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, $IJ \subseteq \mathfrak{p} \iff I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$, per a tot parell d'ideals I, J.

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 ${}^{\mathbb{A}[X]}\!/_{I[X]} \cong \left({}^{\mathbb{A}}\!/_{I}\right)[X]$.

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.

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.