Problemes del Tema 1: Anells.

Estructures Algebraiques. Grau en Matemàtiques, UPC, tardor 2020.

Àlex Batlle Casellas

Problemes de classe.

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

Comprovarem les tres condicions següents que defineixen ser subanell:

- $1_{\mathbb{C}} \in \mathbb{Z}[w]$.
- $x, y \in \mathbb{Z}[w] \implies x - y \in \mathbb{Z}[w]$.
- $x, y \in \mathbb{Z}[w] \implies xy \in \mathbb{Z}[w]$.

La primera és força evident, ja que posant $a = 1, b = 0$ ja tenim la unitat. La segona també és força evident: si $x = a_1 + b_1 w, y = a_2 + b_2 w$, aleshores la seva diferència és $x - y = (a_1 - a_2) + (b_1 - b_2)w \in \mathbb{Z}[w]$. La tercera condició la comprovem seguidament. El producte entre x i y és

$$(a_1 + b_1 w)(a_2 + b_2 w) = a_1 a_2 + (a_1 b_2 + b_1 a_2)w + b_1 b_2 w^2.$$

Veiem què val w^2:

$$w^2 = \left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right)^2 = \frac{1}{4} + \frac{1}{4}d + \frac{1}{2}\sqrt{d} = \frac{d+1}{4} + \left(w - \frac{1}{2}\right) = \frac{d-1}{4} + w.$$

Com que $d \equiv 1 \pmod 4$, la fracció $\frac{d-1}{4}$ és un enter. Per tant, si diem $k = \frac{d-1}{4} \in \mathbb{Z}$, aleshores el resultat del producte és

$$a_1 a_2 + (a_1 b_2 + b_1 a_2)w + b_1 b_2 \left(\frac{d-1}{4} + w\right) = \left(a_1 a_2 + b_1 b_2 \frac{d-1}{4}\right) + (a_1 b_2 + b_2 a_1 + b_1 b_2)w \in \mathbb{Z}[w]$$

■

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 $\mathbb{C}$.

És evident que hi ha la unitat dels enters i que la suma i la diferència es comporten bé dins d'aquest conjunt. El producte és

$$(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4)(b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3 + b_4\zeta^4) = \sum_{i=0,j=0}^{4} a_i b_j \zeta^{i+j}.$$

Com que les potències de ζ són cícliques, és evident que això seran combinacions enteres de potències (fins la quarta) de ζ. Noti's que aquest resultat val per a qualsevol arrel n-èssima de la unitat ■

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

Sigui $I = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\}$. Comprovarem les dues condicions següents que defineixen ser un ideal d'un anell A:

- $x, y \in I \implies x + y \in I$.
- $x \in I, \lambda \in A \implies \lambda x \in I$.

La primera condició és senzilla de comprovar: siguin $f, g \in I$, aleshores el polinomi a coeficients racionals $f + g$ s'anul·la en α: $(f + g)(\alpha) = f(\alpha) + g(\alpha) = 0$. La segona condició també és força senzilla: sigui $a(x) \in \mathbb{Q}[x]$, aleshores el polinomi producte avaluat en α és $(fa)(\alpha) = f(\alpha)a(\alpha) = 0 \cdot a(\alpha) = 0$. Per tant, I és un ideal de $\mathbb{Q}[x]$ ■

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

Si $x, y \in \operatorname{Ann} \mathfrak{a}$, aleshores clarament $\forall \beta \in \mathfrak{a}$ es té que $(x + y)\beta = x\beta + y\beta = 0_A + 0_A = 0_A$. També està clar que si $\alpha \in A$, aleshores $\forall \beta \in \mathfrak{a}$ es té $(\alpha x)\beta = \alpha(x\beta) = \alpha 0_A = 0_A$ ■

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'un anell n'és un ideal. S'anomena *radical* de l'anell.

Anomenem $\operatorname{Rad} A := \{x \in A : \exists n \in \mathbb{N},\ x^n = 0\}$. Siguin $x, y \in \operatorname{Rad} A$, i $\alpha \in A$. Clarament, com que estem en un anell commutatiu, $(\alpha x)^n = \alpha^n x^n = 0$. Per la suma, siguin $n, m \in \mathbb{N}$ tals que $x^m = 0, y^n = 0$. Aleshores, $(x + y)^{n+m} = 0$. Vegem-ho:

$$(x+y)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} x^j y^{n+m-j} =$$

$$\sum_{j=0}^{m} \binom{n+m}{j} x^j y^{n+m-j} + \sum_{j=m+1}^{n+m} \binom{n+m}{j} x^j y^{n+m-j} =$$

