Tema 2: Cossos

2.1. Trobeu les relacions d'inclusió que hi ha entre els cossos $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i,\sqrt{3})$, $\mathbb{Q}(\sqrt{-3}-\sqrt{3})$ i $\mathbb{Q}(i+\sqrt{-3})$.

2.2. Sigui K un cos de característica $\neq 2$. Demostreu que tota extensió E/K de grau 2 és de la forma $E = K(\sqrt{d})$ per a un element $d \in K$.

2.3. Expresseu els elements següents com a polinomis en X de grau ≤ 3 en el cos $\mathbb{Q}[X]/\langle X^4 - 2X + 2\rangle$:

$$X^{-1}, \qquad (X^2+2X)^3, \qquad (X^3+X^2-1)(-2X^3+X^2-1)^{-1}.$$

2.4. Sigui $P(X) \in K[X]$ un polinomi irreductible. Demostreu que, per a tot element $a \in K$, el polinomi $P(X+a)$ també és irreductible i que es té un isomorfisme de cossos $K[X]/\langle P(X)\rangle \simeq K[X]/\langle P(X+a)\rangle$.

2.5. Siguin α, β elements algebraics sobre un cos K. Demostreu que si $\mathrm{Irr}(\alpha, K; X) = \mathrm{Irr}(\beta, K; X)$ aleshores $K(\alpha) \simeq K(\beta)$, però que el recíproc no és cert.

2.6. Sigui K un cos de característica diferent de 3. Siguin $\alpha, \beta \in K$ elements que no són el cub de cap element de K i sigui E/K una extensió que contingui arrels cúbiques $\sqrt[3]{\alpha}$ i $\sqrt[3]{\beta}$ (és a dir, arrels dels polinomis $X^3-\alpha, X^3-\beta$).

1. Demostreu que si $K(\sqrt[3]{\alpha}) = K(\sqrt[3]{\beta})$ aleshores β/α o β/α^2 són el cub d'algun element de K.
   Indicació: eleveu al cub una expressió $\sqrt[3]{\beta} = a + b\sqrt[3]{\alpha} + c\sqrt[3]{\alpha}^2$ amb $a, b, c \in K$ i, calculant amb els coeficients d'aquesta expressió, deduïu que $a = c = 0$ o bé $a = b = 0$.
2. Demostreu que si K conté les arrels cúbiques de la unitat (les tres arrels del polinomi $X^3 - 1 \in K[X]$) aleshores el recíproc de l'apartat anterior també és cert.

2.7. Demostreu que les extensions $\mathbb{Q}(\sqrt{p})$ per als diferents nombres primers p són totes no isomorfes entre elles.

2.8. Calculeu el polinomi irreductible de $\sqrt{3}+\sqrt{5}$ sobre els cossos següents: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$.

2.9. Calculeu el grau de l'extensió $\mathbb{Q}(e^{2\pi i/n} + e^{-2\pi i/n})/\mathbb{Q}$.

2.10. Considerem l'extensió de cossos $\mathbb{C}/\mathbb{R}$ i la $\mathbb{R}$-base $\{1, i\}$. Donat un element $\alpha = a + bi \in \mathbb{C}$, trobeu la matriu en aquesta base de l'endomorfisme $m_\alpha : \mathbb{C} \to \mathbb{C}$, on $m_\alpha(x) = \alpha x$. Calculeu el seu polinomi característic.

2.11. Considerem una extensió quadràtica $K = \mathbb{Q}(\sqrt{d})/\mathbb{Q}$, amb $d \in \mathbb{Z}$ lliure de quadrats, i fixem la $\mathbb{Q}$-base de K $\{1, \sqrt{d}\}$. Escriviu la representació matricial en aquesta base d'un element $\alpha \in K$ qualsevol. Calculeu el polinomi caracterísitic i el polinomi mínim-

2.12. Sigui $K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, i considerem la $\mathbb{Q}$-base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ de K. Determineu la representació matricial d'un element qualsevol de K respecte d'aquesta base. Calculeu la representació matricial de $\beta = 1/(1 + \sqrt[3]{2} + \sqrt[3]{4})$.

2.13. Sigui $K = \mathbb{Q}(\gamma)/\mathbb{Q}$, el cos cúbic generat per una arrel del polinomi $X^3 - X - 1 \in \mathbb{Q}[X]$. Determineu la representació matricial d'un element qualsevol de K respecte la $\mathbb{Q}$-base $\{1, \gamma, \gamma^2\}$ de K.

