423 TEXTOS DOCENTS

EQUACIONS ALGEBRAIQUES: 274 EXERCICIS RESOLTS

Olga Lavila Vidal

Departament de Matemàtiques i Informàtica

UNIVERSITAT DE BARCELONA

EQUACIONS ALGEBRAIQUES: 274 EXERCICIS RESOLTS

Olga Lavila Vidal

Departament de Matemàtiques
i Informàtica

423 TEXTOS DOCENTS

Universitat de Barcelona
Edicions

Índex

PRÒLEG

En aquest text docent es presenten una col·lecció d'exercicis resolts de l'assignatura Equacions Algebraiques, del grau de Matemàtiques de la Facultat de Matemàtiques i Informàtica de la Universitat de Barcelona, alguns dels quals s'utilitzen en les classes de problemes i en els laboratoris de l'assignatura. L'origen dels problemes d'aquest llibre és molt divers. Alguns són originals de l'autora o de la resta de professors que han fet la docència d'aquesta assignatura al llarg dels anys, d'altres provenen de llibres sobre la matèria i alguns s'han fet servir en exàmens de l'assignatura.

Els exercicis estan resolts detalladament i la teoria de l'assignatura hi està inclosa, la major part en forma d'exercicis de dificultat progressiva, la resta enunciada amb referències a llibres on pot trobar-se'n la demostració. El programa actual de l'assignatura comprèn tres hores de teoria, una de problemes i una de laboratoris per setmana, al llarg d'un semestre. Les classes de problemes i laboratoris tenen la finalitat principal d'ajudar a la comprensió de la teoria, aplicant-la a la resolució de problemes. Alguns d'aquests problemes que es treballen a classe són extensos; per això, molts d'aquests exercicis només es poden resoldre de manera parcial a classe i d'altres no es poden fer perquè el temps és molt limitat. L'objectiu d'aquest text docent és, doncs, proporcionar a l'estudiant una eina de consulta i de treball que li permeti completar de manera autònoma els exercicis. Així com actualment hi ha una gran varietat de llibres teòrics sobre equacions algebraiques i teoria de Galois, és més difícil trobar llibres amb problemes resolts de l'assignatura.

La col·lecció de problemes cobreix tot el temari de l'assignatura i amplia el focus a resultats que estenen els de l'assignatura. En començar el curs, se suposa que l'estudiant té coneixements d'espais vectorials, adquirits en l'assignatura Àlgebra Lineal, així com d'anells, cossos i grups, adquirits en l'assignatura Estructures Algebraiques. El text consta de quinze capítols, al principi de cadascun dels quals es recorden les definicions i els resultats teòrics necessaris per resoldre els 274 exercicis proposats.

Molts dels membres de la Facultat de Matemàtiques i Informàtica han col·laborat al llarg del temps en la docència de l'assignatura i han participat tant en el desenvolupament dels programes en el context dels diferents plans d'estudis com en la preparació de les llistes d'exercicis. A tots ells, vull expressar-los el meu agraïment.

Santa Coloma de Queralt, 2019

Capítol 1

IRREDUCTIBILITAT

Exercici 1.1

Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$, *un polinomi. Proveu que si* $\alpha = \frac{p}{q}$, *amb* $p, q \in \mathbb{Z}$, $(p,q) = 1$, *és una arrel racional de* f, *aleshores* $p|a_0$ *i* $q|a_n$.

Solució

Sigui $\alpha = \frac{p}{q}$, amb $p, q \in \mathbb{Z}$, $(p,q) = 1$, una arrel racional de f. Aleshores $f(\alpha) = 0$, és a dir:

$$a_0 + a_1\left(\frac{p}{q}\right) + \cdots + a_n\left(\frac{p}{q}\right)^n = 0.$$

Multiplicant aquesta expressió per q^n tenim una igualtat en l'anell dels enters:

$$a_0q^n + a_1pq^{n-1} + \cdots + a_{n-1}p^{n-1}q + a_np^n = 0.$$

Ara tenim que

$$-a_0q^n = a_1pq^{n-1} + \cdots + a_{n-1}p^{n-1}q + a_np^n$$

i, per tant, p divideix a_0q^n. Com que $(p,q) = 1$, deduïm que $p|a_0$. De manera semblant,

$$a_np^n = -a_0q^n - a_1pq^{n-1} - \cdots - a_{n-1}p^{n-1}q$$

i, per tant, q divideix a_np^n. Com que $(p,q) = 1$, deduïm que $q|a_n$.

Exercici 1.2

Proveu que $X^4 + 4$ *no té arrels racionals però factoritza en* $\mathbb{Q}[X]$.

Solució

Una arrel del polinomi $X^4 + 4$ és $\sqrt[4]{-4} = \sqrt[4]{4e^{i\pi}} = \sqrt{2}e^{\frac{\pi i}{4}} = 1 + i$ i, per tant, les arrels són $\pm(1+i)$ i $\pm(1+i)i = \pm(-1+i)$, cap d'elles racional. En canvi, podem factoritzar el polinomi en $\mathbb{Q}[X]$ de la manera següent:

$$X^4 + 4 = (X-(1+i))(X-(1-i))(X-(-1+i))(X-(-1-i)) = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

Exercici 1.3

Proveu que els polinomis no primitius de $\mathbb{Z}[X]$ *redueixen en* $\mathbb{Z}[X]$.

Solució

Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$, un polinomi no primitiu. Aleshores $c = \text{cont} f = \text{mcd}(a_0, \ldots, a_n) \neq \pm 1$. Per a $i = 0, \ldots, n$, escrivim $a_i = c\, b_i$ per a $b_i \in \mathbb{Z}$ convenients. Aleshores $f(X) = c(b_0 + b_1X + \cdots + b_nX^n)$ és una factorització de f en polinomis no invertibles en $\mathbb{Z}[X]$ i, per tant, $f(X)$ redueix en $\mathbb{Z}[X]$.

