Problemes d'Estructures algebraiques

Aleix Torres i Camps

Jordi Guardia (jordi.guardia-rubies@upc.edu), Anna Rio i Santi Molina
(Martí Oller)

1 Anells

Problema 1. Sigui $d \in \mathbb{Z}$ un enter $d \equiv 1 \pmod 4$. Sigui $w = \frac{1}{2}(1+\sqrt{d}) \in \mathbb{C}$. Demostreu que el conjunt $\mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}$ és un subanell de $\mathbb{C}$.

Solució. Per demostrar el que ens demanen cal comprovar tres propietats. Veure que conté $1_{\mathbf{C}}$ i que és tancat per la resta surt de la PC, PA i PD. Per comprovar que és tancat per la multiplicació, veiem que $w^2 = \frac{1}{4}(1+\sqrt{d})^2 = [d = 4k+1] = k + \frac{1}{2}(1+\sqrt{4k+1}) = k + w$. Llavors quan multipliquem dos elements de $\mathbb{Z}[w]$ ens queda una part entera i un enter multiplicat per w, així que acaba sent un element de $\mathbb{Z}[w]$. □

Problema 2. Sigui $\zeta = e^{2\pi i/5}$ i considereu el conjunt $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 : a_i \in \mathbb{Z}\}$. Demostreu que és un subanell de $\mathbb{C}$.

Solució. Està clar que $1_{\mathbb{C}}$ pertany a $\mathbb{Z}[\zeta]$ i que és tancat per la suma. Ara, per veure que és tancat per la suma només cal notar que $\zeta^5 = 1_{\mathbb{C}}$, aleshores quan es multipliquin tots per tots, la màxima potència que surt és 4. □

Problema 3. Demostreu que, donat $\alpha \in \mathbb{Q}$, el conjunt de polinomis que s'anul·len en α és un ideal de $\mathbb{Q}[x]$.

Solució. Sigui A aquest conjunt que volem veure que és un ideal. Els seus elements són multiples de $(x-\alpha)$ o, el que és el mateix, $(x-\alpha)$ els divideix.

Ara, $\forall u, v \in A$ i $\forall \alpha, \beta \in \mathbb{Q}[x]$, tenim que $\alpha u + \beta v$ és divisible per $(x-\alpha)$ perquè tant u com v ho són i tant α com β no afecten. □

Problema 4. Sigui $\mathfrak{a}$ un ideal de l'anell A. Demostreu que $\mathrm{Ann}(\mathfrak{a}) = \{a \in A : ax = 0 \forall x \in \mathfrak{a}\}$ és un ideal d'A. S'anomena *anul·lador* d'$\mathfrak{a}$.

Solució. Ara, $\forall u, v \in \mathrm{Ann}(\mathfrak{a})$ i $\forall \alpha, \beta \in A$, tenim que $\alpha u + \beta v$ quan el multipliquem per qualsevol element de $\mathfrak{a}$, com que la multiplicació és distributiva i commutativa quan fem au i av ens donarà 0_A perquè s'anul·len. Així que la combinació lineal també s'anul·len. □

Problema 5. Un element a d'un anell s'anomena nilpotent si $a^n = 0$ per algun $n \geq 1$. Demostreu que el conjunt de tots els elements nilpotents d'una anell és un ideal. S'anomena *radical* de l'anell.

Solució. Siguin $u, v \in \mathrm{Ann}(\mathfrak{a})$ i $\alpha \in A$. Tenim que $(\alpha u)^n = \alpha^n\, u^n = 0$, per n que fa $u^n = 0$. Ara, si m és l'enter que fa $v^m = 0$, anem a comprovar que $(u+v)^{n+m} = 0$. En efecte:

$$(u+v)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} u^i v^{n+m-i} = \sum_{i=0}^{m} \binom{n+m}{i} u^i v^{n+m-i} + \sum_{i=m}^{m+n} \binom{n+m}{i} u^i v^{n+m-i} =$$

$$= v^m \Big(\sum_{i=0}^{n} \binom{n+m}{i} u^i v^{n-i}\Big) + u^n \sum_{i=n+1}^{m+n} \binom{n+m}{i} u^{i-n} v^{n+m-i} = 0 + 0 = 0$$

□

Problema 6. Demostreu que la suma d'un element nilpotent i una unitat d'una anell és una altra unitat.

Solució. Sigui n l'element nilpotent i k el primer enter positiu tal que $n^k = 0$ i sigui u una unitat de l'anell. Aleshores, considrem la següent equació, la qual simplement prové de les propietats PD, PA, PC per tant, es compleix per tot anell:

$$x^k - 1 = (1 + x)(1 - x + x^2 - \cdots + (-1)^{k-1}x^{k-1})$$

Ara, a la part dreta de l'equació, multipliquem el terme petit per u i el terme gran per u^-1 (es pot fer per associativitat i la propietat distributiva), a més, considerem els seus inversos per la suma, és a dir, canviem de signe tot:

$$1 - x^k = (u + ux)\left(\sum_{i=0}^{k-1}(-1)^{i+1}u^{-1}x^i\right)$$

Ara substituim $x = u^{-1}n$ i ens queda:

$$1 = 1 - u^{-k}n^k = (u + n)\left(\sum_{i=0}^{k-1}(-1)^{i+1}u^{-i-1}n^i\right)$$

I, per tant, hem trobat que existeix un element tal que multiplicat a $(u + n)$ dona 1. Llavors, $u + n$ és una altra unitat, que és el que volíem veure. □

Problema 7. Siguin $\zeta = e^{2\pi i/5}$ i $k \in \mathbb{Z}$. Considereu l'apliacació:

$$f : \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]$$
$$f(\sum_i (a_i\zeta^i)) = \sum_i a_i\zeta^{ki}$$

Demostreu que és un morfisme d'anells.

Solució. Clarament envia 1 a 1, perquè no té potencies (de fet envia qualsevol enter a ell mateix).

La suma es comprova amb fàcilment agrupant i separant termes amb la propietat distributiva, associativa i commutativa.

