Anells

Per defecte, només considerarem anells commutatius i unitaris.

Exercici 1 ($*$). Sigui A un anell. Proveu les propietats següents.

(a) Si $a \in A$ és una unitat (o sigui, un element invertible), aleshores a no és un divisor de zero.

(b) Si un ideal I de A conté una unitat, aleshores $I = A$.

(c) Si $a \in A$ i $u \in A$ és una unitat, aleshores $(ua) = (a)$.

(d) Si A és un domini d'integritat i a, $b \in A$, aleshores $(a) = (b)$ si, i només si, $b = au$ per a alguna unitat u de A.

Exercici 2. Caracteritzeu, en funció del nombre enter $m > 1$, quins són els elements invertibles i quins els divisors de zero de l'anell $\mathbb{Z}/m\mathbb{Z}$. Deduïu que $\mathbb{Z}/m\mathbb{Z}$ és un domini d'integritat si, i només si, $\mathbb{Z}/m\mathbb{Z}$ és un cos; si, i només si, m és un nombre primer.

Exercici 3. Demostreu que l'ideal $(2, X)$ de $\mathbb{Z}[X]$ no és principal.

Exercici 4 ($*$). Siguin A un anell, a, b, $d \in A$. Recordem que es diu que d és un màxim comú divisor de a i b si se satisfan les dues propietats

(1) $d \mid a$, $d \mid b$; i

(2) si $c \in A$ satisfà que $c \mid a$ i $c \mid b$, aleshores $c \mid d$.

(a) Proveu que si d és un màxim comú divisor de a i b, aleshores tenim la inclusió d'ideals $(a, b) \subseteq (d)$. Doneu un exemple en $\mathbb{Z}[X]$ on no hi hagi igualtat.

(b) Proveu que si A és un domini, aleshores dos màxims comuns divisors de a i b difereixen multiplicativament en una unitat.

(c) Proveu que si A és un domini d'ideals principals, llavors d és un màxim comú divisor de a i b si, i només si, $(a, b) = (d)$. Deduïu que en un domini d'ideals principals, sempre existeix el màxim comú divisor de dos elements.

Exercici 5. Siguin A un anell i f, $g \in A[X]$.

(a) Demostreu que si g és mònic, aleshores existeixen polinomis q, $r \in A[X]$ tals que $f = gq + r$, amb $r = 0$ o bé $gr(r) < gr(g)$. Demostreu que q i r són únics per a aquestes condicions. Una igualtat $f = gq + r$ s'anomena la *divisió entera* de f per g si $r = 0$ o bé $gr(r) < gr(g)$; els polinomis q i r s'anomenen el *quocient* i el *residu* de la divisió entera. Si el residu de la divisió entera de f per g és 0, es té que f és un múltiple de g i que g és un divisor de f.

(b) Doneu un exemple de no-unicitat i un de no-existència en el cas en què g no sigui mònic.

Exercici 6. Siguin I, J_1, J_2 ideals d'un anell A. Proveu que

(a) $I + (J_1 \cap J_2) \subseteq (I + J_1) \cap (I + J_2)$. Si $I \subseteq J_1$ o bé $I \subseteq J_2$ llavors tenim igualtat.

(b) $I \cap (J_1 + J_2) \supseteq (I \cap J_1) + (I \cap J_2)$ (Llei modular). Si $I \supseteq J_1$ o bé $I \supseteq J_2$ llavors hi ha igualtat.

Exercici 7. Siguin A un anell, $I \subseteq A$ un ideal. Es defineix el *radical* de I, $\mathrm{rad}(I)$, com el conjunt d'elements $x \in A$ tals que existeix $n \in \mathbb{N}$ tal que $x^n \in I$. Proveu que si I, J són ideals de A, llavors

(a) $\mathrm{rad}(I)$ és un ideal de A.

(b) Direm que I és un *ideal radical* si $\mathrm{rad}(I) = I$. Proveu que $\mathrm{rad}(I)$ és un ideal radical.

(c) $\mathrm{rad}(IJ) = \mathrm{rad}(I \cap J) = \mathrm{rad}(I) \cap \mathrm{rad}(J)$.

(d) $\mathrm{rad}(I + J) = \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$.

Exercici 8. Sigui $A = \mathbb{R}[X]$ i considerem $I = (X^2 + 1)$, $J = (X^2 + 3)$, ideals de A.

(a) Determineu un sistema de representants de A/I.