$$\underbrace{y^n}_{0_A} \sum_{j=0}^{m} \binom{n+m}{j} x^j y^{m-j} + \underbrace{x^m}_{0_A} \sum_{j=m+1}^{n+m} \binom{n+m}{j} x^{j-m} y^{n+m-j} =$$

$$0_A + 0_A = 0_A.$$

Per tant, el radical d'un anell n'és un ideal ■

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

Sigui z un element nilpotent ($z^n = 0_A$) i u una unitat de l'anell. La motivació per la resolució d'aquest exercici és recordar la identitat notable $(u+z)(u-z) = u^2 - z^2$. Volem que aquest exponent sigui una n, i així l'element nilpotent no contribueix a la suma i podem invertir la resta multiplicant repetidament per l'invers de la unitat. Per tant, observem el següent:

$$(u+z)\left(u^{n-1} - u^{n-2}z + u^{n-3}z^2 - u^{n-4}z^3 + \cdots\right) =$$
$$u^n + zu^{n-1} - u^{n-1}z - u^{n-2}z^2 + \cdots + (-1)^n z^n =$$
$$u^n.$$

Per aquest element ja sabem que tenim invers, per definició d'unitat. Per tant, resumint, $u + z$ es pot invertir fent

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

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

$$\begin{array}{rcl} f : \mathbb{Z}[\zeta] & \longrightarrow & \mathbb{Z}[\zeta] \\ \sum_{i=0}^{4} a_i\zeta^i & \longmapsto & \sum_{i=0}^{4} a_i\zeta^{ki}. \end{array}$$

Demostreu que és un morfisme d'anells.

Veurem que és un morfisme d'anells comprovant les tres condicions següents:

- $f(1) = 1$.
- $x, y \in \mathbb{Z}[\zeta] \implies f(x+y) = f(x) + f(y)$.
- $x, y \in \mathbb{Z}[\zeta] \implies f(xy) = f(x)f(y)$.

La primera condició és bastant evident, ja que $f(1+0+0+0+0) = 1$. La segona condició també és bastant directe, ja que

$$f\left(\sum_i a_i\zeta^i + \sum_i b_i\zeta^i\right) = f\left(\sum_i (a_i+b_i)\zeta^i\right) = \sum_i (a_i+b_i)\zeta^{ki} = \sum_i a_i\zeta^{ki} + \sum_i b_i\zeta^{ki} = f\left(\sum_i a_i\zeta^i\right) + f\left(\sum_i b_i\zeta^i\right).$$

La tercera condició requereix exactament la mateixa quantitat de treball:

$$f(xy) = f\left(\left(\sum_i a_i\zeta^i\right)\cdot\left(\sum_j b_j\zeta^j\right)\right) = f\left(\sum_{i,j} a_ib_j\zeta^{i+j}\right) = \sum_{i,j} a_ib_j\zeta^{k(i+j)} = \sum_i a_i\zeta^{ki}\sum_j b_j\zeta^{kj} = \left(\sum_i a_i\zeta^{ki}\right)\left(\sum_j b_j\zeta^{kj}\right) = f(x)f(y)$$ ■

Noti's que aquest resultat val per qualsevol anell $\mathbb{Z}[\omega]$ per $\omega = e^{2\pi i/n}$, $n \in \mathbb{N} \setminus 0$.

8. Siguin A un anell i $\alpha \in A$. Considereu l'aplicació

$$\begin{array}{rcl} \varphi_\alpha : A[x] & \longrightarrow & A \\ f & \longmapsto & f(\alpha). \end{array}$$

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

És un morfisme d'anells. Efectivament, comprovarem les tres condicions que hem comentat a l'exercici anterior:

- $f(1) = 1$ ja que 1 és un polinomi constant.
- $f(p+q) = (p+q)(\alpha) = p(\alpha) + q(\alpha) = f(p) + f(q)$.
- $f(pq) = (pq)(\alpha) = p(\alpha)q(\alpha) = f(p)f(q)$.