Exercici 1.4

Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_0, \ldots, a_n \in \mathbb{Z}$, un polinomi. Suposem que existeix $p \in \mathbb{Z}$ primer tal que

$$p | a_i,\ i = 0, \ldots, n-1, \quad p \nmid a_n, \quad p^2 \nmid a_0.$$

Demostreu que f és irreductible en $\mathbb{Q}[X]$. Si, a més a més, f és primitiu, aleshores també és irreductible en $\mathbb{Z}[X]$.

Solució

Suposem que $f(X)$ redueix en $\mathbb{Q}[X]$. Aleshores podem escriure $f(X) = p(X)q(X)$ per a certs $p(X), q(X) \in \mathbb{Q}[X]$, $p(X), q(X) \notin \mathbb{Q}[X]^* = \mathbb{Q}^*$; és a dir, $\text{gr}(p(X)) \geq 1$ i $\text{gr}(q(X)) \geq 1$. Escrivim ara $p(X) = \frac{a}{b} p_1(X)$ i $q(X) = \frac{c}{d} q_1(X)$ amb $a, b, c, d \in \mathbb{Z}$, $p_1(X), q_1(X) \in \mathbb{Z}[X]$ polinomis primitius. Aleshores tenim:

$$f(X) = \frac{a\,c}{b\,d} p_1(X) q_1(X)$$

i, per tant, tenim la igualtat

$$b\,d\, f(X) = a\,c\; p_1(X) q_1(X)$$

en $\mathbb{Z}[X]$ i, utilitzant el lema de Gauss, tenim:

$$b\,d\, \text{cont}(f(X)) = \text{cont}(b\,d\, f(X)) = \text{cont}(a\,c\; p_1(X) q_1(X)) = a\,c\,.$$

Per tant, $\text{cont} f = \frac{ac}{bd}$ i, en particular, $\frac{ac}{bd} = r \in \mathbb{Z}$ i tenim que $f(X) = r\, p_1(X) q_1(X)$ factoritza en $\mathbb{Z}[X]$. Així doncs, hem vist que si $f(X)$ redueix en $\mathbb{Q}[X]$, també ho fa en $\mathbb{Z}[X]$. Aleshores $\frac{1}{r} f(X) \in \mathbb{Z}[X]$ és un polinomi primitiu i els coeficients d'aquest polinomi segueixen complint la hipòtesi.

Considerant, doncs, $f(X) \in \mathbb{Z}[X]$ polinomi primitiu que satisfà les hipòtesis de l'enunciat, volem veure que no pot factoritzar com a producte de dos polinomis amb coeficients en $\mathbb{Z}$ de grau més gran o igual que 1. Suposem

$$a_0 + a_1X + \cdots + a_nX^n = (b_0 + b_1X + \cdots + b_mX^m)(c_0 + c_1X + \cdots + c_lX^l),$$

amb $b_i, c_i \in \mathbb{Z}$, $b_m \neq 0$, $c_l \neq 0$, $l, m \geq 1$. Com que $p | a_0 = b_0 c_0$, tenim que $p | b_0$ o $p | c_0$. Sense pèrdua de generalitat, podem suposar que $p | b_0$. Aleshores, com que $p^2 \nmid a_0$, tenim també que $p \nmid c_0$. Si $p | b_m$, tindríem que $p | a_n$, que és absurd. Sigui, doncs, $k \leq m$, tal que $p \nmid b_k$ i $p | b_i$, $\forall i < k$. Aleshores $a_k = b_0 c_k + \cdots + b_{k-1} c_1 + b_k c_0$ i tenim $b_k c_0 = a_k - b_0 c_k - \cdots - b_{k-1} c_1$.

Com que $k \leq m < n$, tenim que $p|a_k$ i també $p|b_i$, per a $i = 0, \ldots, k-1$ i, per tant, tenim que p ha de dividir $b_k c_0$, que és absurd.

Una altra manera de provar-ho és la següent. Considerem el morfisme d'anells

$$\begin{aligned} \pi\colon \mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ b &\mapsto \pi(b) = \overline{b} \end{aligned}$$

i l'estenem a un morfisme d'anells de $\mathbb{Z}[X]$ en $\mathbb{Z}/p\mathbb{Z}[X]$:

$$\begin{aligned} \tilde{\pi}\colon \mathbb{Z}[X] &\longrightarrow \mathbb{Z}/p\mathbb{Z}[X] \\ \sum_{i=0}^{n} b_i X^i &\mapsto \sum_{i=0}^{n} \pi(b_i) X^i. \end{aligned}$$

Com que p és primer, tenim que $\mathbb{Z}/p\mathbb{Z}$ és un cos i, per tant, $\mathbb{Z}/p\mathbb{Z}[X]$ és un domini de factorització única. Observem que $\tilde{\pi}(f) = \overline{a_n} X^n$, ja que $p|a_i, \forall\, i = 0, \ldots, n-1$, i $p \nmid a_n$. Suposem ara que $f(X)$ redueix en $\mathbb{Q}[X]$. Aleshores, com hem vist abans, també redueix en $\mathbb{Z}[X]$ i podem escriure $f(X) = g(X)\,h(X)$ per a certs $g(X), h(X) \in \mathbb{Z}[X]$. Aplicant-hi el morfisme $\tilde{\pi}$, tenim:

$$\overline{a_n} X^n = \tilde{\pi}(f(X)) = \tilde{\pi}(g(X)\,h(X)) = \tilde{\pi}(g(X))\,\tilde{\pi}(h(X))$$

i, tenint en compte que $\mathbb{Z}/p\mathbb{Z}[X]$ és un domini de factorització única, tenim que $\tilde{\pi}(g(X)) = \alpha X^m$ i $\tilde{\pi}(h(X)) = \beta X^{n-m}$, per a certs $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$.