(b) Demostreu que $A/I \cong A/J$ i expliciteu un isomorfisme.

Exercici 9. Siguin A, B anells. En el producte cartesià $A \times B$ definim les operacions $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$.

(a) Proveu que $(A \times B, +, \cdot)$ és un anell i determineu quan és un domini d'integritat.

(b) Proveu que si $I \subseteq A$, $J \subseteq B$ són ideals, llavors $I \times J$ és un ideal de $A \times B$ i que

$$(A \times B)/(I \times J) \cong A/I \times B/J.$$

(c) Proveu que tot ideal de $A \times B$ és de la forma $I \times J$.

(d) Proveu que els únics ideals primers de $A \times B$ són els de la forma $I \times B$, amb $I \subseteq A$ primer, o bé els de la forma $A \times J$, amb $J \subseteq B$ primer.

(e) Demostreu el resultat que s'obté de (d) en substituir "primer" per "maximal".

Exercici 10 ($*$). Siguin $f : A \longrightarrow B$ un morfisme d'anells, I un ideal de A i J un ideal de B.

(a) Demostreu que $J^c := f^{-1}(J)$ és un ideal de A. L'anomenarem la *contracció* de J en A.

(b) Proveu amb un exemple que, en general, $f(I)$ no és un ideal de B. Definim l'*extensió* de I en B, que denotarem per I^e, com l'ideal de B generat per $f(I)$.

(c) Demostreu que $I \subseteq (I^e)^c$ i que $J \supseteq (J^c)^e$.

(d) Demostreu que $I^e = I^{ece}$ i que $J^c = J^{cec}$.

(e) Deduïu que existeix una bijecció entre el conjunt d'ideals contrets de A i el conjunt d'ideals extesos de B.

Exercici 11. (a) Siguin J un ideal de A i $\pi : A \to A/J$ el morfisme de pas al quocient. Proveu que $I^e = (I + J)/J$.

(b) Considerem el morfisme d'inclusió $i : A \to A[X]$. Proveu que $I^e = I[X]$ i que

$$\frac{A[X]}{I[X]} \cong \frac{A}{I}[X].$$

Exercici 12 ($*$). (a) Sigui $f : A \longrightarrow B$ un morfisme d'anells. Demostreu que si J és un ideal de B, llavors tenim un morfisme injectiu d'anells $A/f^{-1}(J) \longrightarrow B/J$.

(b) Siguin A un anell i I un ideal de A. Proveu que existeix una correspondència bijectiva entre el conjunt dels ideals de A/I i el conjunt dels ideals de A que contenen I. Proveu també que la bijecció es pot establir de manera que ideals primers es corresponguin amb ideals primers i ideals maximals amb ideals maximals.

Exercici 13. (a) Demostreu que la contracció d'un ideal primer és un ideal primer.

(b) Considerem la injecció de $\mathbb{Z}$ en $\mathbb{Z}[i]$. Proveu que l'extensió de l'ideal (2) no és un ideal primer.

(c) Siguin A un anell i $\mathfrak{p}$ un ideal primer. Proveu que l'extensió de $\mathfrak{p}$ en $A[X]$ és un ideal primer.

Exercici 14 (∗). Siguin r, s nombres enters ≥ 1 i sigui $d = \mathrm{mcd}(r, s)$.

(a) Proveu que $\mathrm{Hom}_{\mathrm{grups}}\big(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/s\mathbb{Z}\big) \cong \mathbb{Z}/d\mathbb{Z}$.

(b) Què és $\mathrm{Hom}_{\mathrm{anells}}\big(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/s\mathbb{Z}\big)$?

Exercici 15. Sigui A un anell en el qual per a cada element $y \in A$ se satisfà una igualtat $y^n = y$ per a algun nombre enter $n \geq 2$ (que depèn de y). Proveu que tot ideal primer és maximal.

Exercici 16. Proveu que tot domini d'integritat finit és un cos.

Exercici 17 (∗). Sigui A un anell. Demostreu que si A té un nombre finit $n \geq 2$ de divisors de zero, aleshores A és finit i $card(A) \leq n^2$. (*Nota:* $0 \in z(A)$, on $z(A)$ denota el conjunt de divisors de zero de A.)

Exercici 18 (∗). Sigui A un anell commutatiu finit en el qual no suposem en principi que hi hagi element unitat. Demostreu que si en A hi ha un element no divisor de zero, llavors A conté un element unitat. Sabríeu donar-ne un contraexemple en el cas A no finit?