És exhaustiu ja que, donat $a \in A$, el polinomi constant $p(x) = a$ és tal que $f(p) = p(\alpha) = a$. Vegem ara que efectivament $A[x]/(x-\alpha) \cong A$. Si demostrem que $\ker f = (x-\alpha)$, ja haurem provat l'isomorfisme. Clarament, $(x-\alpha) \subseteq \ker f$, ja que $(x-\alpha) = \{h(x)(x-\alpha) : h(x) \in A[x]\}$, i $f(h(x)(x-\alpha)) = h(\alpha)(\alpha-\alpha) = 0$. Vegem ara que $\ker f \subseteq (x-\alpha)$. En efecte, si $p(x) \in \ker f$, aleshores sigui $q(x) = p(x+\alpha)$. $q(x)$ és $q(x) = \sum_{j=0}^{n} q_i x^i$, per alguna $n \in \mathbb{N}$ tal que $q_n \neq 0$. Aleshores, $q_0 = q(0) = p(0+\alpha) = p(\alpha) = 0$. Aleshores, $q(x)$ no té terme independent i podem escriure $q(x) = x\left(q_1 + q_2 x + q_3 x^2 + \ldots + q_n x^{n-1}\right) = x \cdot q'(x)$. Aleshores, tornem a la definició de $q(x)$ i fem $p(x) = q(x-\alpha) = (x-\alpha)q'(x-\alpha)$. Això vol dir, però, que $p(x) \in (x-\alpha)$, i per tant, que $\ker f \subseteq (x-\alpha)$. Per tant, tenim que $(x-\alpha) = \ker f$. Pel primer teorema d'isomorfisme, sabem que el següent és cert:

$$A[x]/(x-\alpha) = A[x]/\ker f \cong \operatorname{Im} f = A \ \blacksquare$$

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

$$\frac{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}}{b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{4}},\ a_i, b_i \in \mathbb{Q}.$$

(a) Demostreu que l'ideal de $\mathbb{Q}[x]$ generat pel polinomi $x^3 - 2$ és maximal.

(b) Definiu un epimorfisme entre $\mathbb{Q}[x]$ i $\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

(c) Concloeu que $\mathbb{Q}[\sqrt[3]{2}]$ és un cos.

(a)
Sigui $I \subseteq \mathbb{Q}[x]$ un ideal tal que $(x^3-2) \subsetneq I$. Aleshores, $\exists p(x) \in I \setminus (x^3-2)$. Per tant, $p(x)$ es pot escriure com $p(x) = q(x) + r(x)$, amb $q(x) \in (x^3-2)$ i $r(x) \notin (x^3-2)$. A més, $r(x) = p(x) - q(x) \in I$, ja que ambdós polinomis en formen part. Com que $x^3 - 2 \in (x^3-2) \subsetneq I$, l'ideal generat per x^3-2 i $r(x)$ es troba tot dins d'I. Però, $(x^3-2, r(x)) = \mathbb{Q}[x]$, ja que $\forall a(x) \in \mathbb{Q}[x]$, $a(x)$ es pot escriure com $a(x) = (x^3-2)q(x) + r(x)s(x)$. Si $a(x) \in (x^3-2)$, aleshores $s(x) \equiv 0$, i si $a(x) \notin (x^3-2)$, aleshores $q(x) \equiv 0$. Per tant, tenim que $\mathbb{Q}[x] = (x^3-2, r(x)) \subseteq I$, i per tant, $\mathbb{Q}[x] = I$. Per tant, (x^3-2) és un ideal maximal.

(b)
Sigui e la següent aplicació:

$$\begin{aligned} e : \mathbb{Q}[x] &\twoheadrightarrow \mathbb{Q}[\sqrt[3]{2}] \\ p(x) &\longmapsto p(\sqrt[3]{2}) \end{aligned}$$

És clarament exhaustiva: sigui $y = y_0 + y_1\sqrt[3]{2} + y_2\sqrt[3]{4}$, aleshores $p_y(x) = y_0 + y_1 x + y_2 x^2$ és tal que $e(p_y) = p_y(\sqrt[3]{2}) = y$.

(c)
Observem que $(x^3-2) = \ker e$, i com ja hem vist, $\mathbb{Q}[\sqrt[3]{2}] = \operatorname{Im} e$. Per tant, com que e és un morfisme d'anells (clarament), pel primer teorema d'isomorfisme tenim que

$$\mathbb{Q}[x]/(x^3-2) = \mathbb{Q}[x]/\ker e \cong \operatorname{Im} e = \mathbb{Q}[\sqrt[3]{2}].$$

A més, com que l'ideal (x^3-2) és maximal, aleshores $\mathbb{Q}[x]/(x^3-2)$ és un cos, i per tant, la seva imatge per un isomorfisme també (comprovació immediata per ser un isomorfisme un morfisme d'anells bijectiu). Per tant, $\mathbb{Q}[\sqrt[3]{2}]$ és un cos $\blacksquare$

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 $\phi : \mathbb{A} \to {}^{\mathbb{A}}\!/_{I} \times {}^{\mathbb{A}}\!/_{J}$ el morfisme que té per components les projeccions canòniques, $\phi(x) = ([x]_I, [x]_J)$. Demostreu que:

(a) Si I i J són coprimers, aleshores $IJ = I \cap J$.
INDICACIÓ: Existeixen $u \in I$ i $v \in J$ amb $u + v = 1$.

(b) 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.