Si $m \geq 1$ i $n-m \geq 1$, $\tilde{\pi}(g(X))$ i $\tilde{\pi}(h(X))$ no tenen terme independent i, per tant, tenim que $p|g(0)$ i $p|h(0)$, cosa que implica que $p^2|g(0)h(0) = f(0) = a_0$, que és una contradicció amb la hipòtesi. Per tant, $m = 0$ o $n - m = 0$, d'on tenim que $\mathrm{gr}(\tilde{\pi}(g(X))) = 0$ o $\mathrm{gr}(\tilde{\pi}(h(X))) = 0$. Però, com que $p \nmid a_n$, tenim que $\mathrm{gr}(\tilde{\pi}(g(X))) = \mathrm{gr}(g(X))$ i $\mathrm{gr}(\tilde{\pi}(h(X))) = \mathrm{gr}(h(X))$ i, per tant, deduïm que $g(X) = c \in \mathbb{Z}$ o $h(X) = c \in \mathbb{Z}$. Per tant, $f(X)$ és irreductible en $\mathbb{Q}[X]$. Si, a més a més, $f(X)$ és primitiu, tenim que $g(X) = \pm 1$ o $h(X) = \pm 1$ i, per tant, $f(X)$ és també irreductible en $\mathbb{Z}[X]$.

Exercici 1.5 (criteri d'Eisenstein)

Siguin $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$, $a_0, \ldots, a_n \in A$, un polinomi, A un domini de factorització única i K el seu cos de fraccions. Suposem que existeix $p \in A$ primer tal que

$$p|a_i,\ i = 0, \ldots, n-1, \quad p \nmid a_n, \quad p^2 \nmid a_0.$$

Demostreu que f és irreductible en $K[X]$. Si, a més a més, f és primitiu, aleshores també és irreductible en $A[X]$.

Solució

Podem repetir els dos arguments de l'exercici anterior. Només comentem el segon argument perquè cal fer un petit matís. Sigui $f(X) \in A[X]$ un polinomi que compleix les hipòtesis de l'enunciat per a un cert $p \in A$ primer. Suposem que $f(X)$ no és irreductible en $K[X]$. Siguin $g(X), h(X) \in K[X]$ polinomis no constants tals que $f(X) = g(X)h(X)$, $\mathrm{gr}(g(X)) = m > 0$, $\mathrm{gr}(h(X)) = n - m > 0$, els quals podem multiplicar per constants adequades per tal que els

seus coeficients siguin de A. Considerem ara el morfisme d'anells

$$\begin{aligned}\pi\colon A &\to A/(p)\\ b &\mapsto \pi(b)=\overline{b}\end{aligned}$$

i l'estenem a un morfisme d'anells de $A[X]$ en $A/(p)[X]$:

$$\begin{aligned}\tilde{\pi}\colon A[X] &\longrightarrow A/(p)[X]\\ f(X)=\sum_{i=0}^{n} b_i X^i &\mapsto \overline{f}(X)=\sum_{i=0}^{n}\pi(b_i)X^i.\end{aligned}$$

El problema en aquest cas és que no podem assegurar que $A/(p)[X]$ sigui un domini de factorització única. Com que $A/(p)$ és íntegre, existeix $K := Q(A/(p))$, el cos de fraccions de $A/(p)$. Aleshores podem pensar que $\tilde{\pi}(f(X)) \in K[X]$ i $K[X]$ és un domini de factorització única. De la igualtat $f(X) = g(X)h(X)$, aplicant $\tilde{\pi}$, tenim que $\overline{a_n}X^n = \overline{f}(X) = \overline{g}(X)\overline{h}(X)$ i $\mathrm{gr}(\overline{g}(X)) = \mathrm{gr}(g(X)) = m > 0$, $\mathrm{gr}(\overline{h}(X)) = \mathrm{gr}(h(X)) = n-m > 0$. Emprant que $K[X]$ és un domini de factorització única, existeixen $b, c \in A/pA$ no nuls tals que $\overline{g}(X) = bX^m$, $\overline{h}(X) = cX^{n-m}$. En particular, els termes independents dels polinomis $g(X)$ i $h(X)$ són divisibles per p. Això vol dir que el terme independent de $f(X)$, el coeficient a_0, és divisible per p^2 i arribem a una contradicció amb les hipòtesis de l'enunciat. Per tant, $f(X)$ és irreductible en $K[X]$.

Exercici 1.6

Siguin A i B dominis i $f : A \longrightarrow B$ un morfisme d'anells. Denotem per $\widetilde{f} : A[X] \longrightarrow B[X]$ el morfisme d'anells donat per

$$\widetilde{f}\left(\sum_i a_i X^i\right) = \sum_i f(a_i)X^i, \qquad a_i \in A.$$

a) *Suposem que A és un domini de factorització única. Demostreu que si $p(X) \in A[X]$ és un polinomi primitiu, i $\widetilde{f}(p(X)) \in B[X]$ és irreductible i del mateix grau que $p(X) \in A[X]$, aleshores $p(X)$ és irreductible en $A[X]$.*

b) *Suposem que $f : A \longrightarrow B$ és un isomorfisme d'anells. Demostreu que $p(X) \in A[X]$ és irreductible si, i només si, $\widetilde{f}(p(X)) \in B[X]$ és irreductible.*

c) *Donat $a \in A$, el polinomi $p(X) \in A[X]$ és irreductible si, i només si, $p(X+a)$ és irreductible.*

d) *Proveu que $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ és irreductible en $\mathbb{Q}[X]$ i en $\mathbb{Z}[X]$.*

e) *És cert que, per a qualsevol n, $X^n + X^{n-1} + \cdots + X + 1$ és irreductible en $\mathbb{Q}[X]$ i en $\mathbb{Z}[X]$? Si és cert, proveu-ho. Altrament, intenteu esbrinar per a quins valors de n és cert.*

