ESTRUCTURES ALGEBRAIQUES

EXAMEN PARCIAL

5 de novembre 2020

1. Sigui $A = \mathbb{Z}[\sqrt{2}]$, i siguin $p \in \mathbb{Z}$ un nombre primer senar i $a \in \mathbb{Z}$ tal que $a^2 \equiv 2 \pmod{p}$.

a) *(0.25 pts)* Doneu un exemple concret de p i a que satisfacin aquesta condició.

b) *(1 pt)* Definiu dos morfismes d'anells d'A en $\mathbb{Z}/p\mathbb{Z}$.

c) *(0.75 pts)* Demostreu que els nuclis dels morfismes anteriors són ideals maximals d'A.

d) *(0.5 pts)* Tenim dos ideals $\mathfrak{m}_1, \mathfrak{m}_2$ d'A tals que $A/\mathfrak{m}_1$ i $A/\mathfrak{m}_2$ són isomorfs. És cert que $\mathfrak{m}_1 = \mathfrak{m}_2$?

e) *(0.5 pts)* Suposem ara que el polinomi $X^2 - 2$ és irreductible a $\mathbb{Z}/p\mathbb{Z}[X]$. És possible definir un morfisme d'A en $\mathbb{Z}/p\mathbb{Z}$?

Solució:

a) 2 no és quadrat ni mòdul 3 ni mòdul 5. En canvi, mòdul 7 tenim $3^2 = 9 \equiv 2 \mod 7$. Per tant, $a = 3$ i $p = 7$ compleixen les condicions.

b) Si φ és morfismes d'anells $A \to \mathbb{Z}/p\mathbb{Z}$, aleshores $\varphi(\sqrt{2})^2 = \varphi(2)$.
Definim $\varphi_1(x + y\sqrt{2}) = \overline{x} + \overline{y}\,\overline{a} = \overline{x + ya}$ i $\varphi_2(x + y\sqrt{2}) = \overline{x} - \overline{y}\,\overline{a} = \overline{x - ya}$, on $\overline{x}$ indica la classe mòdul p. Aleshores,

$$\varphi_i((x + y\sqrt{2}) + (z + t\sqrt{2})) = \varphi_i(x + z + (y + t)\sqrt{2}) = \overline{x + z} \pm (\overline{y + t})\overline{a} = \overline{x} \pm \overline{y}\,\overline{a} + \overline{z} \pm \overline{t}\overline{a}$$

i, per tant, $\varphi_i((x + y\sqrt{2}) + (z + t\sqrt{2})) = \varphi_i(x + y\sqrt{2}) + \varphi_i(z + t\sqrt{2})$. Pel que fa al producte,

$$\varphi_i((x+y\sqrt{2})(z+t\sqrt{2})) = \varphi_i(xz+2yt+(yz+xt)\sqrt{2}) = \overline{xz + 2yt} \pm (\overline{yz + xt})\overline{a} = (\overline{x} \pm \overline{ya})(\overline{z} \pm \overline{t}\overline{a})$$

i, per tant, $\varphi_i((x + y\sqrt{2})(z + t\sqrt{2})) = \varphi_i(x + y\sqrt{2})\varphi_i(z + t\sqrt{2})$. Finalment, és clar que $\varphi_i(1) = \overline{1}$.

c) Clarament, els dos morfismes anteriors són epimorfismes: $\varphi_i(x) = \overline{x}$ per a tot $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$. Sabem que els nuclis de morfismes són ideals i que $A/\ker\varphi_i \simeq \mathrm{Im}\varphi_i = \mathbb{Z}/p\mathbb{Z}$. Atès que el quocient és un cos, es tracta d'ideals maximals.