Pel producte, fem la multiplicacio i factoritzem. □

Problema 8. Siguin K un cos i $\alpha \in K$. Considereu l'aplicació:

$$\varphi_\alpha : K[x] \to K$$
$$f \to \varphi_\alpha(f) = f(\alpha)$$

és un morfisme exhaustiu d'anells. Concloeu que $K[x]/(x - \alpha)$ és isomorf a K.

Solució. Que el φ_α envia 1 a 1 està clar. La suma i producte està clar perquè l'evaliació de suma i producte de polinomis és, per definició, el producte i suma de les evaluacions.

L'exhaustivitat es fàcilment comprovable perquè $\forall a \in K$, el polinomi constant $p(x) = a$ està en la seva antiimatge.

Pel primer teorema d'isomorfisme, tenim que $K[x]/\ker f \cong K$, llavors voolem demostrar que $\ker f = (x - \alpha) = \{p(x)(x - \alpha)\}$. Clarament, l'ideal està dins del nucli perquè evaluant a α dona 0. I tot element del nucli, al ser evaluat a α dona 0, per tant, $p(x)$ té un factor α i llavors es divisible per $(x - \alpha)$ i $p(x)$ estarà en l'ideal de $(x - \alpha)$.

Alternativament, i millor, aquesta última inclusió es pot veure definint $q(x) = q(x + \alpha)$ veien que $q(0) = 0$ i, per tant, que no té coeficient constant, treient-lo per factor comú i tornant a p amb $p(x) = q(x - \alpha)$. □

Problema 9. Volem veure que es pot racionalitzar totes les fraccions de la forma

$$\frac{a+b\sqrt[3]{2}+c\sqrt[3]{4}}{d+e\sqrt[3]{2}+f\sqrt[3]{4}},\ a,b,c,d,e,f\in\mathbb{Q}$$

1. Demostreu que l'ideal de $\mathbb{Q}[x]$ generat pel polinomi x^3-2 és maximal.
2. Definiu un epimorfisme entre $\mathbb{Q}[x]$ i $\mathbb{Q}[\sqrt[3]{2}]=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:a,b,c\in\mathbb{Q}\}$.
3. Concloeu que $\mathbb{Q}[\sqrt[3]{2}]$ és un cos.

Solució.

1. Si volem veure que (x^3-2) és maximal, cal veure que no existeix un polinomi p tal que $(x^3-2)\subsetneq(p)\subsetneq\mathbb{Q}[x]$, perquè tots els ideals de l'anell de polinomis són generats per un element (perquè és principal). Ara bé, com que $(x^3-2)\subsetneq(p)$ implica que $p|x^3-2$ perquè (p) ha de contenir x^3-2. Però com que x^3-2 és irreductible això és impossible i hem acabat. En general, en els anells principals, els ideals generats per elements irreductibles són maximals.
2. Primer de tot, està clar que $\mathbb{Q}[\sqrt[3]{2}]$ és un anell, hereda les operacions típiques tot i que quan es fan potencies terceres torna a 2. Després, que el morfisme φ que agafa un polinimi $p(x)$ de $\mathbb{Q}[x]$ i l'evalua a $\sqrt[3]{2}$ és realment un morfisme (perquè l'1 va a l'1, la suma i el producte es comporten bé). I és exhaustiu perquè amb els polinomis $a+bx+cx^2$ en fem prou. El nucli de φ és $\ker\varphi=(x^3-2)$, perquè el polinomi més petit que conté l'arrel $\sqrt[3]{2}$ és aquest. Llavors, existeix un epimorfisme entre $\mathbb{Q}[x]$ i $\mathbb{Q}[\sqrt[3]{2}]$ tal que el nucle és l'ideal generat per x^3-2.
3. Pel primer teorema d'isomorfisme, tenim que $\mathbb{Q}[\sqrt[3]{2}]\cong\mathbb{Q}/(x^3-2)$, i com que (x^3-2) és maximal implica que el quocient és un cos i per tant, que $\mathbb{Q}[\sqrt[3]{2}]$ és un cos.

Extra: les fraccions de la forma descrita es poden racionalitzar perquè hem vist que tot element de la forma del polinomi de baix té un invers de la mateixa forma, per tant, multiplicant a dalt i a baix per aquest invers tenim que el denominador queda 1. □

Problema 10. *Teorema xinès dels residus.* Dos ideals I,J d'un anell $\mathbb{A}$ es diuen *coprimers* (o *comaximals*) si $I+J=\mathbb{A}$. Sigui $\varphi:\mathbb{A}\to\mathbb{A}/I\times\mathbb{A}/J$ el morfisme que té per components les projeccions canòniques: $\varphi(x)=([x]_I,[x]_J)$. Demostreu que:

1. Si I i J són coprimers aleshores $IJ{=}I\cap J$;

   INDICACIÓ: Existeixen $u\in I$ i $v\in J$ amb $u+v=1$.
2. Si I i J són coprimers aleshores per a tot parell d'elements $a,b\in\mathbb{A}$ existeix un element $x\in\mathbb{A}$ tal que $x\equiv a\pmod I$ i $x\equiv b\pmod J$, i la classe d'aquest element mòdul IJ queda unívocament determinada.
3. φ és exhaustiu si, i només si, I i J són coprimers.
4. Si I i J són coprimers aleshores $\mathbb{A}/IJ\cong\mathbb{A}/I\times\mathbb{A}/J$.

Solució.

1. $\subseteq$) Si tenim una combinació del producte $\sum u_iv_j$ com que, les u_i pertanyen a I, llavors u_iv_j segueix en I i fent la suma segueix en I. Simétricament també pertany a J.

   $\supseteq$) Primer veiem que $\exists u\in I,v\in J$ tal que $u+v=1$, que vé del fet que són coprimers. De fet, és un sí i només sí. Sigui $x\in I\cap J$, llavors $x=x(u+v)=xu+xv$, pel fet de $x\in J$, $u\in I$ i que $x\in I$, $v\in J$, tenim que $xu,xv\in I\cdot J$, llavors la suma també pertany al producte així que x pertany al producte.
2. $x=a+\alpha=b+\beta$, on $\alpha\in I$ i $\beta\in J$, llavors volem $a-b=\beta-\alpha$ que és la resta d'un element de J i un de I, que al ser I i J coprimers es pot fer. Més concretament, utilitzant u i v d'abans. $a-b=(a-b)u+(a-b)v$, per tant, $x=a-(a-b)u=b+(a-b)v$.

