Estructures Algebraiques

Cinc Cèntims d'Anells

Mario Vilar

2 de gener de 2023

Índex

1 Anells

Definició 1.1 (Anell). És un conjunt A no buit dotat de dues operacions internes, la suma i el producte, tals que:

- la suma és associativa, commutativa, amb element neutre 0 i oposat (és grup abelià amb la suma),
- el producte és associatiu ($(ab)c = a(bc)$) i distributiu ($a(b+c) = ab + ac$ i $(b+ca) = ba + ca$) respecte de la suma.

Definició 1.2 (Element invertible). Un element a d'un anell amb unitat A es diu invertible si té invers a A. Si a és element invertible de l'anell A es compleix $ab = 0 \implies b = 0$, ja que $ab = 0 \implies a^{-1}(ab) = a^{-1} \cdot 0 = 0$, i d'altra banda, $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$.

$$A^* = \{a \in A \mid a \text{ és invertible}\}, \ A^* \text{ és grup amb el producte d'} A. \tag{1.1}$$

Es diu que A^* és grup multiplicatiu de l'anell A.

Definició 1.3 (Subanell). Sigui A un anell. Un subanell d'A és un subconjunt no buit B d'A tal que:

- $(B, +)$ és subgrup d'$(A, +)$.
- B és tancat respecte del producte d'A: $b, b' \in B \implies bb' \in B$.

A partir d'ara, anell ≡ anell commutatiu i unitari

Definició 1.4 (Divisor de zero). Un element a d'un anell A, $a \neq 0$, es diu divisor de zero si existeix $b \in A$, $b \neq 0$ tal que $ab = 0$.

Definició 1.5 (Domini d'integritat). Sigui A un anell. Diem que A és un domini d'integritat si no té divisors de zero. Si A és domini d'integritat i prenem $a, b \in A$ tals que $ab = 0$, aleshores $a = 0$ o bé $b = 0$ (o, per contrarrecíproc, $a \neq 0, b \neq 0 \implies ab \neq 0$).

Proposició 1.6. *Si A és domini d'integritat, aleshores $A[X]$ és domini d'integritat.*

Definició 1.7 (Ideal). Donat un anell A, un ideal d'A és un subconjunt I d'A tal que

1. $(I, +)$ és subgrup d'$(A, +)$.
2. $\forall a \in A, \forall x \in I$, aleshores $ax \in I$.

Definició 1.8 (Domini d'ideals principals). Si A és domini d'integritat i tots els ideals d'A són principals, diem que A és un domini d'ideals principals (DIP).

Proposició 1.9. *Si $\mathbb{K}$ és cos, l'anell $\mathbb{K}[X]$ és domini d'ideals principals.*

Definició 1.10 (Divisor). Si A és un anell, amb $a, b \in A$, diem que a divideix b si existeix $c \in A$ tal que $b = ac$. Ho denotem per $a \mid b$. Clarament, $a \mid b \iff b \in (a)$.

Definició 1.11 (Ideal suma). Donats dos ideals I, J de l'anell A, posem $I + J$ el conjunt dels elements de l'anell A que són suma d'un element d'I i un element de J. Clarament, $I + J$ és un ideal d'A i és l'ideal d'A generat pel conjunt $I \cup J$. Anomenem $I + J$ *l'ideal suma* de I i J. Més generalment, si $\{I_j\}_{j\in\mathcal{J}}$ és una família d'ideals d'A:

$$\text{L'ideal suma } \sum_{j\in\mathcal{J}} I_j \text{ és l'ideal generat per } \bigcup_{j\in\mathcal{J}} I_j. \tag{1.2}$$

Definició 1.12 (Ideal producte). Donats dos ideals I, J de l'anell A, posem IJ el conjunt dels elements de l'anell A que són producte d'un element d'I i un element de J.

$$IJ = \{a_1b_1 + \cdots + a_kb_k \mid k \in \mathbb{N}; a_i \in I, b_i \in J; 1 \leq i \leq k\}. \tag{1.3}$$

Anomenem IJ *l'ideal producte* de I i J. Més generalment, si $I_1, \ldots, I_k$ són ideals d'A, posem $I_1 \cdots I_k$ l'ideal generat pel conjunt dels elements de l'anell A que són producte d'un element d'I_1, un element de I_2, i així fins un element d'I_k. Diem que $I_1 \cdots I_k$ és l'ideal producte dels ideals $I_1, \ldots, I_k$.
Està format pels elements de l'anell A que són sumes finites d'elements de la forma $a_1 \cdots a_k$, amb $a_i \in I$ i $1 \leq i \leq k$. Clarament, $I_1 \cdots I_k \subset I_1 \cap \cdots \cap I_k$. Si I és un ideal, posarem I^k per denotar el producte de l'ideal I amb ell mateix k vegades.

