Tema 1 (II): Anells de polinomis

Problemes de classe

1.42. Sigui $\mathbb{A}$ un anell íntegre i sigui K el seu cos de fraccions.

a) Demostreu que per a tot parell de polinomis $f, g \in \mathbb{A}[X]$ tals que el coeficient dominant de g (el coeficient de X^n amb $n = \deg g$) és una unitat de $\mathbb{A}$, existeixen polinomis únics $q, r \in \mathbb{A}[X]$ tals que $f = gq + r$ i $r = 0$ o bé $\deg r < \deg g$.

b) Concloeu que $K[X]$ és un anell euclidià.

c) Deduïu que si $g(X)$ divideix $f(X)$ a l'anell $\mathbb{K}[X]$, aleshores el quocient entre tots dos polinomis és un element de $\mathbb{A}[X]$.

1.43. Sigui $f(X) = a_0 + a_1 X + \ldots a_n X^n$ un polinomi amb coeficients en un anell qualsevol A. Demostreu que:

a) $f(X) \in A[X]^*$ si, i només si, $a_0 \in A^*$ i $a_1, \ldots, a_n$ són nilpotents.

b) $f(X)$ és nilpotent si tots els seus coeficients ho són.

c) $f(X)$ és divisor de zero si, i només si, tots els seus coeficients ho són.

1.44. Siguin $f(X), g(X) \in \mathbb{K}[X]$ polinomis amb $\gcd(f, g) = 1$. Demostreu que per a cada polinomi $h(X) \in \mathbb{K}[X]$ de grau $\deg h < \deg f + \deg g$ existeixen polinomis $u(X), v(X) \in \mathbb{K}[X]$ de graus $\deg u < \deg g$ i $\deg v < \deg f$ tals que

$$f(X)u(X) + g(X)v(X) = h(X),$$

i que aquests polinomis són únics.

1.45. Calculeu identitats de Bézout per a les parelles de polinomis següents: següents:

1. $f(X) = X^3 - 2X + 1$ i $g(X) = 2X^4 + 2X^2 - 1$ a l'anell $\mathbb{Q}[X]$.
2. $f(X) = X^2 + 2X + (1 + 2i)$ i $g(X) = X^4 + (2 - i)X^3 - 2iX^2 - (1 + 4i)X + (2 - i)$ a l'anell $\mathbb{C}[X]$.
3. $f(X) = X^5 + X^4 + X^2 + 1$ i $g(X) = X^5 + X^4 + X^3 + X^2$ a l'anell $\mathbb{Z}/2\mathbb{Z}[X]$.

1.46. Demostreu que, per a tot cos $\mathbb{K}$, l'anell $\mathbb{K}[X]$ conté infinits primers no associats.

1.47. Sigui $\mathbb{A}$ un anell íntegre. Demostreu que si $\mathbb{A}[X]$ és un domini d'ideals principals, llavors $\mathbb{A}$ és un cos.
Observació: El resultat no és cert si $\mathbb{A}$ no és un anell íntegre. En el cas general tenim:

$$A[x] \text{ principal } \iff A \simeq K_1 \cdots K_r, \text{ amb els } K_i \text{ cossos.}$$

Podeu trobar una demostració d'aquest fet a `https://math.stackexchange.com/a/361403`

1.48. Sigui $\mathbb{A}$ el subconjunt de $\mathbb{K}(X,Y)$ següent:

$$\mathbb{A} = \left\{ \frac{X^n f(X,Y) + Y g(X,Y)}{X^n} \in \mathbb{K}(X,Y) : f, g \in \mathbb{K}[X,Y], n \geq 0 \right\}.$$

1. Comproveu que $\mathbb{A}$ és un subanell de $\mathbb{K}(X,Y)$ que conté $\mathbb{K}[X,Y]$.
2. Demostreu que el producte de dos elements de $\mathbb{A} \setminus \mathbb{K}[X,Y]$ és de $\mathbb{A} \setminus \mathbb{K}[X,Y]$.
3. Trobeu $\mathbb{A}^*$.
4. Trobeu totes les descomposicions de Y en producte de dos elements de $\mathbb{A}$.
5. Demostreu que Y no descompon en producte d'irreductibles a $\mathbb{A}$.

1.49. Factoritzeu el polinomi $330X^4 + 715X^3 + 550X^2 + 220X - 165$ a $\mathbb{Z}[X]$.

1.50. Demostreu que el polinomi $X^7 + 6X^5 + 15X^4 - 9X^3 + 27X^2 + 75X + 21$ és irreductible a $\mathbb{Q}[X]$.

1.51. Demostreu que cap nombre primer té cap arrel racional.

1.52. Demostreu que el polinomi $X^3 + X^2 + 1$ és irreductible a $\mathbb{Q}[X]$, reduint-lo mòdul 5.

1.53. Factoritzeu el polinomi $X^3 - X + 5$ en els anells de polinomis $\mathbb{F}_p[X]$ per als primers $p = 2, 3, 5, 7, 11$ i 13.

1.54. Sigui $f(X) \in \mathbb{Z}[X]$ un polinomi de grau 2 amb dues arrels enteres i discriminant Δ. Sigui $p \in \mathbb{Z}$ un nombre primer. Demostreu que el polinomi reduït $\overline{f}(X) \in \mathbb{F}_p[X]$ té una arrel doble si, i només, si, $p \mid \Delta$.
Observació: El resultat és cert encara que $f(X)$ no tingui arrels enteres ni racionals. Utilitzeu-ho per determinar en quins cossos finits té arrels dobles el polinomi $x^2 + x + 1$.

1.55. Demostreu que els polinomis següents són irreductibles:

1. $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$;
2. $12345X^5 - 1234X^4 + 12345678X^3 - 1234567X^2 + 123456X - 123 \in \mathbb{Q}[X]$;
3. $1 + X + \frac{1}{2!}X^2 + \frac{1}{3!}X^3 + \cdots + \frac{1}{p!}X^p \in \mathbb{Q}[X]$ amb p un nombre primer.

Problemes complementaris

1.56. Sigui $\phi(x) \in \mathbb{Z}[X]$ un polinomi mònic no constant qualsevol. Demostreu que qualsevol polinomi $f(x) \in \mathbb{Z}[X]$ admet un desenvolupament ϕ-àdic, és a dir, una expressió:

$$f(x) = \sum_{i=1}^{n} a_i(x)\phi(x)^i,$$

amb els coeficients $a_i(x) \in \mathbb{Z}[X]$ de grau menor que el grau de $\phi(x)$.

1.57. Generalitzeu el problema anterior per veure que, fixat un element b un anell euclidià qualsevol, tot element de l'anell admet un *desenvolupament en base* b.

1.58. Doneu un algorisme que permeti factoritzar qualsevol polinomi de $\mathbb{Q}[X]$ en un nombre finit de passos observant que si $f(X) \in \mathbb{Z}[X]$ descompon com $f(X) = g(X)h(X)$ aleshores per a cada enter $a \in \mathbb{Z}$ es té $g(a) \mid f(a)$. Discutiu per què a la pràctica l'algoritme és totalment ineficient.

1.59. Trobeu tots els primers de $\mathbb{F}_2[X]$ de grau ≤ 4.