Exercici 19 (∗). Sigui A un anell. Utilitzeu l'axioma de Zorn per a demostrar que el conjunt d'ideals primers de A admet elements minimals.

Exercici 20 (∗). Sigui A un anell. Es diu que un element $x \in A$ és *nilpotent* si $x^n = 0$ per a algun nombre enter positiu n. Proveu que

(a) Si x és nilpotent, aleshores $1 - x$ és invertible.

(b) El conjunt d'elements nilpotents de A és un ideal radical, que notem $\eta(A)$ i s'anomena nilradical de A.

(c) $\eta(A)$ està contingut dins de tots els ideals primers de A.

(d) $\eta(A)$ és la intersecció de tots els ideals primers de A. (*Indicació:* Sigui $y \notin \eta(A)$ i definim Σ com el conjunt d'ideals $K \subseteq A$ tals que $y^n \notin K$ per a tot $n > 0$. Vegeu que Σ té un element maximal i que aquest és un ideal primer.)

(e) Sigui J un ideal de A. Proveu que el radical de J és la intersecció de tots els ideals primers de A que contenen J.

Exercici 21 (∗). Siguin J, K dos ideals d'un anell A.

(a) Vegeu que $(J + K) \cdot (J \cap K) \subseteq JK$.

(b) Demostreu que si J, K són ideal primers entre si (comaximals) llavors $J \cap K = JK$.

(c) Siguin $I_1, \ldots, I_n \subseteq A$ ideals primers entre si dos a dos. Proveu que $\displaystyle\prod_{j=1}^{n} I_j = \bigcap_{j=1}^{n} I_j$.

(d) Donats $I_1, \dots, I_n \subseteq A$ ideals, considerem l'homomorfisme d'anells

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & \prod_{j=1}^{n} A/I_j \\ & x & \longrightarrow & (\bar{x}, \dots, \bar{x}). \end{array}$$

Demostreu que si $I_1, \dots, I_n$ són primers entre si dos a dos, llavors φ és exhaustiva. (Aquesta és una versió de l'anomenat teorema xinès del residu.) Calculeu Kerφ en qualsevol cas. (*Indicació:* trobeu una antiimatge de $(1, 0, \dots, 0)$.)

(e) Demostreu que $\mathrm{mcd}(r, s) = 1$ implica que $\mathbb{Z}/rs\mathbb{Z} \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$.

Exercici 22 ($*$). Sigui A un anell commutatiu tal que $a^2 = a$ per a tot $a \in A$, i sigui $\mathrm{Max}(A)$ el conjunt d'ideals maximals de A. Demostreu que:

(a) Tot ideal primer $\mathfrak{p}$ de A és maximal i $A/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$.

(b) $\displaystyle\bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m} = 0.$

(c) Per a cada $\mathfrak{m} \in \mathrm{Max}(A)$, sigui $\varphi_{\mathfrak{m}} : A \longrightarrow A/\mathfrak{m}$ el morfisme de pas al quocient. Proveu que

$$\begin{array}{rcc} \Phi : A & \longrightarrow & \prod_{\mathfrak{m} \in Max(A)} A/\mathfrak{m} \\ a & \longmapsto & (\varphi_{\mathfrak{m}}(a)) \end{array}$$

és un morfisme injectiu d'anells, i que si $\mathrm{Max}(A)$ és finit, llavors Φ és un isomorfisme. Deduïu que A és finit si, i només si, $\mathrm{Max}(A)$ és un conjunt finit.

(d) Se satisfà que $2a = 0$ per a tot $a \in A$, i que tot ideal finitament generat de A és principal. (*Indicació:* $(a, b) = (a + b + ab)$.)

Exercici 23. Sigui $A[X]$ l'anell de polinomis en una indeterminada sobre l'anell A. Prenem $f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in A[X]$ un polinomi de grau n, amb $a_0, \dots, a_n \in A$. Demostreu que

(a) f és una unitat en $A[X]$ si, i només si, a_0 és una unitat en A i $a_1, \dots, a_n$ són nilpotents.

(b) f és nilpotent si, i només si, $a_0, a_1, \dots, a_n$ són nilpotents.

(c) f és divisor de zero en $A[X]$ si, i només si, existeix $a \in A - \{0\}$ tal que $af = 0$. (*Indicació:* es pot començar per prendre un polinomi g de grau mínim per al qual se satisfaci que $fg = 0$).