Proposició 1.13 (Anell quocient). *Sigui A un anell i I un ideal d'aquest anell A. Aleshores, A/I és anell. En particular, direm que A/I és l'anell quocient d'A per I.*

Proposició 1.14.

1. *Si A és un anell de característica k, existeix un únic morfisme de $\mathbb{Z}/(k)$ en A i aquest morfisme és un monomorfisme.*
2. *Si A és un anell i k un enter, $k > 0$, es compleix* car $A = k \iff$ *k és el menor enter positiu tal que $ka = 0$, per a tot $a \in A$.*
3. *Si A és domini d'integritat, la característica de A és 0 bé o o bé un nombre primer.*

2 Morfismes d'anells

Definició 2.1 (Morfisme d'anells). Si A, A' són anells, una aplicació $f : A \longrightarrow A'$ és morfisme d'anells si compleix:

$$f(a + b) = f(a) + f(b) \text{ i } f(ab) = f(a)f(b), \tag{2.1}$$

per a tot parell d'elements a, b d'A, i $f(1_A) = 1_{A'}$. Notem que si $f : A \longrightarrow A'$ és morfisme d'anells, aleshores f és morfisme de grups d'$(A,+)$ en $(A',+)$.

Definició 2.2 (Morfisme injectiu). Si $f : A \longrightarrow A'$ és morfisme d'anells, el nucli de f és $\ker(f) = \{a \in A \mid f(a) = 0_{A'}\}$; és a dir, el nucli de f com a morfisme de grups. Tenim, doncs, que f és un morfisme injectiu si, i només si, $\ker(f) = \{0_A\}$.

Proposició 2.3. *Si $f : A \longrightarrow A'$ és morfisme d'anells,* $\ker(f)$ *és ideal d'A i* $\mathrm{im}(f)$ *és subanell d'A'.*

3
Teorema d'isomorfia

Definició 3.1 (f factoritza a través d'un anell quocient). Siguin A, A' anells, $f : A \longrightarrow A'$ un morfisme d'anells, I un ideal d'A i $\pi : A \longrightarrow A/I$ si existeix un morfisme d'anells $\overline{f} : A/I \longrightarrow A'$ tal que $f = \overline{f} \circ \pi$, és a dir, que faci commutatiu el diagrama:

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"] & & A' \\
& A/I \arrow[ur, "\overline{f}"] &
\end{tikzcd}$$

Figura 1: Diagrama de factorització a través del quocient

Proposició 3.2. *Siguin A, A' anells, $f : A \longrightarrow A'$ un morfisme d'anells, I un ideal propi d'A i $\pi : A \longrightarrow A/I$ el morfisme de pas al quocient. Aleshores, f factoritza a través d'A/I si, i només si, $I \subset$* $\ker(f)$.

Demostració. Hem de seguir la demostració que vam donar per a la factorització a través del quocient (per a grups), solament ens queda veure que, si existeix $\overline{f} : A/I \longrightarrow A'$ tal que $f = \overline{f} \circ \pi$, aleshores $\overline{f}$ és l'únic morfisme d'anells que compleix $f = \overline{f} \circ \pi$. Com $\overline{f}([a]) = f(a)$, per a $a \in A$:

$$\overline{f}(1_{A/I}) = \overline{f}([1_A]) = f(1_A) = 1_B \text{ i } \overline{f}([a][b]) = \overline{f}([ab]) = f(ab) = f(a)f(b) = \overline{f}([a])\overline{f}([b]). \quad (3.1)$$

Amb $\overline{f}([1_A]) = 1_B$ hem trobat l'existència de neutre i $\overline{f}([ab]) = \overline{f}([a])\overline{f}([b])$ tenim morfisme de grups. ■

Teorema 3.3 (Primer teorema d'isomorfia per a anells). *Si A, A' són anells i $f : A \longrightarrow A'$ és un morfisme d'anells, aleshores f factoritza a través d'$A/$*$\ker(f)$ *i tenim $f = i \circ \tilde{f} \circ \pi$, amb $\tilde{f}$ isomorfisme d'anells d'$A/$*$\ker(f)$ *en* $\mathrm{im}(f)$, *i la inclusió d'*$\mathrm{im}(f)$ *en A', $\pi : A \longrightarrow A/$*$\ker(f)$ *el morfisme de pas al quocient. Tenim, doncs, un diagrama commutatiu:*

