

Tema 1 (I): Anells

Problemes de classe

- 1.1. 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} .
- 1.2. 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} .
- 1.3. Demostreu que, donat $\alpha \in \mathbb{Q}$, el conjunt dels polinomis que s'anul·len en α és un ideal de $\mathbb{Q}[x]$.
- 1.4. Sigui \mathfrak{a} un ideal de l'anell A . Demostreu que $\text{Ann}(\mathfrak{a}) = \{a \in A : ax = 0 \forall x \in \mathfrak{a}\}$ és un ideal d' A . S'anomena *anul·lador d'* \mathfrak{a} .
- 1.5. 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 és un ideal. S'anomena *radical* de l'anell.
- 1.6. Demostreu que la suma d'un element nilpotent i una unitat d'un anell és una altra unitat.
- 1.7. Siguin $\zeta = e^{2\pi i/5}$ i $k \in \mathbb{Z}$. Considereu l'aplicació:

$$f : \mathbb{Z}[\zeta] \longrightarrow \mathbb{Z}[\zeta]$$

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

Demostreu que és un morfisme d'anells.

- 1.8. Siguin K un cos i $\alpha \in K$. Considereu l'aplicació:

$$\varphi_\alpha : K[x] \longrightarrow K$$

$$f \longmapsto \varphi_\alpha(f) = f(\alpha),$$

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

- 1.9. Volem veure que es pot racionalitzar totes les fraccions de la forma

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

- 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 $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.
- c) Concloeu que $\mathbb{Q}[\sqrt[3]{2}]$ és un cos.
- 1.10.** *Teorema xinès dels residus.* Dos ideals I, J d'un anell \mathbb{A} es diuen *coprimers* (o *comaximals*) si $I + J = \mathbb{A}$. Sigui $\phi: \mathbb{A} \rightarrow \mathbb{A}/I \times \mathbb{A}/J$ 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 $\mathbb{A}/IJ \simeq \mathbb{A}/I \times \mathbb{A}/J$;
- 1.11.** Demostreu que un ideal \mathfrak{p} és primer si, i només si, $IJ \subseteq \mathfrak{p} \Leftrightarrow I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$, per a tot parell d'ideals I, J .
- 1.12.** Sigui $I \subseteq \mathbb{A}$ un ideal d'un 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 $\mathbb{A}[X]/I[X] \simeq (\mathbb{A}/I)[X]$.
- 1.13.** 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.
- 1.14.** Demostreu que tot domini d'integritat finit és un cos. Deduïu que en un anell finit tot ideal primer és maximal.
- 1.15.** 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 $\alpha^n \beta^n = a^n$.
- 1.16.** Sigui d un enter lliure de quadrats amb $d \equiv 2, 3 \pmod{4}$. Demostreu que l'anell $\mathbb{Z}[\sqrt{-d}]$ no és factorial.
INDICACIÓ: Demostreu que 2 és irreductible però no és primer.

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

1. Els enters \mathbb{Z} , on $\delta(n)$ és el nombre de dígitos 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 $a_i \neq 0$.

1.18. *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 $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

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

1.20. 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 $u^2 \equiv -1 \pmod{p}$ (perquè 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 $\mathbb{Z}[i]$.

1.21. 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: $\pi_p = a + bi$ i $\bar{\pi}_p = a - bi$, que tenen norma p ; i
- 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 d'algun d'ells.

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

Problemes complementaris

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

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

$$I + J = \{a + b : a \in I, b \in J\},$$

$$IJ = A\langle ab : a \in I, b \in J \rangle,$$

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

1.25. Els ideals I_1, \dots, 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 $\phi: \mathbb{A} \rightarrow \prod \mathbb{A}/I_i$ l'homomorfisme que té per components les projeccions canòniques. Demostreu que:

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

1.26. *Teorema xinès a \mathbb{Z} .* Siguin n_1, \dots, 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, \dots, 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 $m_i \in \mathbb{Z}$.

1.27. 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.

1.28. 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 $\langle e \rangle = e\mathbb{A}$ és un anell amb les mateixes operacions de \mathbb{A} . En quin cas és un 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.

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

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

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

1. Comproveu que $\text{Rad}(I)$ és un ideal.
2. Calculeu $\text{Rad}(n\mathbb{Z})$ a l'anell \mathbb{Z} .
3. Demostreu que:
 - (a) $I \subseteq \text{Rad}(I)$;
 - (b) $\text{Rad}(\text{Rad}(I)) = \text{Rad}(I)$;
 - (c) $\text{Rad}(I \cap J) = \text{Rad}(I) \cap \text{Rad}(J)$;
 - (d) $\text{Rad}(I + J) = \text{Rad}(\text{Rad}(I) + \text{Rad}(J))$;
 - (e) $\text{Rad}(I^n) = \text{Rad}(I)$;
 - (f) $\text{Rad}(I) = \mathbb{A} \Leftrightarrow I = \mathbb{A}$;
 - (g) si \mathfrak{p} és primer, $\text{Rad}(\mathfrak{p}) = \mathfrak{p}$.

1.31. 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 \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 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} .