(c) ϕ és exhaustiu si, i només si, I i J són coprimers.

(d) Si I i J són coprimers, aleshores ${}^{\mathbb{A}}\!/_{IJ} \cong {}^{\mathbb{A}}\!/_{I} \times {}^{\mathbb{A}}\!/_{J}$.

(a)
Veurem primer la inclusió $\boxed{IJ \subseteq I \cap J:}$ sigui $\sum_i u_i v_i$ un element de IJ. Aleshores, $u_i \in I \subseteq A, v_i \in J \subseteq A$. Com que tant I com J són ideals, tenim que $\sum_i u_i v_i \in I$, i també que $\sum_i u_i v_i \in J$. Per tant, $\sum_i u_i v_i \in I \cap J$.
Vegem ara la inclusió contrària, $\boxed{IJ \supseteq I \cap J:}$ primer, observem que la condició de ser coprimers I i J, $I + J = A$, és equivalent a dir que existeixen $u \in I, v \in J$ tals que $u + v = 1$. Aleshores, sigui $x \in I \cap J$, llavors $x = x(u + v) = xu + xv$, i com que $x \in I \cap J, u \in I, v \in J$, això és un element de IJ. Per tant, hem demostrat que $IJ = I \cap J$ si I i J són coprimers.

(b)
Volem trobar $\alpha \in I, \beta \in J$ tals que es compleixi

$$\left.\begin{aligned} x &= a + \alpha \\ x &= b + \beta \end{aligned}\right\}$$

Aleshores, clarament tenim que $a - b = \beta - \alpha$. Com que $u + v = 1$, aleshores tenim que $a - b = (a - b)(u + v) = (a - b)u + (a - b)v$, sent el primer un membre d'I i el segon un element de J. Per tant, ja tenim les α i β que buscàvem, i la x serà, per tant,

$$x = a - (a - b)u = b + (a - b)v.$$

Ara vegem que la classe d'x mòdul IJ està unívocament determinada: sigui x' tal que compleix les mateixes relacions que x, és a dir, $x' \equiv a \pmod{I}$ i $x' \equiv b \pmod{J}$. Aleshores, per la primera condició, $x - x' \in I$, i per la segona, $x - x' \in J$. Per tant, $x - x' \in I \cap J = IJ$, i per tant, $[x']_{IJ} = [x]_{IJ}$.

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

Primer prenem $\mathfrak{p}$ un ideal primer. Vegem que es compleix la condició:
$\boxed{\Longrightarrow}$ $IJ \subseteq \mathfrak{p}$. Suposem que $I \not\subset \mathfrak{p}$ i $J \not\subset \mathfrak{p}$. Aleshores, existeixen $a \in I \setminus \mathfrak{p}$, $b \in J \setminus \mathfrak{p}$. L'element ab pertany a l'ideal producte, $ab \in IJ \subseteq \mathfrak{p}$. Però, com que $\mathfrak{p}$ és primer, aleshores o bé $a \in \mathfrak{p}$ o bé $b \in \mathfrak{p}$, contradient el fet que $a \notin \mathfrak{p}$ o que $b \notin \mathfrak{p}$. Per tant, $I \subseteq \mathfrak{p}$ o bé $J \subseteq \mathfrak{p}$.

$\boxed{\Longleftarrow}$ Si $I \subseteq \mathfrak{p}$, aleshores $IJ \subseteq I \cap J \subseteq I \subseteq \mathfrak{p}$. Per tant, $IJ \subseteq \mathfrak{p}$.

Falta comprovar que si es compleix la condició, aleshores $\mathfrak{p}$ és primer. Siguin I i J dos ideals. Sigui $ab \in IJ \subseteq \mathfrak{p}$, amb $a \in I, b \in J$. Com que es compleix la condició, el fet que $ab \in IJ \subseteq \mathfrak{p}$ implica que $a \in \mathfrak{p}$ o bé $b \in \mathfrak{p}$. És a dir, que $\mathfrak{p}$ és un ideal primer ■

12. Sigui $I \subseteq \mathbb{A}$ un ideal d'un anell $\mathbb{A}$.

1. Comproveu que $I[X] = \left\{\sum_i a_i X^i : a_i \in I\right\}$ 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 $\mathbb{A}[X]/I[X] \cong \left(\mathbb{A}/I\right)[X]$.

