Apunts d'estructures algrebraiques

Aleix Torres i Camps

Jordi Guardia (jordi.guardia-rubies@upc.edu), Anna Rio i Santi Molina (Martí Oller)

Índex

Capítol 1

Introducció

1.1 Operacions i propietats

Definició 1.1.1. Una operació en un conjunt A és una aplicació $\varphi : A \times A \to A$

Definició 1.1.2. Algunes propietats de les operacions poden ser:

1. (PC) Propietat commutativa (o abeliana) $\forall a, b \in A \ \varphi(a, b) = \varphi(b, a)$.
2. (PA) Propietat associativa $\forall a, b, c \in A \ \varphi(a, \varphi(b, c)) = \varphi(\varphi(a, b), c)$.
3. (EN) Element neutre $\exists e \in A$ tal que $\forall a \in A \ \varphi(e, a) = \varphi(a, e) = a$.

   Clarament, l'element neutre és únic. En efecte, si n'existisin 2 elements neutres, e i e', aleshores $e = \varphi(e, e') = e'$, amb la qual cosa hem arribat a contradicció.

4. (PI) Invers d'un element $a \in A$ és $b \in A$ tal que $\varphi(a, b) = \varphi(b, a) = e$.

   Si existeix i és associatiu també és únic. En efecte, si $\exists b, c$ tals que $\varphi(a, b) = \varphi(b, a) = \varphi(a, c) = \varphi(c, a) = e$. En aquest cas, $b = \varphi(b, \varphi(a, c)) = \varphi(\varphi(b, a), c) = c$, per tant, $b = c$ i són el mateix element.

5. (PD) Si tenim dues operacions, que la primera (φ) sigui distributiva respecte la segona (μ) vol dir que $\varphi(a, \mu(b, c)) = \varphi(\mu(a, b), \mu(a, c))$ i que $\varphi(\mu(b, c), a) = \varphi(\mu(b, a), \mu(b, c))$.

1.2 Estructures algebraiques bàsiques

Definició 1.2.1. Un Grup $(G, *)$ cal que compleixi EN, PA, PI.

Definició 1.2.2. Un Semigrup $(G, *)$ cal que compleixi EN, PA.

Definició 1.2.3. Un Grup Abelià és un grup amb PC.

Definició 1.2.4. Una Anell $(A, +, *)$ cal que $(A, +)$ sigui un grup abelià, $(A, *)$ un semigrup i la PD respecte la primera.

Definició 1.2.5. Un Anell communtatiu (o abelià) és un anell on $(A, *)$ és commutatiu.

Definició 1.2.6. Un Cos és un Anell $(A, +, *)$ tal que $(A \setminus \{0\}, *)$ és un grup abelià. On 0 és l'element neutre de $(A, +)$.

Definició 1.2.7. Mòdul $(M, +)$ és un mòdul sobre l'Anell A tal que: $(M, +)$ és un grup abelià i $A \times M \to M$ (multiplicació per escalars) tal que: $a(m_1 + m_2) = am_1 + am_2$, $(a+b)m = am + bm$, $a(bm) = (ab)m$ i $1_A m = m$ $(\forall a, b \in A, \forall m, m_1, m_2 \in M$.

Definició 1.2.8. Un espai vectorial és un mòdul sobre un Cos.

Capítol 2

Anells

Sigui $(A, +, \cdot)$ un Anell (sempre ens referirem a Anells commutatius sense haver de dir-ho cada vegada).

2.1 Propietats dels anells

Notació: 0_A és l'emenent neutre de la suma $(+)$, el zero. I a l'element neutre del producte $(\cdot)$ és 1_A, que anomenarem l'u. Denotarem $-a$ l'element invers d'a respecte $+$ (l'"oposat"). a^{-1} l'element invers d'a respecte del producte. $A^* = \{a \in A \text{ tal que } \exists a^{-1}\}$ s'obté un grup abelià.

Proposició 2.1.1. *Propietats:*

1. $\forall a, b, c \in A$ *si* $a + b = a + c$ *llavors* $b = c$.
2. $\forall a \in A$ *es compleix que* $0_A \cdot a = 0_A$.
3. $\forall a \in A$ *es compleix que* $(-1_A) \cdot (-a) = a$.
4. $\forall a \in A$ *es compleix que* $(-1_A) \cdot (a) = -a$.

Demostració.

1. $-a+(a+b) = -a+(a+c) \iff$ (per PA) $(-a+a)+b = (-a+a)+c \iff O_A+b = O_A+c \iff b = c.$
2. $0_A \cdot a + 0_A = 0_A \cdot a = ((0_A + 0_A) \cdot a) = [PD] = 0_A \cdot a + 0_A \cdot a \implies 0_A = 0_A \cdot a.$
3. $(-1_A)(-a) = (-1_A)(-a) + (-a) + (a) = [PD] = (1_A - 1_A)(-a) + a = 0_A + a = a.$
4. $-a = [3] = ((-1_A)(-1_A))(-a) = [PA] = (-1_A)((-1_A)(-a)) = [3] = (-1_A)(a).$

□

Exemple 1. Alguns exemples d'anells.