1.32. Sigui $d \in \mathbb{Z}$ un enter que no és un quadrat. Es considera l'anell

$$\mathbb{A}_d = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Per a cada element $\alpha = a + b\sqrt{d} \in \mathbb{A}_d$ es defineix $\bar{\alpha} = a - b\sqrt{d}$ (si $d < 0$ aquest element és el complex conjugat, però si $d > 0$ tots dos són reals). Es defineix $N : \mathbb{A}_d \rightarrow \mathbb{N}$ posant $N(\alpha) = |\alpha\bar{\alpha}| = |a^2 - db^2|$.

1. Justifiqueu que el conjugat està ben definit gràcies a que d no és un quadrat.
2. Comproveu que $N(\alpha\beta) = N(\alpha)N(\beta)$.
3. Demostreu que $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.
4. Demostreu que $\alpha \in \mathbb{A}_d^* \Leftrightarrow N(\alpha) = 1$.
5. Calculeu \mathbb{A}_d^* quan $d < 0$.

1.33. Sigui $d \in \mathbb{Z}$ amb $d \equiv 1 \pmod{4}$ un enter que no és un quadrat. Es considera l'anell

$$\mathbb{A}_w = \mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\} \subset \mathbb{C}, \quad \text{amb} \quad w = \frac{1}{2}(1 + \sqrt{d}).$$

Per a cada $\alpha = a + bw \in \mathbb{A}_w$ es defineix $\bar{\alpha} = a + b\bar{w}$, on $\bar{w} = \frac{1}{2}(1 - \sqrt{d})$. Es defineix $N(\alpha) = |\alpha\bar{\alpha}|$.

1. Comproveu que $N(\alpha\beta) = N(\alpha)N(\beta)$.
2. Expressen $N(a + bw)$ en termes de a i b .
3. Demostreu que $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.
4. Demostreu que $\alpha \in \mathbb{A}_w^* \Leftrightarrow N(\alpha) = 1$.
5. Calculeu \mathbb{A}_w^* quan $d < 0$.

INDICACIÓ: Pot ser útil observar que $4N(a + bw) = (2a + b)^2 - b^2d$.

1.34. Sigui $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subset \mathbb{R}$. Demostreu que

$$\mathbb{Z}[\sqrt{2}]^* = \{\pm(1 + \sqrt{2})^n : n \in \mathbb{Z}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

fent els passos següents:

1. comproveu que tots els $\pm(1 + \sqrt{2})^n$ són unitats;
2. vegeu que per a tota unitat $u \neq \pm 1$ exactament una de les quatre unitats $\pm u, \pm u^{-1}$ és > 1 , i caracteritzeu aquesta unitat en termes de a i b ;
3. demostreu que no hi ha cap unitat u amb $1 < u < 1 + \sqrt{2}$;
4. demostreu que tota unitat > 1 és una potència de $1 + \sqrt{2}$.

INDICACIÓ: ha d'estar entre dues potències consecutives de $1 + \sqrt{2}$.

1.35. Comproveu que l'anell $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ és un anell euclidià amb la norma definida com $N(a + b\sqrt{-2}) = a^2 + 2b^2$, argumentant de manera anàloga al cas dels enters de Gauss.

Vegeu que el mateix argument s'aplica a l'anell $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subset \mathbb{R}$ considerant ara la norma $N(a + b\sqrt{2}) = |a^2 - 2b^2|$.

1.36. Comproveu que els arguments del problema anterior no es poden aplicar a l'anell $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$, i vegeu que aquest anell no és factorial (i, per tant, tampoc pot ser Euclidià) trobant dues descomposicions diferents de 4 com a producte d'irreductibles no associats.

1.37. Sigui \mathbb{A} el conjunt de les matrius de la forma $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ a coeficients enters. Comproveu que \mathbb{A} és un subanell commutatiu de l'anell $\mathcal{M}_2(\mathbb{Z})$ i demostreu que, per a cada nombre primer p , els elements de \mathbb{A} tals que $a + b \equiv 0 \pmod{p}$ són un ideal maximal d'aquest anell.

- 1.38.** Sigui $\mathbb{A} = \{\frac{a}{b} \in \mathbb{Q} : b = 2^n, n \geq 0\}$. Demostreu que \mathbb{A} és un anell factorial, trobeu \mathbb{A}^* i digueu quins són els primers de \mathbb{A} .
- 1.39.** Sigui $\mathbb{A} = \{\frac{a}{b} \in \mathbb{Q} : b \text{ senar}\}$. Demostreu que \mathbb{A} és un anell factorial, trobeu \mathbb{A}^* i digueu quins són els primers de \mathbb{A} .
- 1.40.** Demostreu que en un anell $\mathbb{A} = \mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$ que és un producte cartesià de cossos tot ideal és principal.
- 1.41.** Sigui \mathbb{A} un domini d'ideals principals. Donats elements $a, b, c \in \mathbb{A}$,
- a) Doneu condicions necessàries i suficients per tal que l'equació $aX + bY = c$ tingui solució a l'anell \mathbb{A} ;
 - b) Doneu una parametrització de les solucions a partir d'una solució particular;
 - c) Expliqueu com es pot trobar una solució particular si l'anell és Euclidià.