   Sigui x' un altre element amb les mateixes congruencies que x, llavors, $x-x'\in I,J$ i, per tant, $x-x'\in I\bigcap J=IJ$, aleshores tenen el mateix módul.

3. $\Longrightarrow$) Com que tot element té antiimatge, fem l'antiimatge de $([0],[1])$ que és un element $\alpha \in \mathbb{A}$ tal que α pertany a I perquè la seva clase és el 0 i existeix un element de J β tal que $\alpha = 1 + \beta$, per tant, l'1 es pot escriure com suma d'un element d'I i un element de J. Això és suficient per veure que I i J són coprimers (com hem dit a l'apartat 1), perquè $\forall x \in \mathbb{A}$ complex que $x\alpha - x\beta = x$ i el primer element és de I i el segon de J. Així que hem vist que I i J són comprimers.

   $\Longleftarrow$) Suposem que I i J són coprimers i agafem un element (a, b) qualsevol de l'espai de sortida de φ, ara busquem un element $x \in \mathbb{A}$ tal que $x \equiv a \pmod{I}$ i $x \equiv b \pmod{J}$ que és exactament l'apartat anterior, per tant, φ és exhaustiva.

4. Anem a veure que $\ker \varphi = IJ$, si un element té per imatge $([0]_I, [0]_J)$ vol dir que pertany a I i a J a la vegada. Per tant, $\ker I \cap J = IJ$ per l'apartat 1. Ara, pel primer teorema d'isomorfisme tenim el que ens demanen: $\mathbb{A}/IJ \cong \mathbb{A}/I \times \mathbb{A}/J$.

□

Problema 11. Demostreu que un ideal $\mathfrak{p}$ és primer si, i només si, $IJ \subseteq \mathfrak{p} \iff I$ o $J \subseteq \mathfrak{p}$, per a tot parell d'ideals I, J.

Solució. Suposem $\mathfrak{p}$ és primer.
$\Longleftarrow$) Si $I \subset \mathfrak{p} \implies IJ \subset \mathfrak{p}$, amb J igual.

$\Longrightarrow$) Suposem que $IJ \subseteq \mathfrak{p}$ i suposem que ni I ni J estan dintre de $\mathfrak{p}$. Llavors existeix $a \in I \setminus \mathfrak{p}$ i $b \in I \setminus \mathfrak{p}$. Però llavors, $ab \in IJ \subseteq \mathfrak{p}$, però per $\mathfrak{p}$ primer tenim que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, que contradiu la primera suposició, per tant, o $I \subseteq \mathfrak{p}$ o $j \subseteq \mathfrak{p}$.

Ara suposem que tenim un ideal $\mathfrak{p}$ tal que compleix la segona condició. Aleshores $\forall ab \in \mathfrak{p}$ com que alemenys $a \in (a)$ i $b \in (b)$ es compleix que $(a)(b) \subseteq \mathfrak{p}$ per tant, o bé $(a) \subset \mathfrak{p}$, o bé $(b) \subseteq \mathfrak{p}$. Llavors, com son els principals, això es pot traduir com: o bé a, o bé b pertanyen a $\mathfrak{p}$. □

Problema 12. Sigui $I \subset \mathbb{A}$ un ideal d'una anell $\mathbb{A}$.

1. Comproveu que $I[X] = \{\sum a_i X^i : a_i \in I\}$ és un ideal de l'anell de polinomis $\mathbb{A}[X]$.
2. Demostreu que I és primer si, i només si, $I[X]$ també ho és, però que tant si I és maximal com si no, $I[X]$ no ho és mai.
3. Demostreu que $\mathbb{A}[X]/I[X] \simeq (\mathbb{A}/I)[X]$.

Solució.

1. És tancat per la suma perquè es treu factor comú de cada X^i i I és tancap per la suma i si multipliques per un altre polinomi com tots els termes tenen un element de I, cada un d'ells pertany a I i la suma d'ells també i, per tant, $I[X]$ és un ideal.
2. Es pot fer a partir de l'apartat 3, per tant, suposem que l'apartat 3 està demostrat. Ara, per $(x) + I[x]$.
3. Ens definim $\varphi : A[x] \to (A/I)[x]$, que envia $\sum_n a_n X^n$ a $\sum_n \bar{a_n} X^n$. Clarament és exhaustiu perquè recull totes les classes. Ara $\ker \varphi = I[x]$, perquè és la classe del 0. I, pel primer teorema d'isomorfisme, $A[x]/I[x] \simeq (A/I)[x]$.

□

Problema 13. Un anell *local* és un anell que té un únic ideal maximal. Sigui $I \subseteq \mathbb{A}$ un ideal propi. Demostreu que:

1. Si $\mathbb{A} \setminus I \subseteq \mathbb{A}^*$ aleshores $\mathbb{A}$ és local i I és el seu ideal maximal.
2. Si I és maximal i $1 + I = \{1 + x : x \in I\} \subseteq \mathbb{A}^*$ aleshores $\mathbb{A}$ és local.

Solució.

1. Anem a veure que I és maximal. Suposem que existeix J tal que $\mathbb{A} \subsetneq J \subsetneq I$, llavors existeix $x \in J \setminus I \subseteq \mathbb{A} \setminus I \subset \mathbb{A}^*$. Llavors x és ínvertible i per tant, $J = \mathbb{A}$ perquè al multiplicar pel seu invers donaria 1 i a partir de 1, genera tot l'anell.

   Anem a veure que $\mathbb{A}$ és local. Sigui J un altre ideal maximal. Per tant, $x \in J \setminus I \subset \mathbb{A} \setminus I \subset \mathbb{A}^*$ i,igual que abans, $J = \mathbb{A}$, per tant no és maximal sino el total.