Solució

a) Suposem que $p(X)$ redueix en $A[X]$. Aleshores $p(X) = q(X)r(X)$, amb $q(X), r(X) \in A[X]$, $q(X), r(X) \notin A[X]^*$. Com que A és íntegre, $A[X]^* = A^*$. Com que $p(X)$ és primitiu, tenim que $q(X), r(X) \notin A$ i, per tant, $\mathrm{gr}(q(X)) = m \geq 1$ i $\mathrm{gr}(r(X)) = k \geq 1$ i $m + k = n = \mathrm{gr}(p(X))$. Aleshores $\widetilde{f}(p(X)) = \widetilde{f}(q(X)r(X)) = \widetilde{f}(q(X))\widetilde{f}(r(X))$ i

$$n = \operatorname{gr}(\widetilde{f}(p(X))) = \operatorname{gr}(\widetilde{f}(q(X))) + \operatorname{gr}(\widetilde{f}(r(X))) \leq m + k = n,$$

d'on deduïm que la desigualtat és en realitat una igualtat i, per tant, $\operatorname{gr}(\widetilde{f}(q(X))) = m \geq 1$ i $\operatorname{gr}(\widetilde{f}(r(X))) = k \geq 1$ i, per tant, $\widetilde{f}(p(X))$ redueix en $B[X]$.

b) Observem que no podem utilitzar l'apartat anterior perquè no sabem que A sigui un domini de factorització única.

Adonem-nos també que si f és un isomorfisme, també ho és $\widetilde{f}$ i $\widetilde{f}^{-1} = \widetilde{f^{-1}}$.

Provarem un resultat més general. Siguin A i B dominis, $\varphi : A[X] \longrightarrow B[X]$ un isomorfisme, i $p(X) \in A[X]$. Aleshores $p(X)$ és irreductible en $A[X]$ si, i només si, $\varphi(p(X))$ és irreductible en $B[X]$.

Suposem primer que $\varphi(p(X))$ és irreductible en $B[X]$. Volem provar que $p(X)$ és irreductible en $A[X]$. Suposem que $p(X) = q(X)r(X)$, amb $q(X), r(X) \in A[X]$. Aleshores, aplicant el morfisme φ a aquesta igualtat, tenim que $\varphi(p(X)) = \varphi(q(X)r(X)) = \varphi(q(X))\varphi(r(X))$, i, per tant, $\varphi(q(X)) \in B[X]^* = B^*$ o $\varphi(r(X)) \in B[X]^* = B^*$. Sense pèrdua de generalitat, podem suposar que $\varphi(q(X)) = b \in B$ i existeix $c \in B$ tal que $\varphi(q(X))c = 1$. Aplicant φ^{-1} a aquesta igualtat, tenim que $q(X)\varphi^{-1}(c) = 1$ i, per tant, $q(X) \in A^*$. El recíproc ja està provat considerant que φ^{-1} és un isomorfisme.

c) Observem que el morfisme d'anells $\varphi : A[X] \longrightarrow A[X]$ definit per $\varphi(p(X)) = p(X+a)$ és un isomorfisme i que $\varphi^{-1}(p(X) = p(X-a)$. Per tant, el resultat es desprèn del resultat provat en l'apartat anterior.

d) El polinomi $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ es pot escriure com $f(X) = \dfrac{X^7-1}{X-1}$. Observem:

$$f(X+1) = \frac{(X+1)^7 - 1}{X} = X^6 + 7X^5 + 21X^4 + 35X^3 + 35X^2 + 21X + 7,$$

que és 7-Eisenstein i, per tant, $f(X+1)$ és irreductible en $\mathbb{Q}[X]$. Segons l'apartat anterior, $f(X)$ és irreductible en $\mathbb{Q}[X]$ i, com que és primitiu, també és irreductible en $\mathbb{Z}[X]$.

e) Com en l'apartat anterior, escrivim $f(X) = X^n + X^{n-1} + \cdots + X + 1 = \frac{X^{n+1}-1}{X-1}$ i intentarem repetir-ne el procediment. Tenim que

$$\begin{aligned} f(X+1) = \frac{(X+1)^{n+1}-1}{X} &= \frac{1}{X}\sum_{i=1}^{n+1}\binom{n+1}{i}X^i \\ &= X^n + (n+1)X^{n-1} + \binom{n+1}{n-1}X^{n-2} + \cdots + \binom{n+1}{2}X + (n+1). \end{aligned}$$

Observem que si $n+1 = p$ és un nombre primer, aleshores $\binom{p}{i}$ és múltiple de p per a qualsevol $i = 1, \ldots, n$ i $p^2 \nmid \binom{p}{1}$, i, per tant, aplicant p-Eisenstein tenim que $f(X+1)$ és irreductible en $\mathbb{Q}[X]$. Aleshores $f(X)$ és irreductible en $\mathbb{Q}[X]$ i, com que és primitiu, també és irreductible en $\mathbb{Z}[X]$.

Si $n+1$ no és un nombre primer, sigui q qualsevol primer tal que $q|n+1$. Aleshores totes les arrels de $X^q - 1$ són arrels q-èsimes de la unitat i, per tant, també arrels $n+1$-èsimes. Per tant, $X^q - 1$ divideix $X^{n+1} - 1$ o, equivalentment, $X^{n+1} - 1 = (X^q - 1)g(X)$ en $\mathbb{Q}[X]$. Aleshores

$$f(X)=\frac{X^{n+1}-1}{X-1}=\frac{X^q-1}{X-1}g(X)$$

i, per tant, $f(X)$ redueix en $\mathbb{Q}[X]$ i, per tant, també en $\mathbb{Z}[X]$.