1.
Siguin $p, q \in I[x], \alpha \in \mathbb{A}[x]$. Aleshores, la suma és

$$p + q = \left(\sum_{i=0}^{d_p} p_i x^i\right) + \left(\sum_{j=0}^{d_q} q_j x^j\right) = \sum_{i=0}^{\max(d_p,d_q)} (p_i + q_i)x^i \in I[x],$$

on ampliem el polinomi de menor grau amb zeros a partir de $\min(d_q, d_p)$. El producte αp és

$$\alpha p = \left(\sum_{i=0}^{d_\alpha} \alpha_i x^i\right)\left(\sum_{j=0}^{d_p} p_j x^j\right) = \sum_{i,j} \alpha_i p_j x^{i+j},$$

i clarament $\alpha_i p_i \in I$ ja que I és un ideal. Per tant, $I[x]$ és un ideal.

2.
$\boxed{\Longrightarrow}$ Recordem que un ideal I és primer si, per definició, passa que

$$ab \in I \implies \begin{cases} a \in I, & \text{o bé} \\ b \in I. \end{cases}$$

Aleshores, sigui pq un element de $I[x]$; és de la forma

$$\sum_{i,j} p_i q_j x^{i+j}.$$

Com que és un element d'$I[x]$, es té que $p_i q_j \in I$ per a tot i, j. Podem assumir que $p_i \in I\ \forall i$. Si no fos així, existiria una parella (i, j) de coeficients p_i, q_j tals que multiplicats donarien un element de fora de l'ideal I i aleshores seria $pq \notin I[x]$. Per tant, $p \in I[x]$.

$\boxed{\Longleftarrow}$ $I[x]$ és primer. Aleshores, sigui $pq \in I[x]$ com abans. Podem assumir que $p \in I[x]$ ja que $I[x]$ és primer. Per tant, tots els $p_i \in I$. D'aquí podem treure tots els productes d'elements de I amb elements d'$\mathbb{A}$, ja que no hi ha cap restricció respecte de què pot ser q. Per tant, sempre que tinguem un producte d'elements $p_i q_j$, serà $p_i \in I$, el que vol dir que I és un ideal primer.

A més, vegem que tant si I és maximal com si no, $I[x]$ no ho és mai. Si ho fos, aleshores $\mathbb{A}[x]/I[x]$ seria un cos isomorf a un anell de polinomis (com veiem al següent apartat), on per exemple l'element x no té invers.

3.
Sigui φ la següent aplicació:

$$\begin{aligned} \varphi : \mathbb{A}[x] &\twoheadrightarrow \left(\mathbb{A}/I\right)[x] \\ \sum a_n x^n &\longmapsto \sum [a_n]_I x^n \end{aligned}$$

És exhaustiva i a més, clarament és $\ker\varphi = I[x]$. Pel Primer Teorema d'Isomorfisme,

$$\mathbb{A}[x]/I[x] = \mathbb{A}[x]/\ker\varphi \cong \operatorname{Im}\varphi = \left(\mathbb{A}/I\right)[x]$$

■

13. Un anell *local* és un anell que té un únic ideal maximal. Sigui $I \subseteq \mathbb{A}$ un ideal propi de l'anell $\mathbb{A}$. 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.

1.
Vegem que I és maximal. Suposem que $I \subsetneq J \subseteq A$. Aleshores, $\exists x \in J \setminus I \subseteq A \setminus I \subseteq A^*$. Si $x \in \mathbb{A}^*$, això vol dir que $(x) \subseteq J$ és l'ideal total, i per tant, que $J = A$, és a dir, que I **és maximal**. Ara vegem que $\mathbb{A}$ és un anell local. Sigui $J \subsetneq \mathbb{A}$ un ideal maximal, $J \neq I$. Aleshores, existeix un punt $x \in J \setminus I \subseteq A \setminus I \subseteq A^*$, i per tant, $x \in \mathbb{A}^*$, o el que és el mateix, $J = A$. Per tant, J no és maximal, i per tant $\mathbb{A}$ és un anell local.

2.
Sigui $x \in A \setminus I$. Aleshores, tenim que $I \subsetneq (x) + I \subseteq A$, i per tant, que $(x) + I = A$. Per tant, (x) i I són coprimers, i llavors existeixen $v \in I, u \in \mathbb{A}$ tals que $v + xu = 1$. Per tant, $xu = 1 - v \in 1 + I \subseteq \mathbb{A}^*$, i per tant $x \in \mathbb{A}^*$. Per l'apartat anterior, $\mathbb{A}$ és un anell local ■

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

Sigui $\mathbb{D}$ un domini d'integritat finit, i $d \in \mathbb{D} \setminus \{0_{\mathbb{D}}\}$ un element no nul qualsevol. Definim $d^{\mathbb{N}} := \{d^k : k \in \mathbb{N}\}$. Aleshores,

$$\left.\begin{array}{l} 0 \notin d^{\mathbb{N}} \\ d^{\mathbb{N}} \subseteq \mathbb{D} \end{array}\right\} \implies \exists i < j \in \mathbb{N} : d^i = d^j \xrightarrow{j=i+k} d^i = d^i d^k \implies d^i(1-d^k) = 0 \xrightarrow{0 \notin d^{\mathbb{N}}} 1 - d^k = 0 \implies d^k = 1.$$