2. Suposem I maximal i que $1 + I \subset \mathbb{A}^*$, anem a veure que $\mathbb{A}$ és local fent servir l'apartat anterior. Sigui $x \in \mathbb{A} \setminus I$, llavors l'ideal $I + (x)$ és el total, perquè inclou sense igualtat a I però aquest és maximal. Llavors, qualsevol element d'$\mathbb{A}$ es pot posar com a suma d'un element de I i un de (x), com $1 = v + ux$ llavors, $xu = 1 - v \in 1 + I \subset A^*$, llavors x és invertible i, per tant $A \setminus I \subset \mathbb{A}^*$ i per l'apartat anterior, $\mathbb{A}$ és local.

□

Problema 14. Demostreu que tot domini d'integritat finit és un cos. Deduïu que en un anell finit tot ideal primer és maximal.

Problema 15. Sigui $\mathbb{A}$ un anell factorial. Siguin $u, v \in \mathbb{A}$ amb gcd(u, v)=1. Demostreu que si $uv = a^n$ amb $a \in \mathbb{A}$ aleshores existeixen $\alpha, \beta \in \mathbb{A}$ tals que $u \sim \alpha^n$ (associats), $v \sim \beta^n$ i $\alpha^n\beta^n = a^n$.

Solució. Com que estem en una anell factorial, podem escriure $a = \gamma p_1^{n_1} \cdots p_r^{n_r}$ $(n_i \neq 0)$, llavors, $a^n = \gamma p_1^{nn_1} \cdots p_r Pnn_r = uv$, per tant, $p_i | uv$, aleshores $p_i | u$ o bé $p_i | v$ i com que u i v no tenen divisors comuns aquesta o és exclusiva. Ara, per inducció, $p_i^{nn_i} | u$. En general, existeix un conjunt d'índexs S tal que $\alpha^n = \prod_{i \in S} p_i^{nn_i} | u$ i $\beta^n = \gamma \prod_{i \notin S} p_j^{nn_j} | v$ i que $\alpha^n\beta^n = a^n$ (perquè son tots els divisors), però per definició, $\alpha^n\beta^n = a^n = uv = (x\alpha^n)(y\beta^n)$, així que $xy = 1$ i, per tant, són unitats, és a dir $u \sim \alpha^n$ i $v \sim \beta^n$. □

Problema 16. Sigui d un enter positiu i $d \neq 1, 2$. Demostreu que l'anell $\mathbb{Z}[\sqrt{-d}]$ no és factorial.
INDICACIÓ: Demostreu que 2 és irreductible però no és primer.

Solució. Anem a veure que 2 és irreductible. Ho farem definint la norma $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + db^2$. Que va de l'anell a $\mathbb{N}$, és diferent de 0 per elements diferents de zero i és multiplicativa $(N(\alpha\beta) = N(\alpha)N(\beta))$ per la propia definició. I també $N(\alpha) = 1 \iff \alpha \in \mathbb{Z}[\sqrt{-d}]^*$, cap a la dreta podem agafar el conjugat i cap a l'esquerra perquè si $\alpha\alpha^{-1} = 1 \implies N(\alpha)N(\alpha^{-1}) = 1 \implies N(\alpha) = 1$.

Ara, suposem que 2 no és irreductible, és a dir, $2 = ab$ amb $a, b \notin Z[\sqrt{-d} \implies 4 = N(2) = N(ab) = N(a)N(b)$, llavors $N(a) = N(b) = 2$, però com que $N(a) = \alpha^2 + d\beta^2 = 2$, però 2 és massa petit ja que $\alpha^2 + d\beta^2$ o bé és 1, o bé és un quadrat més gran o bé és més gran o igual que d, en cap cas és 2. Llavors 2 és irreductible.

Anem a veure que 2 és primer. Per d parell, $2|\sqrt{-d}\sqrt{-d} = d$, però 2 no divideix a $\sqrt{-d}$ perquè si $\sqrt{-d} = 2(a + b\sqrt{-d})$ llavors $a = 0$ i $b = \frac{1}{2}$ que no és un enter. Per d senar, $2|(1 + \sqrt{-d})(1 - \sqrt{-d}) = 1 + d^2$, però 2 no divideix ni a un ni a l'altre perquè 2 no pot dividir a 1. □

Problema 17. Demostreu que els anells següents són euclidians amb les normes donades:

1. Els enters $\mathbb{Z}$, on $\delta(n)$ és el nombre de dígits en la representació en base 2 de $|n|$ (per exemple, $\delta(-6) = 3$ ja que 6 és 110 en base binària).
2. L'anell $\mathbb{Q}[X]$, on $\delta(f) = 2^{\deg f}$.
3. L'anell $\mathbb{Q}[[X]]$, on $\delta(\sum_{i=0}^{\infty} a_i X^i)$ és el i més petit tal que $a_i \neq 0$.

Solució.

1. Per aquesta funció, està clar que $\delta(2n) = \delta(n) + 1$, perquè quan es multiplica per 2, en binari, s'afegeix un 0 al final de més. En general, si multipliquem per altres dígits, almenys augmenta en 1 el nombre de digits, així que $\delta(ab) \geq \delta(a)$. La segona propietat és la dividir i que el residu doni o bé 0 o bé tingui una δ estrictament més petita. Aleshores, el que fem és fer la divisió normal i movent el residu de tal manera que $|r| \leq \frac{d}{2}$, aleshores $\delta(r) < \delta(d)$.

2. meh

3. La primera pròpietat és sencilla perquè la multiplicació de dos element té grau més petit la suma dels graus més petits, llavors ($\delta(pq) = \delta(p) + \delta(q)$). Fixem-nos que $\delta(p) = n$ llavors $p = x^n q$ amb $\delta(q)$ (i el recíproc també és cert). Després veurem que $\delta(p) = 0 \iff p \in Q[[X]]^*$. Utilitzant aquest petit lema, tenim que $D = x^n u$ (amb u unitat) i $d = x^m u_2$. Si $n \geq m$ llavors $D = x^{n-m} d u_1 u_2^{-1}$. Si $n < m$ llavors $r = D$ amb $q = 0$ i funciona perquè la pròpia δ ja és més petit. Ara anem a demostrar $\delta(p) = 0 \iff p$ unitat.