Nota 1.1. *Hem vist en l'exercici 1.6e que el polinomi $X^n+X^{n-1}+\cdots+X+1$ és irreductible en $\mathbb{Q}[X]$ si, i només si, $n+1$ és un nombre primer. Donat un nombre primer $p\in\mathbb{Z}$, anomenem polinomi ciclotòmic p-èsim el polinomi $\Phi_p(X):=X^{p-1}+X^{p-2}+\cdots+X+1$.*

Nota 1.2. *La hipòtesi A domini de factorització única ens permet parlar de contingut d'un polinomi i, en particular, de polinomi primitiu. Tot i així, per a un anell A qualsevol, podem estendre la definició de polinomi primitiu a aquell els coeficients del qual generen A; és a dir, $f(X)=a_0+a_1X+\cdots+a_nX^n\in A[X]$ és primitiu si $(a_0,\ldots,a_n)=A$. Amb aquesta definició, la hipòtesi A domini de factorització única no és necessària en l'exercici 1.6a.*

Nota 1.3. *Donat un nombre primer $p\in\mathbb{Z}$, l'anell quocient $\mathbb{Z}/p\mathbb{Z}$ és un cos. Notarem indistintament $\mathbb{Z}/p\mathbb{Z}$ o $\mathbb{F}_p$ aquest cos, que veurem que és l'únic cos de p elements llevat isomorfismes.*

Exercici 1.7 (criteri de reducció)

a) *Siguin A i B dominis d'integritat, L el cos de fraccions de B i $f:A\longrightarrow B$ un morfisme d'anells qualsevol. Anomenem també $\widetilde{f}:A[X]\longrightarrow B[X]$ el morfisme d'anells que s'obté en aplicar f als coeficients dels polinomis de $A[X]$. Sigui $p(X)\in A[X]$ un polinomi tal que $\widetilde{f}(p(X))\in B[X]$ és del mateix grau que $p(X)\in A[X]$. Llavors, si $\widetilde{f}(p(X))$ és irreductible en $L[X]$, $p(X)$ no admet cap factorització en $A[X]$ de la forma $p(X)=q(X)r(X)$, amb $q(X)$, $r(X)\in A[X]$, $\mathrm{gr}(q(X))\geq 1$ i $\mathrm{gr}(r(X))\geq 1$.*

b) *Trobeu tots els polinomis irreductibles de grau 2, 3, 4, 5 i 6 de $\mathbb{F}_2[X]$.*

c) *Demostreu que els polinomis X^2+aX+b, X^3+aX+b, X^4+aX+b i X^6+aX+b, amb a, $b\in\mathbb{Z}$ senars, són irreductibles en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$.*

d) *Trobeu noves famílies de polinomis irreductibles en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$.*

Solució

a) Suposem que $p(X)$ admet una factorització en $A[X]$ de la forma $p(X)=q(X)r(X)$, amb $q(X)$, $r(X)\in A[X]$. Aleshores $\widetilde{f}(p(X))=\widetilde{f}(q(X)r(X))=\widetilde{f}(q(X))\widetilde{f}(r(X))$, ja que $\widetilde{f}$ és un morfisme d'anells. Sabem que $\mathrm{gr}(\widetilde{f}(p(X))=\mathrm{gr}(p(X))$ i, per tant, necessàriament s'ha de complir que $\mathrm{gr}(\widetilde{f}(q(X)))=\mathrm{gr}(q(X))$ i $\mathrm{gr}(\widetilde{f}(r(X)))=\mathrm{gr}(r(X))$. Com que $\widetilde{f}(p(X))$ és irreductible en $L[X]$, tenim $\widetilde{f}(q(X))\in L[X]^*=L^*$ o bé $\widetilde{f}(r(X))\in L[X]^*=L^*$, ja que L és domini, i són, per tant, constants. Així doncs, $\mathrm{gr}(q(X))=0$ o bé $\mathrm{gr}(r(X))=0$, i ja tenim el resultat provat.

b) Els polinomis de grau 2 de $\mathbb{F}_2[X]$ són de la forma $f(X)=X^2+aX+b$, amb $a,b\in\mathbb{F}_2$, i, per tant, n'hi ha quatre: X^2+X+1, X^2+X, X^2+1 i X^2. Observem que $X^2+X=X(X+1)$, $X^2+1=(X+1)^2$ i X^2 redueixen. En canvi, X^2+X+1 no redueix perquè no té arrels en $\mathbb{F}_2$. Per tant, X^2+X+1 és l'únic polinomi irreductible de grau 2 en $\mathbb{F}_2[X]$.

Els polinomis de grau 3 de $\mathbb{F}_2[X]$ són de la forma $f(X)=X^3+aX^2+bX+c$, amb $a,b,c\in\mathbb{F}_2$, i, per tant, n'hi ha vuit. Seran irreductibles els que no tinguin arrels en $\mathbb{F}_2$. Per tant, $c=1$ i només hi pot haver un nombre senar de termes no nuls. Les úniques possibilitats són, doncs, X^3+X^2+1 i X^3+X+1.

Els polinomis de grau 4 de $\mathbb{F}_2[X]$ són de la forma $f(X) = X^4 + aX^3 + bX^2 + cX + d$, amb $a, b, c, d \in \mathbb{F}_2$, i, per tant, n'hi ha setze. Perquè 0 no sigui arrel cal que $d = 1$ i perquè 1 no sigui arrel cal que tingui un nombre senar de termes no nuls. Les úniques possibilitats són, doncs, $X^4 + X^3 + X^2 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^2 + 1$ i $X^4 + X + 1$. Que no tinguin arrels no vol dir que siguin irreductibles. Si reduïssin, però, haurien de ser producte de dos polinomis irreductibles de grau 2 en $\mathbb{F}_2[X]$. Com que l'únic polinomi irreductible de grau 2 en $\mathbb{F}_2[X]$ és $X^2 + X + 1$, tindrem que si un d'aquests polinomis redueix, ha de ser $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Per tant, $X^4 + X^3 + X^2 + X + 1$, $X^4 + X^3 + 1$ i $X^4 + X + 1$ són els únics polinomis irreductibles de grau 4 en $\mathbb{F}_2[X]$.