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[d, "\pi"'] & & A' \\
A/\ker(f) \arrow[urr, "\overline{f}"] \arrow[rr, "\tilde{f}"] & & \mathrm{im}(f) \arrow[u, "i"']
\end{tikzcd}$$

Figura 2: Diagrama commutatiu del primer teorema d'isomorfis per a anells

Demostració. La proposició anterior ens dona que existeix un morfisme d'anells $\overline{f} : A/\ker(f) \longrightarrow A'$ tal que $f = \overline{f} \circ \pi$. A més, $\overline{f}$ és injectiu, i $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$. Per tant, $\overline{f} = i \circ \tilde{f}$ amb $\tilde{f} : A/\ker(f) \longrightarrow \mathrm{im}(f)$ isomorfisme d'anells definit per $\tilde{f}([a]) = \overline{f}([a])$. ■

4

Ideals primers i maximals

Definició 4.1 (Ideal primer). Sigui A un anell, un ideal I d'A es diu ideal primer si és ideal propi ($I \neq A$) i es compleix el següent per a tot $a, b \in A$: $ab \in I \implies a \in I$ o bé $b \in I$.

Proposició 4.2. *Sigui I un ideal de l'anell A. Aleshores, I és primer si, i només si, A/I és domini d'integritat.*

Demostració. D'entrada, ja sabem que $a \in I \iff [a] = [0]$.

- $\Rightarrow$ Si $[a][b] = [0]$, per definició de quocient tenim que $[ab] = [0]$ i això implica que $ab \in I$. Per tant, $a \in I$ o bé $b \in I$; és a dir, $[a] = [0]$ o bé $[b] = [0]$.
- $\Leftarrow$ Sigui ara $ab \in I$. Aleshores, $[ab] = [a][b] = [0]$ en A/I. Per tant, $[a] = [0]$ (de manera que $a \in I$) o bé $[b] = [0]$ (de manera que $b \in I$).

■

Definició 4.3 (Ideal maximal). Un ideal I d'un anell A es diu maximal si és ideal propi i no existeix cap ideal J d'A tal que $I \subsetneq J \subsetneq A$. En altres paraules:

$$\left.\begin{array}{r} I \subsetneq J \implies J = A \\ I \subset J \subsetneq A \implies J = I \end{array}\right\} \iff I \text{ és maximal.} \tag{4.1}$$

Proposició 4.4. *Sigui I un ideal d'un anell A. Aleshores, I és maximal si, i només si, A/I és un cos. En particular, tot ideal maximal és primer.*

Demostració.

- $\Rightarrow$ Suposem I maximal. Sigui $\overline{a} \in A/I$, tal que $\overline{a} \neq \overline{0}$. Així, $a \notin I$ i $I \subsetneq I + (a) \subset A \implies I + (a) = A$ pel fet de ser I un ideal maximal. En particular, podem escriure 1 com una combinació lineal d'un element d'I i l'ideal generat per l'element a, (a): $1 = x + \lambda a$, amb $x \in I, \lambda \in A$. Prenent classes mòdul I, obtenim:

$$\overline{1} = \overline{x} + \overline{\lambda}\overline{a} \implies \overline{1} = \overline{a} \cdot \overline{\lambda} \implies \overline{\lambda} \text{ és invers d'} \overline{a} \text{ en } A/I. \tag{4.2}$$

Això passa perquè $\overline{x} = \overline{0}$, ja que $x \in I$. Per tant, $\overline{a}$ és invertible i hem provat que tot element no nul d'A/I és invertible i, per tant, A/I és un cos.

$\boxed{\Leftarrow}$ Sigui, ara, A/I un cos ($I \subsetneq J$) i J un ideal d'A tal que $I \subsetneq J \subset A$. Existeix $a \in J$ amb $a \notin I$ tal que $\overline{a} \neq \overline{0}$ en A/I. Pel fet que A/I és un cos, existeix $\overline{b} \in A/I$ tal que $\overline{a}\overline{b} = \overline{1}$ ($\overline{a}$ és invertible). Ens queda:

$$ab - 1 = x \iff 1 = ab - x \implies 1 \in J \implies J = A. \tag{4.3}$$

Hem usat que $x \in I$, $I \subset J$ i $ab - x \in J$.