   $\Longrightarrow$) $\exists q$ tal que $pq = 1$, llavors $\delta(p) + \delta(q) = \delta(pq) = \delta(1) = 0$, llavors $\delta(p) = 0$.

   $\Longleftarrow$) Suposem $p = a_0 + a_1 x + a_2 x^2 + \cdots$ amb $a_0 \neq 0$ i el multipliquem per $q = b_0 + b_1 x + b_2 x^2 + \cdots$. Multiplicant, volem que sorti el primer igual a 1 i els altres graus igual a 0. Ara, per calcular les poténcia n-éssima només calen els n primers coeficients de p i q i que $a_0 \neq 0$ perquè queda $b_n a_0 + \cdots = 0$ passant restant i invers tenim b_n.

□

Problema 18. *Enters de Gauss.* Comproveu que l'anell $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ és euclidià amb la norma definida com $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

Solució. Que és un anell es pot veure comprovant que és un subanell de $\mathbb{C}$, ja que conté l'1, si restem dos element de $\mathbb{Z}[i]$ agrupant termes ens quedem en el mateix conjunt i quan multipliquem dos element, com que $i^2 = -1$ ens quedem a l'anell $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

Comencem reduint-nos al cas que volguem dividir $y = a + bi \in \mathbb{Z}[i]$ amb un $x \in \mathbb{N}$, utilitzant la divisió en els enters. Llavors, fem la divisió d'a i b entre x, però volem la condició que els residus en valor absolut siguin menors que $\frac{x}{2}$. Això es pot fer perquè en el cas que el residu fos entre $\frac{x}{2}$ i x el que podem fer és restar x. Aleshores, podem escriure $a = q_1 x + r_1$ i $b = q_2 x + r_2$, amb $|r_1||r_2| \leq \frac{x}{2}$. Llavors ens queda: $a + bi = (q_1 + q_2 i)x + (r_1 + r_2 i) = qx + r$, i tenim que $N(r) = r_1^2 + r_2^2 \leq \frac{x^2}{4} + \frac{x^2}{4} < x^2 = N(x)$.

En el cas general, volem dividir y entre x, però en comtes d'això dividim $y\bar{x}$ per $x\bar{x} = N(x)$, llavors és un natural. Pel cas anterior podem fer-ho: $y\bar{x} = qN(x) + r$, $N(r) < N(x)^2 = x^2\bar{x}^2$, llavors fem $r = y\bar{x} - qx\bar{x} = (y - qx)\bar{x} = r_0\bar{x}$, per tant $N(r_0) = N(r)N(\bar{x})^{-1} < N(x)^2 N(\bar{x})^{-1} = N(x)N(\bar{x})N(\bar{x})^{-1} = N(x)$. Retornant, $y = qx + r_0$, perquè $r_0 = y - qx$, i, per tant, hem dividit y entre x. □

Problema 19. Siguin $p \equiv 3 \pmod 4$ un nombre primer. Demostreu que no existeix un enter de Gauss de norma p.

Solució. Normalment, el 2 es deixa de banda. Llavors, anem a veure que si un primer compleix que existeix x tal que $p = N(x)$ aleshores $p \equiv 1(4)$ i per tant, per contrarecíproc, si tenim un $p' \equiv 3(4)$ no pot existir un x tal que $p = N(x)$. Ara, com p és la norma d'un cert enter de Gauss $x = a + bi$, tenim: $p = a^2 + b^2$, sense perdua de generalitat, suposem $a = 2n$ i $b = 2m + 1$ (al revés també funciona), llavors $p = 4n^2 + 4m^2 + 4m + 1 \equiv 1(4)$. □

Problema 20. Sigui $p \equiv 1 \pmod 4$ un nombre primer. Demostreu que existeix un enter de Gauss de norma p.

INDICACIÓ: Sigui $u \in \mathbb{Z}$ un enter tal que $u^2 \equiv -1 \pmod p$ (per què existeix?). Agafeu tots els enters de la forma $a + bu$ amb $0 \leq a, b < \sqrt{p}$, demostreu que n'hi ha dos que són congruents mòdul p i considereu la seva diferència.

ALTERNATIVA: amb el mateix u d'abans considereu $\gcd(u + i, p)$ a $\mathbb{Z}[i]$.

Solució. Anem a veure que si $p \equiv 1(4)$ llavors existeix un x tal que $p = N(x)$.

Primer fet $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} =< \alpha >$, perquè és un cos cíclic (amb ordre $p - 1$), per tant, podem trobar un generador les potencies del qual donen tots els elements. Llavors sigui $u = \alpha^{\frac{p-1}{4}}$, si l'elevem a la quarta tenim $\alpha^{p-1} \equiv 1(p)$ (per ser $p - 1$ l'ordre del cos). Llavors si només l'elevem al quadrat, tenim que $u^2 \equiv 1, -1(p)$, però pel fet que l'ordre és $p-1$ només pot ser -1, llavors, existeix un $u \leq p-1$ tal que $u^2 \equiv -1(p)$.

Considerem tots els nombres de la forma $\alpha + \beta u$ amb $0 \leq \alpha, \beta \leq \sqrt{p}$. Ara, com que hi ha almenys $\lfloor \sqrt{p}+1 \rfloor^2 \geq p$, pel principi del colomar, hi ha almenys dos nombres congruents modul p. Sigui $a+bu$ la diferència d'aquests nombres, que és un múltiple de p. Fixem-nos que $-\sqrt{p} < a, b < \sqrt{p}$. Per tant, $0 < a^2+b^2 < 2p$, anem a veure que és un múltiple de p: mòdul p $a \equiv -bu$ tenim que $a^2 \equiv -b^2$, llavors $a^2 + b^2 \equiv 0$ mòdul p. Com que l'únic múltiple de p entre 0 i $2p$ no inclosos és p, tenim que $a^2 + b^2 = p$, per tant, que existeix un nombre tal que la seva norma és p $(a + bi)$. □

Problema 21. Comproveu que els elements de $\mathbb{Z}[i]$ següents són primers:

1. $\pi_2 = 1 + i$ és un primer de norma 2.
2. Per a cada primer enter $p \equiv 1 \pmod 4$ hi ha dos primers diferents (no associats) conjugats: $\pi_p = a + bi$ i $\overline{\pi_p} = a - bi$, que tenen norma p;
3. Tot primer enter $q \equiv 3 \pmod 4$ és també un primer a $\mathbb{Z}[i]$, de norma q^2,

i que tot primer de $\mathbb{Z}[i]$ és associat d'algun d'ells.