Repetint arguments, els únics polinomis irreductibles de grau 5 de $\mathbb{F}_2[X]$ que no tenen arrels en $\mathbb{F}_2$ són $X^5 + X^4 + X^3 + X^2 + 1$, $X^5 + X^4 + X^3 + X + 1$, $X^5 + X^4 + X^2 + X + 1$, $X^5 + X^3 + X^2 + X + 1$, $X^5 + X^4 + 1$, $X^5 + X^3 + 1$, $X^5 + X^2 + 1$ i $X^5 + X + 1$. Tampoc s'han de poder escriure com a producte d'un polinomi irreductible de grau 2 i un polinomi irreductible de grau 3 i, per tant, no són irreductibles $(X^2 + X + 1)(X^3 + X^2 + 1) = X^5 + X + 1$ i $(X^2 + X + 1)(X^3 + X + 1) = X^5 + X^4 + 1$. Per tant, hi ha només sis polinomis de grau 5 irreductibles en $\mathbb{F}_2[X]$: $X^5 + X^4 + X^3 + X^2 + 1$, $X^5 + X^4 + X^3 + X + 1$, $X^5 + X^4 + X^2 + X + 1$, $X^5 + X^3 + X^2 + X + 1$, $X^5 + X^3 + 1$ i $X^5 + X^2 + 1$.

Els polinomis irreductibles de grau 6 de $\mathbb{F}_2[X]$ no tenen arrels en $\mathbb{F}_2$ i, per tant, tenen terme independent 1, han de tenir un nombre senar de termes, i no poden ser productes de polinomis irreductibles de grau inferior trobats abans. Amb aquestes condicions només ens queden els nou següents: $X^6 + X^5 + X^4 + X^2 + 1$, $X^6 + X^5 + X^4 + X + 1$, $X^6 + X^5 + X^3 + X^2 + 1$, $X^6 + X^5 + X^2 + X + 1$, $X^6 + X^4 + X^3 + X + 1$, $X^6 + X^4 + X^2 + X + 1$, $X^6 + X^5 + 1$, $X^6 + X^3 + 1$ i $X^6 + X + 1$.

En l'exercici 9.18 trobarem una fórmula per determinar el nombre de polinomis irreductibles d'un cert grau en $\mathbb{F}_2[X]$. Podrem comprovar aleshores que no ens n'hem deixat cap.

c) Sigui $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ el morfisme definit per $\pi(n) = \overline{n}$. Prenent $p(X) = X^2 + aX + b$, amb a i b senars, tenim que $\widetilde{\pi}(p(X)) = X^2 + \overline{a}X + \overline{b} = X^2 + X + 1$ és irreductible en $\mathbb{F}_2[X]$ i del mateix grau que $p(X)$. Per tant, i tenint en compte que $p(X)$ és primitiu, $p(X)$ és irreductible en $\mathbb{Z}[X]$ i, per tant, també en $\mathbb{Q}[X]$. Amb els altres polinomis podem fer el mateix raonament, ja que $X^3 + X + 1$, $X^4 + X + 1$ i $X^6 + X + 1$ són irreductibles en $\mathbb{F}_2[X]$.

d) Per exemple, tenint en compte que el polinomi $X^5 + X^2 + 1$ és irreductible en $\mathbb{F}_2[X]$, també qualsevol polinomi de la forma $X^5 + aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Z}[X]$, amb a, b, d parells i c, e senars, és irreductible en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$. Podem trobar moltes més famílies de polinomis irreductibles en $\mathbb{Z}[X]$ amb aquest argument.

Exercici 1.8

a) *Demostreu que els polinomis* $X^4 - 10X^2 + 1$ *i* $X^4 + 1$ *són irreductibles en* $\mathbb{Z}[X]$.

b) *Demostreu que aquests polinomis factoritzen en* $\mathbb{Z}/p\mathbb{Z}[X]$ *per a tot nombre primer* p.

Solució

a) No podem aplicar el criteri d'Eisenstein per assegurar que $P(X) = X^4 - 10X^2 + 1$ sigui irreductible i la reducció mòdul 2 no serveix perquè $\overline{P}(X) = X^4 + 1 = (X + 1)^4$ redueix en $\mathbb{Z}/2\mathbb{Z}[X]$. Ho provarem directament. Les seves arrels racionals, si existeixen, dividei-

xen el terme independent. Com que en aquest cas és 1, les possibles arrels serien 1 i -1. Però $P(1) = P(-1) = -8 \neq 0$. Per tant, l'única descomposició possible de $P(X)$ és com a producte de dos polinomis de grau 2. Suposem, doncs, que

$$X^4 - 10X^2 + 1 = (\alpha X^2 + aX + b)(\beta X^2 + cX + d),$$

amb $\alpha, \beta, a, b, c, d \in \mathbb{Z}$. Com que $\alpha\beta = 1$, tenim que $\alpha = \beta = \pm 1$. Sense pèrdua de generalitat, podem suposar que $\alpha = \beta = 1$. Aleshores obtenim:

$$X^4 - 10X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a+c)X^3 + (d + ac + b)X^2 + (ad + bc)X + bd,$$

que és equivalent al sistema següent:

$$\begin{cases} a + c = 0 \\ d + ac + b = -10 \\ ad + bc = 0 \\ bd = 1. \end{cases}$$

Per tant, $c = -a$ i $b = d = \pm 1$. Si $b = d = 1$, substituint en la segona equació tenim $-a^2 = -12$, $a \in \mathbb{Z}$, i, per tant, absurd. Anàlogament, si $b = d = -1$, tenim $-a^2 = -8$, $a \in \mathbb{Z}$, i, per tant, absurd. Així doncs, el sistema no té solucions enteres i el polinomi és, en conseqüència, irreductible en $\mathbb{Z}[X]$.