Exercici 24. Sigui $A[[X]]$ l'anell de sèries de potències de coeficients en A. Prenem $f = \sum_{i \geq 0} a_i X^i \in A[[X]]$, $a_i \in A$. Demostreu que

(a) f és una unitat en $A[[X]]$ si, i només si, a_0 és una unitat de A.

(b) Si f és nilpotent, aleshores a_i és nilpotent, per a tot $i \in \mathbb{N}$. És cert el recíproc?

(c) Sigui k un cos. Proveu que els ideals no nuls de $k[[X]]$ són de la forma (X^i).

Exercici 25. Sigui A un anell commutatiu.

(a) Demostreu que $A - A^*$ (el conjunt complementari de les unitats) és un ideal si, i només si, A té un únic ideal maximal.

(b) Demostreu que A té un únic ideal primer si, i només si, tot element de A és invertible o nilpotent.

Exercici 26. Sigui A un domini d'integritat. Proveu que l'anell de polinomis $A[X]$ és un domini d'ideals principals si, i només si, A és un cos.

Exercici 27 ($*$). Siguin A un domini d'ideals principals, B un domini d'integritat, i $f : A \to B$ un morfisme d'anells exhaustiu. Demostreu que o bé B és un cos, o bé f és un isomorfisme.

Exercici 28. Sigui A un domini d'integritat amb la propietat que donada una cadena descendent d'ideals $I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq \ldots$, existeix un nombre enter m tal que $I_n = I_m$ per a tot $n \geq m$. Demostreu que A és un cos.

Exercici 29 ($*$). Sigui A un domini. Considerem els parells ordenats (a, b) on $a, b \in A$ i $b \neq 0$, amb la relació següent:

$$(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0.$$

(a) Comproveu que $\sim$ és una relació d'equivalència. Denotem per $\frac{a}{b}$ la classe d'equivalència de (a, b) i K el conjunt de classes d'equivalència. En K, definim les operacions següents:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

amb $a, b, c, d \in A$, $b \neq 0$ i $d \neq 0$. Comproveu que estan ben definides.

(ii) Demostreu que K és un cos. El cos K s'anomena el *cos de fraccions* de A.

(iii) Demostreu que l'aplicació

$$\begin{array}{ccc} A & \longrightarrow & K \\ a & \longmapsto & \dfrac{a}{1} \end{array}$$

és un morfisme d'anells injectiu.

Exercici 30 ($*$). Siguin A un domini d'integritat i K el seu cos de fraccions. Demostreu que se satisfà la propietat següent:
Si $f : A \longrightarrow B$ és un morfisme d'anells tal que $f(a) \in B^*$ per a tot $a \in A - \{0\}$, aleshores f s'estén de manera única a un morfisme d'anells $\widetilde{f} : K \longrightarrow B$.
Deduïu que K és el més petit de tots els cossos que contenen A com a subanell.

Exercici 31. Determineu quins dels anells següents són dominis d'integritat i doneu-ne els cossos de fraccions corresponents:
(a) $\mathbb{Z}[X]/(X)$; (b) $\mathbb{Z}[X]/(X^2)$; (c) $\mathbb{Z}/n\mathbb{Z}[X]$; (d) $\mathbb{Z}[X]/(p, X)$, amb $p \in \mathbb{Z}$ primer.

Exercici 32. Demostreu que la característica d'un domini d'integritat és o bé zero o bé un nombre primer. Deduïu que tot cos conté un subcòs isomorf a $\mathbb{Q}$ o a $\mathbb{Z}/p\mathbb{Z}$, per a un cert nombre primer p.

Exercici 33. Per a un nombre enter lliure de quadrats, d, considerem $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ i l'aplicació $N : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}$ definida per $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$, per a $a, b \in \mathbb{Z}$.

(a) Demostreu que $\mathbb{Z}[\sqrt{d}]$ és un anell.

(b) Demostreu que l'aplicació N és multiplicativa; és a dir, que $N(\alpha\beta) = N(\alpha)N(\beta)$, per a tot α, $\beta \in \mathbb{Z}[\sqrt{d}]$. Aquesta aplicació es coneix amb el nom de *norma*.

(c) Demostreu que $\alpha \in \mathbb{Z}[\sqrt{d}]$ és una unitat si, i només si, $N(\alpha) = \pm 1$.

Exercici 34. Considerem l'anell $\mathbb{Z}[i] := \{a + b\,i : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ i la seva norma $N(a + b\,i) = a^2 + b^2$, $a, b \in \mathbb{Z}$.