Per tant, $d^{-1} = d^{k-1}$, i per tant, tots els elements no nuls tenen invers. Això implica que $\mathbb{D}$ és un cos, ja que compleix totes les condicions de la definició. A més, vegem que en un anell finit, tot ideal primer és maximal. Sigui $\mathfrak{p} \subseteq \mathbb{A}$ un ideal primer d'un anell finit. Aleshores, sabem que $\mathbb{A}/\mathfrak{p}$ és un domini d'integritat, i finit. Per tant, com acabem de veure, $\mathbb{A}/\mathfrak{p}$ és un cos. Això només passa si $\mathfrak{p}$ és un ideal maximal ■

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 $u \sim \alpha^n, v \sim \beta^n$ i $\alpha^n \beta^n = a^n$.

Com que $\mathbb{A}$ és un anell factorial, això vol dir que a es pot escriure com a producte d'irreductibles, $a = \gamma p_1^{n_1} \cdots p_r^{n_r}$. Llavors, $a^n = \gamma^n p_1^{n \cdot n_1} \cdots p_r^{n \cdot n_r}$, que per hipòtesi és uv. Per tant, tenim que $p_i \mid uv$, i com que $\gcd(u, v) = 1$, aleshores podem assumir que $p_i \mid u$ i $p_i \nmid v$. També, de la descomposició deduïm que $p_i^{n \cdot n_i} \mid u$. Aleshores, tenim (sent $\mathcal{S}$ el conjunt d'índexos i tals que $p_i \mid u$)

$$\left.\begin{array}{l} \overbrace{\prod_{i \in \mathcal{S}} p_i^{n \cdot n_i}}^{\alpha^n} \mid u \\ \overbrace{\prod_{j \notin \mathcal{S}} p_j^{n \cdot n_j}}^{\beta^n} \mid v \end{array}\right\} \implies \alpha^n \beta^n = a^n.$$

Vegem ara que $u \sim \alpha^n$ i que $v \sim \beta^n$: suposem que $u = \alpha^n x, v = \beta^n y$. Aleshores, $\alpha^n \beta^n = a^n = uv = \alpha^n \beta^n xy$. Per tant, $xy = 1$, el que vol dir que tant x com y són unitats, i per tant, que $u \sim \alpha^n, v \sim \beta^n$ ■

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

Primer de tot, recordem que quan un anell és factorial, els elements irreductibles són primers. Per tant, si trobem un element irreductible no primer, haurem demostrat que aquests anells no són factorials. Per a fer això, definim la següent aplicació:

$$\begin{array}{rcl} N : \mathbb{Z}[\sqrt{-d}] & \longrightarrow & \mathbb{N} \\ a + b\sqrt{-d} & \longmapsto & (a + b\sqrt{-d})(a - b\sqrt{-d}) \end{array}$$

Clarament tenim que $N(z) \neq 0$ si $z \neq 0$, i que $N(\alpha\beta) = N(\alpha)N(\beta)$. Sigui $A := \mathbb{Z}[\sqrt{-d}]$. Vegem que $N(\alpha) = 1 \iff \alpha \in A^*$.

$$\boxed{\Longrightarrow}\ N(\alpha) = \alpha\bar{\alpha} = 1 \implies a^2 + db^2 = 1 \overset{d>2}{\Longrightarrow} a = \pm 1 \implies a \in A^*,$$
$$\boxed{\Longleftarrow}\ \alpha\alpha^{-1} = 1 \implies N(\alpha\alpha^{-1}) = 1 \implies N(\alpha)N(\alpha^{-1}) = 1 \implies N(\alpha) = 1.$$

Ara, vegem que $2 \in A$ és irreductible però no és primer:

(i) 2 és irreductible: vegem-ho per reducció a l'absurd. Sigui $2 = \alpha\beta$, amb cap d'elles una unitat. Aleshores,
$$4 = N(2) = N(\alpha)N(\beta) \implies N(\alpha) = N(\beta) = 2,$$
però $N(\alpha) = a^2 + db^2 = 2$ és una contradicció, ja que $a^2, b^2 \geq 1$, i $1 + d > 2$. Per tant, 2 és irreductible.