Estudiem ara el polinomi $P(X) = X^4 + 1$. Observem que no podem aplicar el criteri d'Eisenstein per assegurar que sigui irreductible i la reducció mòdul 2 no serveix perquè $\overline{P}(X) = X^4 + 1$ redueix en $\mathbb{Z}/2\mathbb{Z}[X]$. Les seves arrels racionals, si existeixen, divideixen el terme independent. Com que en aquest cas és 1, les possibles arrels són ± 1. Però $P(1) = P(-1) = 2 \neq 0$. Per tant, l'única descomposició possible de $P(X)$ és com a producte de dos polinomis de grau 2. Suposem, doncs, que

$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d),$$

amb $a, b, c, d \in \mathbb{Z}$. Igualant, hem de resoldre el sistema següent:

$$\begin{cases} a + c = 0 \\ d + ac + b = 0 \\ ad + bc = 0 \\ bd = 1. \end{cases}$$

Tenim, doncs, que $c = -a$ i $b = d = \pm 1$. Substituint en la segona equació tenim $-a^2 = -b - d = -2b = \pm 2$, $a \in \mathbb{Z}$, i, per tant, absurd. Per tant, el sistema no té solucions enteres i el polinomi és, en conseqüència, irreductible en $\mathbb{Z}[X]$.

Una altra opció és tenir en compte que $P(X+1) = (X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$ és 2-Eisenstein i, per tant, irreductible en $\mathbb{Z}[X]$. Aleshores, per l'exercici 1.6 tenim que també $P(X)$ és irreductible en $\mathbb{Z}[X]$.

També podíem adonar-nos que les arrels de X^4+1 en el cos dels nombres complexos són $\pm\frac{\sqrt{2}}{2}(1+i)$ i $\pm\frac{\sqrt{2}}{2}(-1+i)$. Per tant, la factorització de $P(X)$ en irreductibles en $\mathbb{R}[X]$ és $P(X) = P_1(X)P_2(X)$, amb $P_1(X) = (X - \frac{\sqrt{2}}{2}(1+i))(X - \frac{\sqrt{2}}{2}(1-i)) = X^2 - \sqrt{2}X + 1$ i $P_2(X) =$

$(X+\frac{\sqrt{2}}{2}(1+i))(X+\frac{\sqrt{2}}{2}(1-i))=X^2+\sqrt{2}X+1$. Però $P_1(X), P_2(X)\notin\mathbb{Z}[X]$ i, per tant, $P(X)$ és irreductible en $\mathbb{Z}[X]$.

b) Volem veure si podem escriure el polinomi $P(X)=X^4-10X^2+1$ com a producte de dos polinomis en $\mathbb{Z}/p\mathbb{Z}[X]$. En el cas $p=2$, $\overline{P}(X)=X^4+1=(X+1)^4$ redueix. En el cas $p=3$, $\overline{P}(X)=X^4-X^2+1=(X^2+1)^2$. Entendrem més endavant per què hem distingit aquests dos casos. Sigui ara p un nombre primer, $p\neq 2,3$, i suposem que

$$X^4-10X^2+1=(\alpha X^2+aX+b)(\beta X^2+cX+d),$$

amb $\alpha,\beta,a,b,c,d\in\mathbb{Z}/p\mathbb{Z}$. Com que $\alpha\beta=1$, dividint els coeficients del primer polinomi per α i els del segon per β, podem suposar que $\alpha=\beta=1$. Aleshores obtenim que

$$X^4-10X^2+1=(X^2+aX+b)(X^2+cX+d)=X^4+(a+c)X^3+(d+ac+b)X^2+(ad+bc)X+bd,$$

que és equivalent al sistema següent:

$$\begin{cases} a+c=0\\ d+ac+b=-10\\ ad+bc=0\\ bd=1. \end{cases}$$

De la primera equació, $c=-a$, i substituint en la tercera equació, $0=a(d-b)$. Així doncs, $a=0$ o bé $d=b$.

Suposant que $a=0$, tenim que $bd=1$ i $d+b=-10$, d'on deduïm que $-10=b+\frac{1}{b}$ i tenim $b^2+10b+1=0$. Com que $p\neq 2$, tenim $b=-5\pm 2\sqrt{6}$ i, per tant, existeix solució en $\mathbb{Z}/p\mathbb{Z}$ si $6\in(\mathbb{Z}/p\mathbb{Z})^2$.

Suposant que $d=b$, tenim $b^2=1$ i, per tant, $b=d=\pm 1$. Aleshores $a^2=10+2b$ i, per tant, $a^2=12$ o $a^2=8$ i, per tant, existeix solució en $\mathbb{Z}/p\mathbb{Z}$ si $12\in(\mathbb{Z}/p\mathbb{Z})^2$ o $8\in(\mathbb{Z}/p\mathbb{Z})^2$, equivalentment si $3\in(\mathbb{Z}/p\mathbb{Z})^2$ o $2\in(\mathbb{Z}/p\mathbb{Z})^2$.

En resum, el sistema té solució en $\mathbb{Z}/p\mathbb{Z}$ si, i només si, 2, 3 o 6 són un quadrat de $\mathbb{Z}/p\mathbb{Z}$.

Recordem que el símbol de Legendre està definit per:

$$\left(\frac{n}{p}\right):=\begin{cases} 0, & \text{si } p\mid n\\ 1, & \text{si } n \text{ és un quadrat de } \mathbb{Z}/p\mathbb{Z}\\ -1, & \text{si } n \text{ no és un quadrat de } \mathbb{Z}/p\mathbb{Z}\end{cases}$$

i satisfà que $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Per tant, de la terna (a,b,ab), com a mínim n'hi ha un que és un quadrat de $\mathbb{Z}/p\mathbb{Z}$.