Sigui I un ideal maximal d'A. Com ja hem vist, se segueix que A/I és cos i, per tant, que A/I és domini d'integritat. Si A/I és domini d'integritat, I és primer. ■

Lema 4.5 (Lema de Zorn). *Sigui S un conjunt no buit ordenat inductivament. Aleshores, existeix un element maximal a S.*

Proposició 4.6. *Sigui A un anell i $\mathfrak{a}$ un ideal propi d'A, és a dir, un ideal d'A diferent d'A. Aleshores, existeix un ideal maximal d'A que conté $\mathfrak{a}$.*

Demostració. Considerem el conjunt S dels ideals propis de l'anell A que contenen $\mathfrak{a}$, és a dir:

$$S = \{I \mid \mathfrak{a} \subset I,\ I \text{ ideal propi d'}A\}. \tag{4.4}$$

El conjunt S és no buit, ja que conté l'ideal $\mathfrak{a}$ i està ordenat per la inclusió. Volem veure que S està ordenat inductivament. Sigui T un subconjunt de S totalment ordenat, és a dir tal que per a tot parell I_1, I_2 d'elements de T, tenim $I_1 \subset I_2$ o $I_2 \subset I_1$. Volem veure que T té cota superior, és a dir que existeix un ideal J propi de A contenint a tal que $I \subset J$, per a tot $I \in T$. Sigui J la reunió de tots els ideals de T, és a dir:

$$J = \bigcup_{I \in T} I \tag{4.5}$$

Vegem que J és ideal de A:

1. Si $a_1, a_2 \in J$, tenim $a_1 \in I_1, a_2 \in I_2$, per certs elements I_1, I_2 de T. Com T està totalment ordenat, podem comparar els ideals; tenim $I_1 \subset I_2$ o $I_2 \subset I_1$, per tant:
   - $a_1, a_2 \in I_2$, que implica $a_1 - a_2 \in I_2$, o bé
   - $a_1, a_2 \in I_1$, que implica $a_1 - a_2 \in I_1$.
2. En qualsevol cas, $a_1 - a_2 \in J$. Si $a \in J, b \in A$, tenim $a \in I$, per un cert I de T; per tant, $ba \in I \subset J$. Clarament J conté $\mathfrak{a}$.

Vegem ara $J \subsetneq A$, és a dir, que J és un ideal propi. Raonem per reducció a l'absurd: si fos $J = A$, tindríem $1 \in J$, per tant $1 \in I$, per a algun I de T, que donaria $I = A$, que contradiu la definició de S (el conjunt dels ideals propis també és propi). Hem provat doncs que J és cota superior de T.

Aplicant el lema de Zorn, obtenim que S té un element maximal, és a dir que A té un ideal propi M contenint $\mathfrak{a}$ tal que si I és ideal propi de A i $M \subset I$, es té $M = I$. Per tant M és ideal maximal de A. ■

Corol·lari 4.7. *Tot anell té al menys un ideal maximal.*

5 Cos de fraccions d'un domini

Sigui A un domini d'integritat. En el conjunt $A\times(A\setminus\{0\})$, definim $(a,b)\sim(a',b') \iff ab'=a'b$, on $\sim$ és una relació d'equivalència. La prova que és, en efecte, d'equivalència, és prou senzilla. Solament indicarem la transitivitat:

$$\left.\begin{aligned}(a,b)\sim(a',b') &\iff ab'=a'b\\ (a',b')\sim(a'',b'') &\iff a'b''=a''b'\end{aligned}\right\} \implies (ab'')b'=a'bb''=a''b'b=(a''b)b' \\ \implies ab''=a''b \iff (a,b)\sim(a'',b''). \tag{5.1}$$

en l'última implicació hem hagut d'usar que A és un domini d'integritat, ja que hem aplicat la propietat cancel·lativa.

Definició 5.1 (Cos de fraccions d'A). Sigui $\mathbb{K}(A)$ el conjunt quocient de $A\times(A\setminus\{0\})$ per la relació d'equivalència $\sim$. Posem $\frac{a}{b}$ la classe d'(a,b) de manera que:

$$\frac{a}{b}=\frac{a'}{b'} \iff ab'=a'b. \tag{5.2}$$

Volem definir a $\mathbb{K}(A)$ una suma i un producte. Definim la suma per:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}. \tag{5.3}$$

Volem veure que no depèn del representant. Si $\frac{a}{b}=\frac{a'}{b'}$ i $\frac{c}{d}=\frac{c'}{d'}$, tenim que $ab'=a'b$ i $cd'=c'd$; per tant, $(ad+bc)b'd'=(a'd'+c'b')bd$ i

$$a'd'bd+c'b'bd=adb'd'+bb'cd' \implies \frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}. \tag{5.4}$$

Per a la suma tenim que el neutre és $\frac{0}{b}$ i l'oposat, $-\frac{a}{b}=\frac{-a}{b}$. Per tant, la suma no depèn del representant i està ben definida. Pel que fa al producte, el definim per:

$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}. \tag{5.5}$$

Hem de veure que no depèn del representant. En efecte, si $\frac{a}{b}=\frac{a'}{b'}$ i $\frac{c}{d}=\frac{c'}{d'}$, tenim $ab'=a'b$ o $cd'=c'd$ i, per tant:

$$(ac)(b'd')=(ab')(cd')=(a'b)(c'd)=(a'c')(bd) \implies \frac{ac}{bd}=\frac{a'c'}{b'd'}. \tag{5.6}$$

Clarament, $\frac{1}{1}$ és el neutre pel producte. Per tant, $\mathbb{K}(A)$ és anell amb aquestes suma i producte. Tot element no nul de $\mathbb{K}(A)$ té inversa, ja que per a $\frac{a}{b}\neq 0_{\mathbb{K}_A}$ tenim que $a\neq 0$ i $\frac{b}{a}\frac{a}{b}=\frac{ab}{ab}=1_{\mathbb{K}(A)}$. Per tant, $\mathbb{K}(A)$ és un cos que anomenem *cos de fraccions d'A*.

Proposició 5.2. *Siguin A un domini d'integritat, L un cos i $g : A \longrightarrow L$ un monomorfisme d'anells. Aleshores, existeix un únic monomorfisme de cossos $h : \mathbb{K}(A) \longrightarrow L$ tal que $g = h \circ i$; és a dir, tal que el diagrama:*

$$\begin{tikzcd}
A \arrow[rr, "g"] \arrow[dr, "i"'] & & L \\
& \mathbb{K}(A) \arrow[ur, "h"'] &
\end{tikzcd}$$

Figura 3: Diagrama de 5.2

commuta.

Demostració. Si h ha de complir que $g = h \circ i$, ha de ser $h(\frac{a}{1}) = h(i(a)) = g(a)$, per a tot $a \in A$. Per tant, si $b \in A \setminus \{0\}$, ha de ser:

$$\begin{gathered} h\left(\frac{1}{b}\right) = h\left(\left(\frac{b}{1}\right)^{-1}\right) = g(b)^{-1} \\ h\left(\frac{a}{b}\right) = h\left(\frac{a}{1} \cdot \frac{1}{b}\right) = h\left(\frac{a}{1}\right) \cdot h\left(\frac{1}{b}\right) = g(a)g(b)^{-1}, \end{gathered} \tag{5.7}$$

de forma que h queda determinat per g. Per tant, si h existeix, és únic. Veiem ara que h, en efecte, existeix. Definim $h(\frac{a}{b}) = g(a)g(b)^{-1}$. Hem de veure que h està ben definit. Si tenim $\frac{a}{b} = \frac{c}{d}$ a $\mathbb{K}(A)$, es compleix que $ab = bc$ a A. Aleshores, com g és morfisme d'anells, tenim $g(a)g(d) = g(b)g(c)$, que implica $g(a)g(b)^{-1} = g(c)g(d)^{-1}$, com volíem. Ara, és clar que com g és morfisme d'anells, h també. I com $\mathbb{K}(A)$ és cos, h és injectiu. ■

6 Divisibilitat

Definició 6.1 (Elements associats). Dos elements a, b d'un anell A es diuen associats si existeix una unitat $u \in A$ (element invertible) tal que $b = ua$. Posem $a \sim b$ per indicar que a i b són associats. Clarament, la relació $\sim$ és d'equivalència.

Proposició 6.2. *Sigui A un anell, $a, b \in A$. Si més no un dels dos elements a, b és no divisor de zero, es compleix:*

$$a \mid b \text{ i } b \mid a \iff a \sim b. \tag{6.1}$$

En particular, si A és domini d'integritat, aleshores es compleix l'equivalència per a tot parell d'elements $a, b \in A$.

Definició 6.3 (Divisors propis). Si a és un element no nul d'un anell A, les unitats d'A i els elements associats d'a divideixen a. Direm divisors propis d'a els divisors d'a diferents d'aquests.

Definició 6.4 (Element irreductible). Un element a no nul d'un domini d'integritat d'A s'anomena *irreductible* si no és una unitat i no té divisors propis. Un element a no nul i no unitat s'anomena compost si té divisors propis.

Definició 6.5 (Màxim comú divisor). Siguin A un anell, $a, b, d \in A$. Diem que d és un màxim comú divisor d'a i b si se satisfan les dues propietats següents:

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

El màxim comú divisor queda determinat tret d'associats.

Definició 6.6 (Mínim comú múltiple). Siguin A un anell i $a, b, m \in A$. Diem que m és un màxim comú múltiple d'a i b si se satisfan les dues propietats següents:

1. $a \mid m, b \mid m$ i
2. si $n \in A$ satisfà que $a \mid n$ i $b \mid n$, aleshores $m \mid n$.