(a) Demostreu que per a tota parella d'elements $x, y \in \mathbb{Z}[i]$, $y \neq 0$, existeixen q, $r \in \mathbb{Z}[i]$ tals que $x = qy + r$, amb $r = 0$ o bé $N(r) < N(y)$.

(b) Deduïu que $\mathbb{Z}[i]$ és un domini d'ideals principals.

Exercici 35. Considerem l'anell $\mathbb{Z}\left[\sqrt{-2}\,\right] := \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ i la seva norma $N(a + b\sqrt{-2}) = a^2 + 2b^2$, a, $b \in \mathbb{Z}$. Proveu que $\mathbb{Z}\left[\sqrt{-2}\,\right]$ és un domini d'ideals principals.

Exercici 36. Considerem l'anell $\mathbb{Z}\left[\sqrt{-3}\,\right] \subseteq \mathbb{C}$.

(a) Trobeu les unitats d'aquest anell.

(b) Proveu que 2, $1 + 2\sqrt{-3}$ i $1 + \sqrt{-3}$ són elements irreductibles. És $\mathbb{Z}\left[\sqrt{-3}\right]$ un domini de factorització única?

(c) Demostreu que l'ideal $(7, 2 + \sqrt{-3}\,)$ és primer.

Exercici 37. L'anell $\mathbb{Z}\left[\sqrt{2}\,\right]$ és un domini de factorització única.

(a) Comproveu que $23 = (3 + 4\sqrt{2})(-3 + 4\sqrt{2}) = (11 + 7\sqrt{2})(11 - 7\sqrt{2})$. Contradiu aquesta igualtat el fet que $\mathbb{Z}\left[\sqrt{2}\,\right]$ sigui domini de factorització única?

(b) Proveu que $\mathbb{Z}\left[\sqrt{2}\,\right]$ té infinites unitats.

Exercici 38. Considereu el domini d'integritat $\mathbb{Z}[\sqrt{-6}]$.

(a) Demostreu que $\mathbb{Z}[\sqrt{-6}]^* = \{+1, -1\}$ i que, en aquest anell, no hi ha elements de norma 5.

(b) És $1 + 2\sqrt{-6}$ un element irreductible?

(c) És $1 + 2\sqrt{-6}$ un element primer?

(d) És $\mathbb{Z}[\sqrt{-6}]$ un domini de factorització única?

Exercici 39 ($*$). Siguin d un nombre enter lliure de quadrats i $A = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) A partir de la igualtat $(d + \sqrt{d})(d - \sqrt{d}) = d(d - 1)$, proveu que 2 no és un element primer de l'anell A. Deduïu que, si A és un domini de factorització única, 2 no és irreductible a A.

(b) Demostreu que, si d és negatiu, A és un domini de factorització única si, i només si, $d = -1$ o $d = -2$.

(c) Proveu que 5 és irreductible a $\mathbb{Z}\left[\sqrt{-2}\,\right]$ i que l'anell quocient $\mathbb{Z}\left[\sqrt{-2}\,\right]/(5)$ té un subcòs isomorf a $\mathbb{Z}/5\mathbb{Z}$.

Exercici 40. Es considera l'anell $\mathbb{Z}[\sqrt{d}\,]$, on $d \in \mathbb{Z}$ no és un quadrat perfecte. Sigui $x + \sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$, $x \in \mathbb{Z}$, un element de norma $N(x + \sqrt{d}) = n$.

(a) Demostreu que l'aplicació

$$\begin{array}{rccc} f: & \mathbb{Z}[\sqrt{d}\,] & \to & \mathbb{Z}/n\mathbb{Z} \\ & a + b\sqrt{d} & \mapsto & \overline{a - xb} \end{array}$$

és un morfisme d'anells que factoritza en un isomorfisme $\overline{f} : \mathbb{Z}[\sqrt{d}\,]/(x + \sqrt{d}) \simeq \mathbb{Z}/n\mathbb{Z}$.

Sigui $d = 15$ i considerem l'anell $\mathbb{Z}\left[\sqrt{15}\,\right]$.

(b) Esbrineu si els elements $1+\sqrt{15}$, $2+\sqrt{15}$ són primers. Són irreductibles?

Indicació: Demostreu que l'equació $z^2 = \pm 2$ no té solucions en $\mathbb{Z}/5\mathbb{Z}$.

(c) És $\mathbb{Z}\left[\sqrt{15}\,\right]$ un domini de factorització única?