$$\mathfrak{m}_i = \ker\varphi_i = \{x + y\sqrt{2} \mid \overline{x \pm ya} = 0\} = \{x + y\sqrt{2} \mid x = \mp ya + \lambda p,\ \lambda \in \mathbb{Z}\}$$

$$\mathfrak{m}_i = \ker\varphi_i = \{\mp ya + y\sqrt{2} + \lambda p, \quad \lambda \in \mathbb{Z}\} = \{y(\mp a + \sqrt{2}) + \lambda p, \quad \lambda \in \mathbb{Z}\}$$

d) No és cert. A l'apartat anterior hem vist que $A/\mathfrak{m}_1 \simeq \mathbb{Z}/p\mathbb{Z} \simeq A/\mathfrak{m}_2$. Però $\mathfrak{m}_1$ i $\mathfrak{m}_2$ no són iguals:

$$-a + \sqrt{2} \in \mathfrak{m}_1 = \ker\varphi_1, \quad \varphi_2(-a + \sqrt{2}) = \overline{-a - a} = \overline{-2a} \not\equiv 0 \mod p,$$

ja que p és primer senar i per tant no divideix 2 ni a. (per hipòtesi $a^2 \equiv 2$). Així doncs, $-a + \sqrt{2}$ pertany a $\mathfrak{m}_1$ però no pertany a $\mathfrak{m}_2 = \ker\varphi_2$.

e) Si $\varphi A \to \mathbb{Z}/p\mathbb{Z}$, tindrem $\varphi(0) = \overline{0}$ i $\varphi(1) = \overline{1}$. D'això es dedueix que $\varphi(-1) = -\overline{1} = \overline{-1}$ i que $\varphi(x) = \overline{x}$ per a tot $x \in \mathbb{Z}$. Així, si posem $\alpha = \varphi(\sqrt{2})$ tindrem $\alpha^2 = \varphi(2) = \overline{2}$. És a dir, $\alpha \in \mathbb{Z}/p\mathbb{Z}$ ha de ser una arrel de $X^2 - 2 \in \mathbb{Z}/p\mathbb{Z}[X]$. Si el polinomi és irreductible no tindrà arrels i no és possible definir cap morfisme.

2. Sigui K un cos i sigui $A = \{f(X) \in K[X] \mid f'(0) = 0\}$.

a) *(0.5 pts)* Demostreu que A és un subanell de $K[X]$ i determineu el conjunt A^* de les seves unitats.

b) *(0.5 pts)* Demostreu que X^3 és un element irreductible de A.

c) *(1 pt)* Demostreu que A no és factorial.

d) *(0.5 pts)* Trobeu un ideal d'A que no sigui principal.

e) *(0.5 pts)* És euclidià?

Solució:

a) Comprovem que A és un subanell de $K[X]$:

- És clar que $1 \in A$.
- Si $f, g \in A$, llavors $(f+g)'(0) = f'(0) + g'(0) = 0$, i per tant $f - g \in A$.
- Si $f, g \in A$, llavors $(fg)'(0) = f(0)g'(0) + f'(0)g(0) = 0$, i per tant $fg \in A$.

Observem que $K \subseteq A$, ja que les constants tenen derivada zero. Així, si $u \in K^* \subseteq A$ llavors $u^{-1} \in K^* \subseteq A$, i per tant $K^* \subseteq A^*$. L'altra inclusió també és certa: si f és invertible en A, llavors també seria invertible en $K[X]$, però $K[X]^* = K^*$, i per tant $f \in K^*$.

En conclusió, $A^* = K^*$.

b) Abans de tot, observem que si $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ és un element de $K[X]$, la condició $f'(0) = 0$ equival a $a_1 = 0$. En particular, A no conté cap polinomi de grau 1.

Suposem que $X^3 = fg$, amb $f, g \in A \setminus A^*$. D'una banda, sabem que $\deg f + \deg g = 3$, i de l'altra no pot ser que ni f ni g tinguin grau 0, ja que llavors serien invertibles (per l'apartat anterior). Llavors, un dels dos polinomis ha de tenir grau 2 i l'altre grau 1, però això és impossible ja que A no conté polinomis de grau 1. Per tant, X^3 és irreductible en A.