El mínim comú múltiple queda determinat tret d'associats.

7 Dominis euclidians

Definició 7.1 (Domini euclidià). Sigui A un domini d'integritat. Direm que A és un domini euclidià si existeix una aplicació $\partial : A \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

1. Si $a, b \in A \setminus \{0\}$ i $a \mid b$, aleshores $\partial(a) \leq \partial(b)$.
2. *Divisió entera respecte de ∂*: Donats $a, b \in A$, amb $b \neq 0$, existeixen $q, r \in A$ tals que $a = bq + r$ i $\partial(r) < \partial(b)$, sempre que $r \neq 0$ (si $r = 0$, $a = bq$).

Si A és un domini euclidià i $\partial : A \setminus \{0\} \longrightarrow \mathbb{N}$ és una aplicació que compleix ambdues propietats, direm que (A, ∂) és un domini euclidià.

Proposició 7.2. *Tot domini euclidià és domini d'ideals principals.*

Demostració. Sigui (A, ∂) un domini euclidià i I un ideal d'A. Vegem que I és un ideal principal. Com $(0) = \{0\}$, podem suposar $I \neq (0)$. Sigui $b \in I \setminus \{0\}$ amb $\partial(b)$ mínim, és a dir, $\partial(b) \leq \partial(x)$ per a tot $x \in I \setminus \{0\}$. Aleshores, és clar $(b) \subset I$. Vegem $I \subset (b)$: sigui $a \in I$ i posem $a = qb + r$, amb $\partial(r) < \partial(b)$, si $r \neq 0$. Com $r = a - qb \in I$ ha de ser $r = 0$ per l'elecció de b. Per tant, $a = qb \in (b)$. ■

Definició 7.3 (Norma euclidiana). Sigui A un anell. Una norma d'A és una aplicació $N : A \longrightarrow \mathbb{Z}$ tal que compleix les següents propietats:

1. Si $a \in A$, $N(a) = 0$ si, i només si, $a = 0$;

2. $N(ab) = N(a)N(b)$ per a qualssevol elements a, b d'A.

Proposició 7.4. *Sigui A un anell que té una norma N; aleshores:*

1. *A és domini d'integritat.*
2. *$\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ definida per $\delta(a) = |N(a)|$ compleix la primera propietat del domini euclidià.*
3. *$N(1) = 1$.*
4. *$u \in A^* \implies N(u) = \pm 1$.*

8 Factorialitat en dominis d'ideals principals

Definició 8.1 (Element primer). Un element p d'un domini d'integritat A es diu primer si p és no nul i no unitat, i per a $a, b \in A$ es compleix:

$$p \mid ab \implies p \mid a \text{ o bé } p \mid b. \tag{8.1}$$

Proposició 8.2. *En un domini d'integritat A, un element p no nul és primer si, i només si, l'ideal (p) és primer.*

Proposició 8.3. *En un domini d'integritat, tot element primer és irreductible. En un domini d'ideals principals, tot element irreductible és primer.*

9 Dominis de factorització única

Definició 9.1 (Domini de factorització única). Un domini d'integritat A es diu *domini de factorització única* si es compleixen les dues propietats següents:

1. Per a tot element a no nul i no unitat d'A, existeixen elements irreductibles $p_1, \dots, p_r$ d'A tals que $a = p_1 \cdots p_r$.
2. Si $p, p_1, \dots, p_r$ són elements irreductibles d'A i $p \mid p_1 \cdots p_r$, aleshores p és associat amb algun p_i.

Definició 9.2 (Domini de factorització). Si A és un domini d'integritat que compleix la primera propietat de la factorització única, direm simplement que és un *domini de factorització*.

Observació 9.3. Tenim que tot domini euclidià és un domini d'ideals principals. Al seu torn, tot domini d'ideals principals és domini de factorització única. Es dona, doncs, aquesta cadena d'equivalències.

Proposició 9.4. *Sigui A un domini de factorització. Aleshores, A és domini de factorització única si, i només si, tot element irreductible d'A és primer.*

Demostració. Sigui A un domini de factorització única, p un element irreductible tal que $p \mid ab$. Anem a plantejar una sèrie de casos:

- Si $a = 0$, $p \mid a$, i si $b = 0$, $p \mid b$.
- Si A és unitat, $p \mid b$ i, si b és unitat, $p \mid a$.