(ii) 2 no és primer. Separem-ho en dos casos: d parell i d senar. Si d és **parell**, aleshores $\sqrt{-d}\sqrt{-d} = -d \in (2)$, però observem que $\sqrt{-d} \notin (2)$. Si fos el contrari, seria $\sqrt{-d} = 2(a + b\sqrt{-d}) \implies a = 0, b = 2^{-1}$, el que no pot ser ja que $2 \notin A^*$ (la norma de 2 és 4).
Si d és **senar**, aleshores $(1 + \sqrt{-d})(1 - \sqrt{-d}) = 1 + d \in (2)$, però $1 + \sqrt{-d}, 1 - \sqrt{-d} \notin (2)$ ■

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 $\mathbb{Q}[[x]]$.

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

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

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 de congruents mòdul p i considereu la seva diferència.
ALTERNATIVA: Amb el mateix nombre u d'abans, considereu $\gcd(u + i, p)$ a $\mathbb{Z}[i]$.

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

- $\pi_2 = 1 + i$ és un primer de norma 2;
- per a cada primer enter $p \equiv 1 \pmod 4$ hi ha dos primers diferents (no associats) conjugats: $\pi_p = a + ib$ i $\bar{\pi}_p = a - ib$, que tenen norma p;
- tot primer enter $q \equiv 1 \pmod 4$ és també un primer a $\mathbb{Z}[i]$, de norma q^2,

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

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

Problemes complementaris.

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

Per comprovar que $(\mathcal{P}(X), \Delta, \cap)$ és un anell abelià, hem de:

- Veure que la suma és commutativa.
- Trobar un neutre per la suma.
- Trobar l'oposat per la suma.
- Veure que el producte és commutatiu.
- Trobar un neutre pel producte.
- Comprovar la propietat distributiva.

Veiem primer que la suma és commutativa: en efecte,

$$A + B = A\Delta B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B\Delta A = B + A.$$

L'element neutre de la suma és el conjunt buit, $\varnothing$. Vegem-ho:

$$A + \varnothing = A\Delta\varnothing = (A \cup \varnothing) \setminus (A \cap \varnothing) = A \setminus \varnothing = A.$$

L'oposat d'A per la suma és A mateix:

$$A + A = A\Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \varnothing.$$

El producte és evidentment commutatiu ja que és la intersecció de conjunts típica. El neutre pel producte és el conjunt total, X. Vegem-ho:

$$A \cdot X = A \cap X = A.$$

Per últim, comprovem la propietat distributiva:

$$\begin{aligned} A \cdot (B + C) = A \cap (B\Delta C) = A \cap \big((B \cup C) \setminus (B \cap C)\big) = \big(A \cap (B \cup C)\big) \setminus (B \cap C) = \\ A \cap (B \cup C) \cap (B \cap C)^C = A \cap (B \cup C) \cap (B^C \cup C^C \cup A^C) = \\ \big((A \cap B) \cup (A \cap C)\big) \setminus (A \cap B \cap C) = \big((A \cap B) \cup (A \cap C)\big) \setminus \big((A \cap B) \cap (A \cap C)\big) = \\ (A \cap B)\Delta(A \cap C) = A \cdot B + A \cdot C. \end{aligned}$$

Per tant, hem vist que $(\mathcal{P}(X), \Delta, \cap)$ és un anell commutatiu ■

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

$$I + J := \{a + b : a \in I, b \in J\}$$
$$IJ := \left\{ \sum_{j<\infty} a_j b_j : a_j \in I, b_j \in J \right\}$$

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

$I + J$ és un ideal.
Sigui $\alpha \in A$ i $a \in I, b \in J$. Aleshores, $\alpha(a + b) = \alpha a + \alpha b$, de manera que, com que el primer és d'I i el segon és de J, aquest element pertany a $I + J$. A més, siguin $u, v \in I + J$, per tant $u = a_1 + b_1, v = a_2 + b_2$. Aleshores, $u + v = a_1 + b_1 + a_2 + b_2 = (a_1 + a_2) + (b_1 + b_2) \in I + J$.

IJ és un ideal.

Exemple en el que $I \cup J$ no és un ideal.
Per exemple, si estem a $A = \mathbb{Z}$, quan unim els ideals generats per 3 i per 4, tenim el següent: $7 = 3+4$, però $7 \notin (3)$ i $7 \notin (4)$, per tant, $7 \notin (3) \cup (4)$. Per tant, $(3) \cup (4)$ no és un ideal.