2.14. Si L/K és una extensió finita, definim la traça i la norma d'un element $\alpha \in L$ respecte l'extensió L/K com a:

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha), \qquad N_{L/K}(\alpha) = \det(m_\alpha),$$

on $m_\alpha \colon L \to L$ és l'endomorfisme K-lineal de E definit per $m_\alpha(x) = \alpha x$.

a) Quant valen la traça i la norma d'un element de K?
b) Proveu que la traça és additiva i que la norma és multiplicativa.
c) Determineu la traça i la norma en els exemples dels problemes anteriors.
d) Proveu que $1 + \sqrt[3]{2}$ no és un quadrat perfecte a $\mathbb{Q}(\sqrt[3]{2})$.
e) Sigui M/L una altra extensió finita. Demostreu que:

$$N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)), \qquad \mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)).$$

2.15. Trobeu elements primitius de cossos de descomposició dels polinomis $X^3 - 2$ i $X^4 - 2$ sobre $\mathbb{Q}$.

2.16. Siguin α, β elements algebraics de grau 3 sobre un cos K. Estudieu les diferents possibilitats per al grau $[K(\alpha, \beta) : K]$.

2.17. Sigui $r = f(X)/g(X) \in K(X)$ una funció racional no constant a coeficients en un cos K, expressada com a quocient de polinomis f i $g \neq 0$ relativament primers. Demostreu que

1. L'element $r \in K(X)$ és transcendent sobre K.
2. $[K(X) : K(r)] = \max\{\deg f, \deg g\}$.
3. Els automorfismes de $K(X)$ que deixen fixos els elements de K són els que envien X a $\frac{aX+b}{cX+d}$ amb $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$.

2.18. Siguin α, β elements tals que α és transcendent sobre K i algebraic sobre $K(\beta)$. Demostreu que β és transcendent sobre K i algebraic sobre $K(\alpha)$.

2.19. Sigui E/K una extensió. Demostreu que els elements de E que són algebraics sobre K formen un subcos E^a amb $K \subseteq E^a \subseteq E$.

2.20. Construiu explícitament els cossos finits $\mathbb{F}_8$ i $\mathbb{F}_{16}$. Per a cadascun d'ells doneu un element primitiu sobre el seu cos primer $\mathbb{F}_2$.

2.21. Doneu dues construccions diferents del cos $\mathbb{F}_9$ com a extensió de $\mathbb{F}_3$. Establiu un isomorfisme entre elles.

2.22. Estudieu els cossos que s'obtenen en fer el quocient de l'anell $\mathbb{Z}[i]$ per un ideal maximal. Recordeu que aquest anell és principal i que els seus primers no nuls, llevat d'unitats, són els següents:

- els nombres primers $q \equiv 3 \pmod 4$;
- els elements $a + bi$ amb $a^2 + b^2$ un primer $p \equiv 1 \pmod 4$; i
- l'element $1 + i$.

2.23. Per a quins cossos finits $\mathbb{F}_q$ existeixen polinomis irreductibles de la forma $X^3 - a$ a l'anell $\mathbb{F}_q[X]$?

2.24. Determineu els cossos finits $\mathbb{F}_q$ en els quals el polinomi $X^2 + X + 1$ és primer.

2.25. Quins polinomis primers de $\mathbb{F}_5[X]$ segueixen sent primers a $\mathbb{F}_{25}[X]$?

2.26. Caracteritzeu els cossos finits per als quals la inclusió entre els seus subcossos és un ordre total: donats dos subcossos qualsevol sempre un dels dos està contingut a l'altre.

2.27. Sigui $\mathbb{F}_q$ un cos finit de característica $\neq 2$. Demostreu que un element $a \in \mathbb{F}_q^*$ té arrel quadrada a $\mathbb{F}_q$ si, i només si, $a^{(q-1)/2} = 1$. Quins elements tenen arrel quadrada a un cos finit de característica 2?

2.28. Sigui $P(X) \in \mathbb{F}_q[X]$ un polinomi irreductible a coeficients en un cos finit. Demostreu que $P(X)$ descompon completament en tota extensió $E/\mathbb{F}_q$ que contingui alguna arrel de $P(X)$.

2.29. Considerem el cos $K = \mathbb{F}_p(S,T)$ de les fraccions polinòmiques en les variables S, T amb coeficients en el cos finit $\mathbb{F}_p$.

a) Demostreu que els polinomis $f(X) = X^p - S, g(X) = X^p - T \in K[X]$ són irreductibles.

b) Siguin $\alpha = \sqrt[p]{S}, \beta = \sqrt[p]{T}$ respectivament arrels de $f(X)$ i $g(X)$ en K_{fg}. Demostreu que $[K(\alpha,\beta) : K] = p^2$.

c) Proveu que tot $\gamma \in K(\alpha,\beta)$ satisfà $\gamma^p \in K$.

d) Concloeu que l'extensió $K(\alpha,\beta)/K$ no admet cap element primitiu.