Solució.

1. Anem a veure que π_2 és irreductible (llavors, com els enters de Gauss és un anell factorial, implicarà que és primer). Suposem que $\pi_2 = \alpha\beta$, fem normes, $2 = N(\pi_2) = N(\alpha)N(\beta)$ llavors, o bé $N(\alpha) = 1$ o bé, $N(\beta) = 1$. Llavors, o un o l'altre és una unitat. Per tant, π_2 és irreductible i primer.
2. Per l'exercici 20, existeix π_p tal que $p = a^2 + b^2 = \pi_p\overline{\pi_p}$. Suposem que $\pi_p = \alpha\beta \implies N(\pi_p) = p = N(\alpha)N(\beta)$ llavors un dels dos té norma 1, llavors és una unitat. I el mateix per $\overline{\pi_p}$. Ara, no són associats $(a \neq ub)$ perquè $a^2+b^2 = p$ que és senar llavors $a \neq b$ i diferents de 0, a més que només hi ha 4 possibilitats $u \in \{1, -1, i, -i\}$ que en tots els casos impliquen que $a = b$, contradicció. Llavors no poden ser associats.
3. Anem a veure que si $q \equiv 3(4)$ aleshores q primer. Suposem que $N(q) = q^2 = N(\alpha)N(\beta)$ i no pot ser que $N(\alpha) = N(\beta) = q$ perquè a l'exercici 19 hem vist que no pot ser. Així que un és q^2 i l'altre 1, per tant, un és una unitat i q és primer.

Suposem ara que tenim $\alpha \in \mathbb{Z}[i]$ primer, llavors

$$N(\alpha) = 2^n \prod_{p\equiv 1(4)} p^{n_p} \prod_{q\equiv 3(4)} q^{n_q} = (\pi_2)^n \overline{\pi_2}^n \prod_{p\equiv 1(4)} \pi_p^{n_p} \overline{\pi_p}^{n_p} \prod_{q\equiv 3(4)} q^{n_q} = \alpha\overline{\alpha}$$

llavors, com α és primer, ha de ser algun d'aquests primers o associats. □

Problema 22. Trobeu la factorització en primers de $2067 + 312i$ a $\mathbb{Z}[i]$.

Problemes complementaris

Problema 23. Comproveu que el conjunt $\mathcal{P}(X)$ de les parts d'un conjunt X, amb la "suma"definida com la *diferència simètrica* $A + B := A \triangle B = (A \bigcup B)$ i el "producte"definit com la intersecció $A \cdot B = A \bigcap B$ és un anell commutatiu.

Problema 24. Siguin I, J dos ideals d'un anell A. Demostreu que els conjunts:

$$\begin{aligned} I + J &= \{a + b : a \in I, b \in J\} \\ IJ &= A\langle ab : a \in I, b \in J\rangle \end{aligned}$$

són ideals d'A. Doneu un exemple en el qual $I \bigcup J$ no sigui un ideal.

Problema 25. Els ideals $I_1, \cdots, I_k$ d'un anell $\mathbb{A}$ es diuen coprimers si $\sum I_i = \mathbb{A}$ i coprimers dos a dos si $I_i + I_j = \mathbb{A}$ per a tot $i \neq j$. Sigui $\varphi : \mathbb{A} \to \prod \mathbb{A}/I_i$ l'homeomorfisme que té per components les proheccions canòniques. Demostreu que:

1. si $I_1, \ldots, I_k$ són coprimers dos a dos aleshores cada I_i és coprimer amb $\prod_{j\neq i} I_j$;

2. si $I_1, \ldots, I_k$ són coprimers dos a dos aleshores $\prod I_i = \bigcap I_i$;

3. si els I_i són coprimers dos a dos alehsores, donats elements $a_i \in \mathbb{A}$ existeix un element $x \in \mathbb{A}$ tal que $x \equiv a_i \pmod{I_i}$ per a tot i, i aquest element queda unívocament determinat llevat elements de $\prod I_i$.

4. φ és exhaustiu si, i només si, els I_i són coprimers dos a dos;

5. si els I_i són coprimers dos a dos aleshores $\mathbb{A}/\prod I_i \simeq \prod \mathbb{A}/I_i$.

Enuncieu i demostreu un resultat anàleg al del punt 2 que valgui per a ideals I_i, arbitraris.

Problema 26. *Teorema xinès a* $\mathbb{Z}$. Siguin $n_1, \cdots, n_k$ enteres positius coprimers dos a dos; o sigui $\gcd(n_1, n_2)=1$ per a tot $i \neq j$. Donats k enters $a_1, \cdots, a_k$, demostreu que existeix un enter $x \in \mathbb{Z}$ tal que $x \equiv a_i \pmod{n_i}$ per a tot i, i que aquest enter està unívocament determinat mòdul el producte $n_1 n_2 \cdots n_k$. Proveu que aquest x es pot expressar com

$$x = \sum_{i=1}^{k} a_i M_i N_i$$

on $N_i = N/n_i$ i M_i és un enter tal que $M_i N_i + m_i n_i = 1$, amb $m_i \in \mathbb{Z}$.

Problema 27. Determineu les unitats de l'anell $K[[x]]$ de sèries de potències amb coeficients en un cos K. Descriviu el cos de fraccions d'aquest anell.

Problema 28. Sigui $\mathbb{A}$ un anell commutatiu. Un element $e \in \mathbb{A}$ es *idempotent* si $e^2 = e$. Dos idempotents e_1, e_2 es diuen *ortogonals* si $e_1 e_2 = 0$.