25. Els ideals $I_1, \ldots, I_k$ d'un anell $\mathbb{A}$ es diuen coprimers si $\sum_i I_i = \mathbb{A}$ i coprimers dos a dos si $I_i + I_j = \mathbb{A}$ per a tot $i \neq j$. Sigui $\phi : \mathbb{A} \to \prod_i \mathbb{A}/I_i$ l'homomorfisme que té per components les projeccions 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 $\prod_i I_i = \bigcap_i I_i$;
3. Si els I_i són coprimers dos a dos, aleshores, 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 tota i, i aquest element queda unívocament determinat llevat d'elements de $\prod_i I_i$;
4. ϕ és exhaustiva si, i només si, els I_i són coprimers dos a dos;
5. Si els I_i són coprimers dos a dos, aleshores $\mathbb{A}/\prod_i I_i \cong \prod_i \mathbb{A}/I_i$.

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

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

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

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

27. Determineu les unitats de l'anell $\mathbf{k}[[x]]$ de sèries de potències amb coeficients en un cos $\mathbf{k}$. Descriviu el cos de fraccions d'aquest anell.

28. Sigui $\mathbb{A}$ un anell commutatiu. Un element $e \in \mathbb{A}$ es diu *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 tots dos són ortogonals.

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

3. Demostreu que tot ideal principal d'$\mathbb{A}$ que sigui també un anell amb les operacions d'$\mathbb{A}$ 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 $\mathbb{A} \cong e_1\mathbb{A} \times e_2\mathbb{A}$.

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.

1.
Si e és idempotent, aleshores $(1-e)^2 = 1 + e^2 - 2e = 1 - e$. A més, $e(1-e) = e - e^2 = e - e = 0$.

2.
Siguin $x, y \in \mathbb{A}$, aleshores $ex, ey \in e\mathbb{A}$. La suma i el producte són els d'$\mathbb{A}$, i per tant mantenen les seves propietats. A més, $ex + ey = e(x+y) \in e\mathbb{A}$, i pel producte, $(ex)(ey) = e^2xy = exy \in e\mathbb{A}$. Observem que el neutre pel producte és e. Per tant, $e\mathbb{A}$ és un anell. Serà un subanell quan el neutre per la multiplicació d'$\mathbb{A}$ estigui a $e\mathbb{A}$, i això passarà quan $e \in \mathbb{A}^*$. Però llavors, $e\mathbb{A} = \mathbb{A}$.

3.
Sigui I un ideal principal que també és un anell. Això vol dir que conté neutre per la multiplicació. Suposem que aquest, al que anomenarem e_I, no és de $\mathbb{A}^*$, ja que en cas contrari, com hem vist a l'apartat anterior, necessàriament és $I = \mathbb{A}$. Com que és el neutre per la multiplicació, en particular passa que $e_I^2 = e_I e_I = e_I$. Segueix que I està generat per e_I necessàriament, ja que tots els elements d'I en són múltiples per la condició d'identitat multiplicativa en l'anell I.

4.
Segons la definició d'anell producte, les operacions es fan com:

- $(a_1, b_1) +_{\mathbb{A}_1 \times \mathbb{A}_2} (a_2, b_2) := (a_1 +_{\mathbb{A}_1} a_2, b_1 +_{\mathbb{A}_2} b_2)$
- $(a_1, b_1) *_{\mathbb{A}_1 \times \mathbb{A}_2} (a_2, b_2) := (a_1 *_{\mathbb{A}_1} a_2, b_1 *_{\mathbb{A}_2} b_2)$

Seguint d'aquí, és bastant evident que els elements $(1_{\mathbb{A}_1}, 0_{\mathbb{A}_2})$ i $(0_{\mathbb{A}_1}, 1_{\mathbb{A}_2})$ són idempotents i ortogonals. Vegem-ho:

$$\begin{aligned} (1,0)^2 &= (1*1, 0*0) = (1,0), \\ (0,1)^2 &= (0*0, 1*1) = (0,1), \\ (1,0)*(0,1) &= (1*0, 0*1) = (0,0) \equiv 0_{\mathbb{A}_1 \times \mathbb{A}_2}. \end{aligned}$$

Nota: també podríem haver vist la idempotència pensant que aquests elements representen la projecció sobre la primera i la segona component, respectivament.

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

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) $I \subseteq \mathrm{Rad}(I)$;
   (b) $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$;
   (c) $\mathrm{Rad}(I \cap J) = \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$;
   (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 un ideal primer, $\mathrm{Rad}(\mathfrak{p}) = \mathfrak{p}$.

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. $\mathbb{A}_\mathfrak{p} := \{\frac{a}{b} : a, b \in \mathbb{A}, b \notin \mathfrak{p}\} \subseteq \mathbb{K}$ 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'únic ideal maximal d'$\mathbb{A}_\mathfrak{p}$;
3. $\mathbb{A} = \bigcap_\mathfrak{m} \mathbb{A}_\mathfrak{m}$, on la intersecció es fa sobre tots els ideals maximals $\mathfrak{m}$ d'$\mathbb{A}$.