Si a i $b \neq 0$, tals que a, b no són unitats, podem escriure a i b com $a = p_1 \cdots p_r$ i $b = q_1 \cdots q_s$ ($p_1 \cdots p_r$ i $q_1 \cdots q_s$ són irreductibles), respectivament. Aleshores, podem escriure $p \mid ab$ com:

$$p \mid p_1 \cdots p_r q_1 \cdots q_s \implies \begin{cases} p \sim p_i \implies p \mid a \\ p \sim q_j \implies p \mid b \end{cases} \tag{9.1}$$

Suposem ara que tot irreductible d'A és primer $p, p_1, \ldots, p_r$ irreductibles d'A i $p \mid p_1 \cdots p_r$. Com p és primer, en particular $p \mid p_i$ per a cert $i \in \{1, \ldots, r\}$ i $p \sim p_i$. ■

Proposició 9.5. *Per a un nombre enter d lliure de quadrats, l'anell $\mathbb{Z}[\sqrt{d}]$ és domini de factorització.*

10 Factorialitat en un anell de polinomis

Proposició 10.1. *Sigui A un domini d'integritat. Les propietats següents són equivalents:*

1. *A és un cos.*
2. *$A[X]$ és un domini euclidià.*
3. *$A[X]$ és un domini d'ideals principals.*

Definició 10.2 (Contingut d'un polinomi). Sigui $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$ un polinomi amb coeficients en un domini de factorització única A. Anomenarem *contingut* de f un màxim comú divisor dels coeficients d'f. Denotem per $c(f)$ el contingut de f. Tenim, doncs:

$$c(f) = \mathrm{mcd}(a_0, a_1, \ldots, a_n). \tag{10.1}$$

Clarament, el contingut d'un polinomi d'$A[X]$ queda determinat tret d'un factor d'A^*.

Definició 10.3 (Primitiu). Direm que f és primitiu si el seu contingut $c(f)$ és una unitat.

Definició 10.4 (Polinomi primitiu corresponent a f). Donat $f \in A[X]$, existeix clarament un polinomi primitiu f^* tal que $f = c(f)f^*$. El polinomi f^* és únic en el sentit següent: si $f = c\tilde{f}$, amb $c \in A$ i $\tilde{f}$ primitiu, aleshores $c \sim c(f)$ i $\tilde{f} \sim f^*$. Direm que f^* és un polinomi primitiu corresponent a f.

Proposició 10.5 (Lema de Gauss). *Sigui A un domini de factorització única. Aleshores, en $A[X]$ el producte de polinomis primitius és primitiu. Més generalment, si $f, g \in A[X]$, $c(fg) \sim c(f)c(g)$.*

Demostració. Sigui $p \in A$ un element irreductible i considerem el morfisme d'anells:

$$\begin{array}{cccc} \varphi : & A[X] & \longrightarrow & (A/(p))[X] \\ & \sum_{i=0}^{n} a_i X^i & \longmapsto & \sum_{i=0}^{n} \pi(a_i) X^i \end{array} \tag{10.2}$$

on π és el morfisme de pas al quocient d'A en $A/(p)$. El nucli d'aquest morfisme és el conjunt de polinomis on tots els seus coeficients cauen en la classe del zero, és a dir, que p divideix cadascun d'aquests elements i, en particular, divideix el seu contingut. En altres paraules, donat $h \in A[X]$, $\varphi(h) = 0$ si, i només si $p \mid c(h)$. Siguin ara f, g dos elements d'$A[X]$. Com $\varphi(fg) = \varphi(f)\varphi(g)$, tenim $\varphi(fg) = 0$ si, i només si, $\varphi(f) = 0$ o bé $\varphi(g) = 0$. Alternativament, $fg \in \ker(\varphi)$ si, i només si, $f \in \ker(\varphi)$ o bé $g \in \ker(\varphi)$. En més detall, com A és domini de factorització única, p és primer i, per tant, $A/(p)$ és un domini d'integritat. Com $A/(p)$ és un domini d'integritat, $A/(p)[X]$ també ho és. Equivalentment, p és factor irreductible de $c(fg)$ si, i només si, ho és de $c(f)$ o bé de $c(g)$.
Suposem f, g primitius, és a dir, tals que $c(f)$ i $c(g)$ són unitats. Suposem, al seu torn, $c(fg)$ no unitats. Aleshores, p és irreductible i compleix que $p \mid c(fg) \implies p \mid c(f)$ o bé $p \mid c(g)$. *Arribem a contradicció, que ve de suposar f, g primitius.* En general, posem $f = c(f)f^*$, $g = c(g)g^*$ tal que f^*, g^* són primitius. Aleshores, $fg = c(f)c(g)(f^*g^*)$ i f^*g^* és primitiu. Per tant, $c(fg) \sim c(f)c(g)$. ■

Corol·lari 10.6. *Sigui A un domini de factorització única, $\mathbb{K}$ el cos de fraccions d'A i $f \in A[X]$ mònic. Si $f = gh$, amb $g, h \in \mathbb{K}[X]$ mònics, aleshores $g, h \in A[X]$.*

Definició 10.7 (Element irreductible, anell de polinomis). Sigui A un domini de factorització única. Un element d'A és element irreductible d'$A[X]$ si, i només si, és element irreductible d'A (un element d'$A[X]$ de grau positiu no pot dividir un element d'A).