1. Demostreu que si e és un idempotent aleshores $1 - e$ també ho és i són ortogonals.

2. Sigui e un idempotent. Demostreu que l'ideal principal (e) és un anell amb les mateixes operacions de $\mathbb{A}$. En quin cas és subanell?

3. Demostreu que tot ideal principal de $\mathbb{A}$ que sigui també un anell amb les operacions de $\mathbb{A}$ està generat per algun idempotent.

4. Comproveu que, al producte cartesià $\mathbb{A}_1 \times \mathbb{A}_2$ de dos anells, els elements (1,0) i (0,1) són idempotents ortogonals.

5. Demostreu que dos idempotents e_1, e_2 amb $e_1 + e_2 = 1$ indueixen un isomorfisme d'anells $\mathbb{A} \simeq e_1\mathbb{A} \times e_2\mathbb{A}$.

6. Trobeu tots els idempotents de $\mathbb{Z}/60\mathbb{Z}$ i doneu totes les descomposicions d'aquest anell com a producte cartesià de dos anells, llevat d'isomorfisme.

7. Enuncieu un resultat que relacioni les descomposicions $\mathbb{A} \simeq \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ d'un anell com a producte cartesià d'anells amb idempotents ortogonals de l'anell.

Problema 29. Demostreu que el radical d'un anell és la intersecció de tots els ideals primers de l'anell.

Problema 30. *Radical d'un ideal.* Sigui $I \subseteq \mathbb{A}$ un ideal. El seu radical es defineix com

$$\mathrm{Rad}(I) = \{a \in \mathbb{A} : \exists n \geq 1, a^n \in I\}$$

1. Comproveu que $\mathrm{Rad}(I)$ és un ideal.

2. Calculeu $\mathrm{Rad}(n\mathbb{Z})$ a l'anell $\mathbb{Z}$.

3. Demostreu que:

   (a) $I \subseteq R(I)$;

   (b) $\mathrm{Rad}(\mathrm{Rad}(I))=\mathrm{Rad}(I)$;

   (c) $\mathrm{Rad}(I \bigcap J)=\mathrm{Rad}(I) \bigcap \mathrm{Rad}(J)$;

   (d) $\mathrm{Rad}(I + J)=\mathrm{Rad}(\mathrm{Rad}(I)+\mathrm{Rad}(J))$;

(e) $\mathrm{Rad}(I^n)=\mathrm{Rad}(I)$;

(f) $\mathrm{Rad}(I)=\mathbb{A} \iff I=\mathbb{A}$;

(g) si $\mathfrak{p}$ és primer, $\mathrm{Rad}(\mathfrak{p})=\mathfrak{p}$.

Problema 31. Sigui $\mathbb{A}$ un anell íntegre i $\mathbb{K}$ el seu cos de fraccions. Sigui $\mathfrak{p}\subset\mathbb{A}$ un ideal primer. Demostreu que:

1. $\mathbb{A}_\mathfrak{p}:=\{\frac{a}{b}:a,b\in\mathbb{A},b\notin\mathfrak{p}\}\subseteq K$ és un subanell de $\mathbb{K}$ que conté a $\mathbb{A}$;
2. $\mathfrak{m}_\mathfrak{p}:=\{\frac{a}{b}\in\mathbb{A}_\mathfrak{p}:a\in\mathfrak{p}\}\subseteq\mathbb{A}_\mathfrak{p}$ és l'ideal maximal de $\mathbb{A}_\mathfrak{p}$;
3. $\mathbb{A}=\bigcap_\mathfrak{m}\mathbb{A}_\mathfrak{m}$ on la intersecció es fa sobre tots els ideals maximals $\mathfrak{m}$ de $\mathbb{A}$.

2 Anells de polinomis

Problema 32. 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 $q,r\in A[X]$ tals que $f=gq+r$ i $r=0$ o bé $\deg r<\deg g$.

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

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

Solució.

1. En el cas que $\deg f<\deg g$ escollint $q=0$ i $r=f$ ja ho tindriem, a més, per altres q, com que el grau és additiu, el polinomi resultant sempre queda de grau major o igual que $\deg g$ així que l'elecció és única.

   En el cas que $\deg f\geq\deg g$, ho argumentarem per inducció mentre el grau de f sigui major o igual que el de g. Anirem contruint el quocient terme a terme. Si $f(x)=a_0+a_1x+\ldots+a_nx^n$ i $g(x)=b_0+b_1x+\ldots+b_mx^m$, amb $b_m\in\mathbb{A}^*$. Llavors fem $f(x)-g(x)(b_m^{-1}a_nx^{n-m})$ per tal que el polinomi resultant sigui de grau $n-1$ i haguem disminuit el grau en 1. Així que el terme dominant del quocient és $b_m^{-1}a_nx^{n-m}$. D'aquesta manera es poden construir tots els termes, ja que les hipotesis es segueixen cumplint fins que el grau de f sigui menor que el de g i no poguem multiplicar per cap poténcia de x o el residu, és a dir, el resultat de la resta, sigui 0. La divisió és única perquè si algun dels termes del quocient fos diferent la resta no tindria un grau menys i els altres components no poden compençar aquesta mancança i el residu ve determinat quan ja tenim el quocient.

2. $K[X]$ és euclidià perquè l'aplicació $\delta(f)=\deg(f)$ defineix una norma en els polinomis, ja que $\deg(fg)=\deg(f)+\deg(g)\geq\deg(f)$ si $f,g\notin K[X]\setminus\{0\}$ i per l'apartat anterior, com que tots els coeficients són unitats el mateix algoritme serveix. Aleshores $K[X]$ és euclidià.

3. Per una banda, com que en aquest cas tenim un algoritme de la divisió en $A[x]$, existeixen q i r tal que $f=gq+r$ i suposem que $r\neq0$ per tant $\deg r<\deg g$. Per altra banda, tenim que $K[x]$, g divideix a f, per tant, $f=gq'$, aquest $q'\in K[x]$. Ara bé, si $gq'=gq+r$, tenim que $(q'-q)g=r$ i com que el grau és additiu $\deg g+\deg(q'-q)=\deg r$, però això no pot ser perquè l'algoritme de divisió ens assegurava que $\deg g>\deg r$. Així que $q'-q$ ha de ser 0. I, per tant, g divideix a f en $A[x]$.