Si $2\in(\mathbb{Z}/p\mathbb{Z})^2$, aleshores el polinomi $P(X)$ factoritza de la manera següent:

$$P(X)=X^4-10X^2+1=(X^2+2\sqrt{2}X-1)(X^2-2\sqrt{2}X-1).$$

Si $3\in(\mathbb{Z}/p\mathbb{Z})^2$, aleshores el polinomi $P(X)$ factoritza de la manera següent:

$$P(X)=X^4-10X^2+1=(X^2+2\sqrt{3}X+1)(X^2-2\sqrt{3}X+1).$$

Si $2,3 \notin (\mathbb{Z}/p\mathbb{Z})^2$, $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)(-1) = 1$, ja que $p \nmid 2$ i $p \nmid 3$ perquè $p \neq 2,3$. Per tant, $6 \in (\mathbb{Z}/p\mathbb{Z})^2$ i $P(X)$ factoritza com

$$P(X) = X^4 - 10X^2 + 1 = (X^2 - 5 + 2\sqrt{6})(X^2 - 5 - 2\sqrt{6}).$$

Observem també que si $p \neq 2$, resolent la biquadrada $X^4 - 10X^2 + 1 = 0$, tenim que

$$X^2 = \frac{1}{2}(10 \pm \sqrt{96}) = 5 \pm 2\sqrt{6} = (\sqrt{2} \pm \sqrt{3})^2,$$

i, per tant, $X = \pm\sqrt{5 \pm 2\sqrt{6}} = \pm(\sqrt{2} \pm \sqrt{3})$. De manera directa podem obtenir, doncs, les factoritzacions de $P(X)$. Si $\sqrt{6} \in \mathbb{Z}/p\mathbb{Z}$, tenim que $P(X) = (X^2 - (5 + 2\sqrt{6}))(X^2 - (5 - 2\sqrt{6}))$. Si $\sqrt{2} \in \mathbb{Z}/p\mathbb{Z}$, tenim que $X \pm \sqrt{2} = \pm\sqrt{3}$ i, per tant, $(X \pm \sqrt{2})^2 = 3$ i podem factoritzar-lo com $P(X) = ((X + \sqrt{2})^2 - 3)((X - \sqrt{2})^2 - 3)$. Si $\sqrt{3} \in \mathbb{Z}/p\mathbb{Z}$, tenim que $X \pm \sqrt{3} = \pm\sqrt{2}$ i, per tant, $(X \pm \sqrt{3})^2 = 2$ i podem factoritzar-lo com $P(X) = ((X + \sqrt{3})^2 - 2)((X - \sqrt{3})^2 - 2)$.

Adonem-nos també que, emprant el símbol de Legendre, de la terna $(2,3,6)$, o bé exactament un element és un quadrat de $\mathbb{Z}/p\mathbb{Z}$ o bé ho són tots tres. Si 2 és l'únic element que és un quadrat, les arrels de $P(X)$ són $\pm(\sqrt{2} \pm \sqrt{3}) \notin \mathbb{Z}/p\mathbb{Z}$, i el mateix raonament val si 3 és l'únic quadrat. Si 6 és l'únic quadrat, tenint en compte que $(\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3}) = -1$, o bé cap de les arrels de $P(X)$ pertany a $\mathbb{Z}/p\mathbb{Z}$ o bé hi pertanyen les dues. En el segon cas, tindríem que $(\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}) = 2\sqrt{2} \in \mathbb{Z}/p\mathbb{Z}$, que és absurd. Així doncs, en aquest cas, $P(X)$ no té arrels en $\mathbb{Z}/p\mathbb{Z}$ i els polinomis de grau 2 que apareixen en les factoritzacions de $P(X)$ anteriors són irreductibles en $\mathbb{Z}/p\mathbb{Z}[X]$. En el segon cas, és a dir, si 2, 3 i 6 són quadrats, tenim que $P(X)$ té quatre arrels en $\mathbb{Z}/p\mathbb{Z}$ i, per tant, $P(X)$ factoritza com a producte de polinomis de grau 1: $P(X) = (X - \sqrt{2} - \sqrt{3})(X + \sqrt{2} + \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3})$.

Considerem ara el polinomi $P(X) = X^4 + 1$. Si $p = 2$, tenim que $\overline{P}(X) = X^4 + 1 = (X + 1)^4$. Sigui ara un nombre primer p, $p \neq 2$. Si $P(X)$ factoritzés com a producte de dos polinomis de grau 2, tindríem que

$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d),$$

amb $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$. Igualant, hem de resoldre el sistema següent:

$$\begin{cases} a + c = 0 \\ d + ac + b = 0 \\ ad + bc = 0 \\ bd = 1. \end{cases}$$

De la primera equació, deduïm que $c = -a$, i substituint en la tercera equació, $0 = a(d - b)$. Així doncs, $a = 0$ o bé $d = b$.

Si $a = 0$, tenim que $d = -b$ i, per tant, $b^2 = -1$. Per tant, $P(X)$ factoritza en $\mathbb{Z}/p\mathbb{Z}[X]$ si -1 és un quadrat de $\mathbb{Z}/p\mathbb{Z}$.

Si $d = b$, deduïm que $b^2 = 1$ i, per tant, $b = d = \pm 1$. Aleshores $a^2 = d + b = \pm 2$ i, així doncs, $P(X)$ factoritza en $\mathbb{Z}/p\mathbb{Z}[X]$ si 2 o -2 és un quadrat de $\mathbb{Z}/p\mathbb{Z}$.

En resum, el sistema té solució en $\mathbb{Z}/p\mathbb{Z}$ si, i només si, -1, 2 o -2 són un quadrat de $\mathbb{Z}/p\mathbb{Z}$.

Si $-1 \in (\mathbb{Z}/p\mathbb{Z})^2$, $P(X)$ factoritza com $P(X) = (X^2 + \sqrt{-1})(X^2 - \sqrt{-1})$.