Proposició 10.8. *Sigui A un domini de factorització única i sigui $f(X) \in A[X]$. Les condicions següents són equivalents:*

1. *$f(X)$ té grau positiu i és irreductible a $A[X]$.*
2. *$c(f) \sim 1$ (f és primitiu) i $f(X)$ és irreductible a $\mathbb{K}[X]$.*

Demostració. Provarem la implicació cap a baix, $\Rightarrow$, i cap a dalt, $\Leftarrow$.

- $\boxed{\Rightarrow}$ Suposem que $f(X)$ té grau positiu i és irreductible a $A[X]$. Tot element irreductible d'A és irreductible a $A[X]$. La factorització $f = c(f)f^*$, amb f^* primitiu, és no trivial (sempre que $c(f)$ no sigui una unitat). Com que f és irreductible, deduïm que $c(f)$ és una unitat; és a dir, $c(f) \sim 1$. Per veure que $f(X)$ és irreductible a $\mathbb{K}[X]$, posem $f = gh$, amb $g, h \in \mathbb{K}[X]$ i $\mathrm{gr}(h) > 0$. *Volem veure que g ha de tenir grau zero i, per tant, ha de ser una unitat de* $\mathbb{K}[X]$. Si a és denominador comú dels coeficients de $g(X)$ i b dels de $h(X)$, tenim que ag i bh són elements d'$A[X]$ i $abf = (ag)(bh)$ és una factorització d'abf en $A[X]$. Siguin g^*, h^* els polinomis primitius corresponents a ag i bh: $ag = c(ag)g^*$

i $bh = c(bh)h^*$. Aleshores:

$$ab \sim c(abf) = c((ag)(bh)) \sim c(ag)c(bh), \tag{10.3}$$

pel lema de Gauss i, per tant, $f = ug^*h^*$, amb $u \in A^*$. Com f és irreductible a $A[X]$ i h^* té grau positiu, g^* és una unitat d'$A[X]$ i, per tant, $g^* \in (A[X])^* = A^*$. En conseqüència, g^* és de grau 0 i g és constant.

$\boxed{\Leftarrow}$ Sigui $f \in A[X]$ amb $c(f) \sim 1$, i suposem que f és irreductible a $\mathbb{K}[X]$. Posem $f = gh$, amb $g, h \in A[X]$, h de grau positiu. Com $A[X] \subset \mathbb{K}[X]$, g ha de tenir grau 0 i, així, $g \in \mathbb{K} \cap A[X] = A$. Ara, la relació $1 \sim c(f) \sim c(g)c(h) \sim g \cdot c(h)$ dona que $g \in A^*$. Per tant, f és irreductible a $A[X]$.

■

Lema 10.9. *Si $p \in A$ és un primer en A, aleshores p també és un primer en $A[X]$.*

Teorema 10.10. *Si A és un domini de factorització única, aleshores $A[X]$ és un domini de factorització única.*

Proposició 10.11 (Criteris d'irreductibilitat)**.**

1. *Sigui $f(X) \in A[X]$, $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Si $\frac{c}{d}$ és una arrel de f a $\mathbb{K}$, amb* $\operatorname{mcd}(c, d) = 1$, *aleshores $c \mid a_0$ i $d \mid a_n$.*
2. *Sigui $f(X) \in A[X]$ un polinomi primitiu de grau 2 o 3. Aleshores, $f(X)$ és irreductible si, i només si, no té cap arrel a $\mathbb{K}$.*

Proposició 10.12 (Criteri modular)**.** *Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, primitiu, i suposem que existeix $p \in A$, irreductible, tal que $p \nmid a_n$ i que el polinomi $\overline{f}(X) = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \in (A/(p))[X]$ és irreductible (on $\overline{a}$ indica la classe d'$a \in A$ en el quocient $A/(p)$ pel morfisme de pas al quocient $\pi : A \longrightarrow A/(p)$). Aleshores, f és irreductible en $A[X]$.*

Proposició 10.13 (Criteri d'Eisenstein)**.** *Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ primitiu i sigui $p \in A$, irreductible en A. Suposem que $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, p \mid a_n$ i $p^2 \nmid a_0$. Aleshores, $f(X)$ és irreductible.*