c) Demostrarem que A no és factorial trobant dues descomposicions diferents de X^6 com a producte d'irreductibles. A l'apartat anterior hem vist que X^3 és irreductible, i per un argument anàleg es pot demostrar que X^2 també ho és. Però $X^6 = (X^3)^2 = (X^2)^3$, que són dues descomposicions diferents ja que tenen un nombre diferent de factors irreductibles. Per tant, A no és factorial.

d) L'ideal $I = (X^2, X^3)$ de A no és principal. Suposem que existeix $f \in A$ tal que $I = (f)$. Com que $X^2 = fg$ per a cert $g \in A$, el polinomi f ha de tenir grau 0 o grau 2. Observem que f no pot ser constant, ja que els elements de I són de la forma $uX^2 + vX^3$, i per tant tenen terme constant nul. En conseqüència, f ha de tenir grau 2. Llavors, si $X^3 = fh$ per a cert $h \in A$, necessàriament h tindria grau 1, una contradicció.

e) Tot anell euclidià és principal i factorial. Per tant, A no pot ser euclidià.

3. Considereu els cossos $K = \mathbb{Q}(\sqrt[3]{5})$, $L = \mathbb{Q}(\sqrt[5]{3})$, $M = KL$.

a) *(0.5 pts)* Calculeu els graus de les extensions M/K, M/L i $M/\mathbb{Q}$.

b) *(0.5 pts)* Construiu una $\mathbb{Q}$-base de M a partir d'una $\mathbb{Q}$-base de K i una $\mathbb{Q}$-base de L.

c) *(1 pt)* Sigui $\alpha \in L$, i sigui R_α la seva representació matricial en la $\mathbb{Q}$-base de M de l'apartat anterior. Demostreu que el polinomi característic de R_α és el cub d'un polinomi.

d) *(1 pt)* Demostreu que per $\gamma \in M$ és un element primitiu $M = \mathbb{Q}(\gamma)$ si, i només si, la seva representació matricial en qualsevol $\mathbb{Q}$-base de M té polinomi característic irreductible.

Solució:

a) Els polinomis $X^3 - 5$ i $X^5 - 3$ són irreductibles sobre $\mathbb{Q}$ (per exemple, pel criteri d'Eisenstein), la qual cosa ens diu que $[K : \mathbb{Q}] = 3$ i $[L : \mathbb{Q}] = 5$. Atès que

$$[M : \mathbb{Q}] = [M : K][K : \mathbb{Q}] = [M : L][L : \mathbb{Q}]$$

i que 3 i 5 són coprimers, tenim que $15 \mid [M : \mathbb{Q}]$. Per altra banda, $M = L(\sqrt[3]{5})$ i per això $[M : L] \leq 3$ i, per tant, $[M : \mathbb{Q}] = 15$. D'aquí deduim que $[M : L] = 3$ i $[M : K] = 5$.

b) Siguin $\gamma = \sqrt[3]{5}, \delta = \sqrt[5]{3}$. Una $\mathbb{Q}$-base de K és $B_K = \{1, \gamma, \gamma^2\}$ i una $\mathbb{Q}$-base de L és $B_L = \{1, \delta, \delta^2, \delta^3, \delta^4\}$. A partir d'aquí es dedueix fàcilment que $B_M = \{\gamma^i \delta^j\}_{i,j}$ és una $\mathbb{Q}$-base de M.

c) Denotem per T_α la representació matricial d'α en la base B_L. La matriu R_α és diagonal per blocs, amb 3 còpies de T_α a la diagonal. Això ens diu que el polinomi característic de R_α és el cub del polinomi característic de T_α.

d) Recordem que el polinomi mínim de R_α coincideix amb $f(X) = \mathrm{Irr}(\alpha, \mathbb{Q}, x)$. Si el polinomi característic de R_α és irreductible, coincidirà amb el polinomi mínim, i en particular $\deg f = 15$ i $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 15$, $M = \mathbb{Q}(\alpha)$.

Recíprocament, si $M = \mathbb{Q}(\alpha)$, llavors el grau del polinomi mínim de R_α és 15, i per tant coincideix amb el polinomí característic, que en particular és irreductible.

4. *(1 pt)* Demostreu que tot anell euclidià és principal.