbb{Z}_{\geq 1}$. Deduïu-ne la finitud del conjunt $\{\alpha^r\}_{r\geq 1}$.

Exercici 3. Sigui $K = \mathbb{Q}(\sqrt{5})$. Demostreu que

$$(\mathcal{O}_K)^\times = \left\{ \pm \left(\frac{1+\sqrt{5}}{2} \right)^n : n \in \mathbb{Z} \right\}.$$

Indicació: Utilitzant el teorema de les unitats de Dirichlet, mostreu que existeix $\mu \in (\mathcal{O}_K)^\times$ tal que

$$(\mathcal{O}_K)^\times = \{\pm\mu^n : n \in \mathbb{Z}\}.$$

Utilitzant que si $x \in (\mathcal{O}_K)^\times$, aleshores $x, -x, x^{-1}, -x^{-1} \in (\mathcal{O}_K)^\times$, demostreu que podem prendre

$$\mu = \frac{a_1 + b_1\sqrt{5}}{2}, \qquad amb\ a_1, b_1 \in \mathbb{Z},$$

de manera que $a_1, b_1 > 0$. Aquesta μ s'anomena la unitat fonamental de K. Escrivim

$$\mu^n = \frac{a_n + b_n\sqrt{5}}{2}, \qquad amb\ a_n, b_n \in \mathbb{Z}.$$

Demostreu que $\{a_n + b_n\}_{n\geq 1}$ és una successió estrictament creixent. Deduïu-ne que un algoritme per trobar μ és considerant el conjunt

$$\{(a, b) \in \mathbb{Z}^2_{>0} : a\ i\ b\ tenen\ la\ mateixa\ paritat\}$$

i identificant-ne l'element amb $a + b$ mínim tal que $a^2 - 5b^2 = \pm 4$.

Exercici 4. Sigui p un primer senar, ζ_p una arrel primitiva p-èsima de la unitat, i $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ l'anell d'enters de $K = \mathbb{Q}(\zeta_p)$.

i) Demostreu que si k és un enter tal que $0 \leq k \leq p-1$, aleshores

$$\xi = 1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{k-1} \in \mathcal{O}_K^\times.$$

Indicació: Tal com vam veure a FP 8 Ex. 3, recordeu que $|N_{K/\mathbb{Q}}(1-\zeta_p)| = |N_{K/\mathbb{Q}}(1-\zeta_p^k)| = p$ i noteu que $\xi(1-\zeta_p) = 1-\zeta_p^k$.

ii) Demostreu que $\mu_K = \{\pm\zeta_p^k : 0 \leq k \leq p-1\}$.

Indicació: Tot subgrup finit del cos multiplicatiu d'un cos és cíclic. Per tant $\mu_K = \langle\zeta_n\rangle$ per una certa arrel primitiva n-èsima de la unitat ζ_n. Noteu que $2p|n$ i que $\varphi(n) = \varphi(2p)$, on φ és la funció d'Euler.

iii) Preneu una immersió $K \subseteq \mathbb{C}$. Demostreu que tota unitat $u \in \mathcal{O}_K^\times$ pot ser escrita com $u = \zeta_p^i v$, on $0 \leq i \leq p-1$ i $v \in \mathbb{R} \cap \mathcal{O}_K^\times$.

Indicació: Sigui c la conjugació complexa i noteu que restringeix a un automorfisme de K. Mostreu que $u/c(u)$ és una arrel de la unitat a K utilitzant Ex. 2. Noteu que $\mathfrak{p} = (1-\zeta_p) = (1-c(\zeta_p)) \subseteq \mathcal{O}_K$ és un ideal primer i descarteu $u/c(u) = -\zeta_p^j$, per algun $0 \leq j \leq p-1$, trobant una contradicció reduint mòdul $\mathfrak{p}$. Deduïu el resultat a partir de $u/c(u) = \zeta_p^j$.

iv) Siguin $p = 5$, $\zeta = \zeta_5$. Demostreu que

$$\mathcal{O}_K^\times = \{\pm\zeta^i(1+\zeta)^j \,|\, 0 \leq i \leq 4, j \in \mathbb{Z}\}.$$

Indicació: Observeu que

$$\sqrt{5} = \zeta - \zeta^2 - \zeta^3 + \zeta^4, \qquad -\zeta^2(1+\zeta) = (1+\sqrt{5})/2$$

i utilitzeu iii) i Ex. 3.