□

Problema 33. Sigui $f(X)=a_0+a_1X+\ldots+a_nX^n$ 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 $a_1,\ldots,an$ 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.

Solució.

1. $\Longleftarrow$) Com que $a_1, \ldots, a_n$ són elements nilpotents i combinació d'elements nilpotents és un element nilpotent perquè el radical és un ideal, tenim que $a_1 x + \ldots + a_n x^n$ és un element nilpotent. Ara, com que a_0 és una unitat i unitat més element nilpotent és una unitat, tenim que $f(x)$ és una unitat.

   $\Longrightarrow$) Sabem que existeix $g(x)$ tal que $f(x)g(x) = 1$, en particular $f(0)g(0) = a_0 g(0) = 1$, per tant, a_0 és una unitat. Ara, considerem cada un dels termes de la multiplicació $f(x)g(x)$ i com que el resultat és 1, el termes més grans es cancel·len. Ara tenim que $b_m a_n = 0$, després $b_{m-1}a_n + a_{m-1}b_m = 0$, per tant, si multipliquem per a_n tenim: $b_{m-1}a_n^2 + a_{m-1}b_m a_n = b_{m-1}a_n^2 = 0$. I apliquem aquest métode amb tots el termes, multiplicant cada vegada per una potencia més gran, tots els termes es cancelen excepte el que té a_n i queda que$b_{m-r}a_n^{r+1} = 0$, per $r = 0, \ldots, m$. Mirant l'últim de tots, $b_0 a_n^{m+1} = 0$, però com que b_0 és invertible, multiplicant pel seu invers queda que a_n^{m-1}, és a dir, a_n és un element nilpotent. Ara podem considerar $f_1 = f - a_n x^n$ que és el mateix polinomi que f excepte l'últim grau. Fixem-nos que f és una unitat i que $-a_n x^n$ un element nilpotent, per tant, f_1 és una unitat. Així que d'aquesta manera, es compleixen les mateixes hipotesis que abans i seguint el mateix argument tindriem que a_{n-1} és un element nilpotent. Per inducció, arribarem a que $a_1, \ldots, a_n$ són tots elements nilpotents i hem acabat.

2. Utilitzarem que el radical d'un anell (el conjunt dels elements nilpotents) és un ideal.

   $\Longleftarrow$) Com que el radical d'un anell és un ideal, la combinació d'elements nilpotents és nilpotent i, per tant, si cada un dels quocifients d'un polinomi és nilpotent, el polinomi ho és.

   $\Longrightarrow$) Tenim que f és un element nilpotent, aleshores, existeix un enter m tal que $f^m = 0$, si mirem els quoficients, veiem que l'últim és $a_n^m x^{n+m}$ que ha de ser 0, per tant, $a_n^m = 0$, llavors a_n és un element nilpotent (de fet es pot veure que a_0 també ho és així de ràpid). D'aquesta manera, podem considerar $f_1 = f - a_n x^n$ que és un element nilpotent però de grau més petit. A cada pas reduïm un grau i veiem que un altre coeficient és nilpotent. Fins arribar a que tots els coeficients són nilpotents.

3. Els divisors de 0 d'un anell també és un ideal. En efecte, si $a, b \in A$ i son divisors de 0 ($ac = 0$ i $bd = 0$), llavors $\lambda a + \mu b$ és un dividor de 0, multiplicant per cd, $\lambda(ac)d + \mu(bd)c = 0$.

   $\Longleftarrow$) La combinació lineal de divisors de 0 és un altre divisor de 0, així que combinant coeficients que són divisors de 0 ens queda un polinomi que és divisor de 0.

   $\Longrightarrow$)Si $f(x)$ és divisor de 0, existeix $g(x) = b_0 + \ldots + b_m x^m$ tal que $f(x)g(x) = 0$. Llavors, el coeficient més gran és $a_n b_m = 0$, per tant, a_n és un divisor de 0. Fent el mateix raonament d'abans, restem $a_n x^n$ a f i ens segueix quedant un altre divisor de 0. Si fem el mateix argument veurem que a_{n-1} és un divisor de 0. Així anar fent fins que veiem que tots els element són divisors de 0.

□

Problema 34. 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.

Problema 35. Calculeu identitats de Bézout per a les parelles de polinomis 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. $f(X) = X^5 + X^4 + Xr + 1$ i $g(X) = X^5 + X^4 + X^3 + X^2$ a l'anell $\mathbb{Z}/2\mathbb{Z}[X]$.

Problema 36. Demostreu que, per a tot cos $\mathbb{K}$, l'anell $\mathbb{K}[X]$ conté infinits primers no associats.

Problema 37. Sigui A un anell íntegre. Demostreu que si $\mathbb{A}[X]$ és un domini d'ideals principals, llavors $\mathbb{A}$ és un cos.

Solució. Considerem $\alpha \in A \setminus \{0\}$. Llavors considerem l'ideal $(\alpha) + (x) = (f(X))$ ja que $\mathbb{A}[X]$ és principal. Ara bé, $\alpha \in (f(x)) \implies g(x)f(x) = \alpha$, però com que en anells íntegres el grau és additiu el grau de $f(x)$ ha de ser 0. A més, $x \in (f(x)) \implies f(x)h(x) = ch(x) = c(c^{-}1x)$, és a dir, $f(x)$ és un unitat. L'ideal generat per una unitat és el total, llavors $1 \in (f(x)) = (\alpha) + (x)$, és a dir, un element del primer més un del segon és 1. Però si en el segon posem μ, en el primer, com a mínim ens cal $-\mu x$ per compençar els elements que són de grau més gran o igual que 1. A part, d'un element de grau 0 que obligatoriament ha d'estar dins del λ i només pot ser α^{-1} per tal que multiplicat per λ doni 1. Aleshores $\mathbb{A}[X]$ és un cos. $\square$