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. $Z[x] \subset Q[x] \subset R[x] \subset C[x]$
3. $M_n(A)$ on A és un Anell
4. $\mathbb{Z}[J] = \{a_0 + a_1 J + a_2 J^2 + a_3 J^3 + a_4 J^4 : a_i \in \mathbb{Z}\}$ $J = e^{2\pi i/5}$
5. $\mathbb{Z}/n\mathbb{Z}$ Taules d'operacions per $n = 6, 8$.

Proposició 2.1.2. *Sigui A un anell tal que neutre de la suma és el neutre del producte ($0_A = 1_A$) aleshores l'Anell té un sol element ($A = \{0_A\}$).*

Demostració. Suposem que tenim un element $a \in A$ diferent del neutre. Aleshores, $0_A = 0_A \cdot a = 1_A \cdot a = a$. I, per tant, aquest element també és 0_A. □

Definició 2.1.3. Sigui A un anell, $n \in \mathbb{Z}$ i $a \in A$. Llavors, si $n > 0$, $n \cdot a := a + \cdots + a$, si $n < 0$, $n \cdot a := (-a) + \cdots + (-a)$, si $n = 0_{\mathbb{Z}}$, $0_{\mathbb{Z}} \cdot a = 0_A$. De la mateixa manera, si $n > 0$, $a^n := a \cdot \ldots \cdot a$, si $n < 0$, $a^n := a^{-1} \cdot \ldots \cdot a^{-1}$ i si $n = 0_{\mathbf{Z}}$, $a^n = 1_A$.

Definició 2.1.4. Direm que l'anell A té característica n, si n és el menor nombre enter positiu més petit tal que $n \cdot 1_A = 0_A$. En cas que no existeixi ($n \cdot 1_A \neq 0_A \ \forall n \in \mathbb{Z}^+$), direm que té característica 0.

Observació 2.1.5. *Està clar que* $char(A) \cdot a = O_A \ \forall a \in A$.

2.2 Subanells i anells productes

Definició 2.2.1. Un subanell d'un anell A és un subconjunt S tal que:

1. $1_A \in S$
2. $a, b \in S \implies a - b \in S$
3. $a, b \in S \implies a \cdot b \in S$

Proposició 2.2.2. $1_A \in S \subset A$, *llavors* S *és un subanell* $\iff$ S *és un anell.*

Demostració.

$\Longrightarrow$) Cal veure que $(S, +)$ és un grup (Abelià), $(S, \cdot)$ és un semigrup i que és compleix la PD. De les operacions de A s'hereden automaticament les propietats PA, PC, PD. Ara de la primera característica dels subanells tenim $1_A \in S$. I de la 2a, fent $b = a$, tenim $0_A \in S$ i ara, fent $a = 0_A$, $b = a$, tenim l'invers per la suma. Per tant, S és un anell.

$\Longleftarrow$) Si S és un anell, té el neutre de la multiplicació, té invers de la suma, està tancat per la suma i està tancat per la multiplicació. Cosa que demostra les característiques 1, 2 i 3, respectivament. □

Exemple 2. $\mathbb{Z} \subset \mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ són anells.

$2\mathbb{Z} = \{a \in \mathbb{Z} : a \cong 0(\text{mod}2)\} = \{2k : k \in \mathbb{Z}\}$ No és un subanell.

2.3 Ideals

Proposició 2.3.1. *Sigui* $J = e^{2\pi i/n}$. $\mathbb{Z}[J] = \{a_0 + a_1 J + \ldots + a_{n-1} J^{n-1} : a_i \in \mathbb{Z}\}$ Demostreu que és una anell comprovant que és un subanell de $\mathbb{C}$.

Definició 2.3.2. Donats A, B anells. el seu anell producte és el conjunt $A \times B$ amb les operacions:

$$\begin{aligned} + : (A \times B) \times (A \times B) &\to A \times B \\ (a_1, b_1), (a_2, b_2) &\to (a_1 + a_2, b_1 + b_2) \\ \cdot : (A \times B) \times (A \times B) &\to A \times B \\ (a_1, b_1), (a_2, b_2) &\to (a_1 \cdot a_2, b_1 \cdot b_2) \end{aligned}$$

Definició 2.3.3. Sigui A un anell. Un subconjunt $I \subset A$ és un ideal si $\forall u, v \in I, \ \forall \alpha, \beta \in A$.

1. $u \in I, \alpha \in A \implies \alpha \cdot u \in I$
2. $u, v \in I \implies u + v \in I$

I, per tant, només cal comprovar que $\alpha u + \beta v \in I$.

Exemple 3. Alguns ideals:

1. $\{0_A\}$ L'ideal zero. A l'ideal total.
2. $m\mathbb{Z} \subset \mathbb{Z}$ és un ideal.
3. Anell principals o l'anell generat per $a \in A$ és $(a) := \{am : m \in A\}$. Similarment l'ideal finitament generat per $a_1, \ldots, a_n \in A$ és $(a_1, a_2, \ldots, a_n) := \{a_1m_1 + \ldots + a_nm_n : m_i \in A\}$.
4. Per $\alpha \in \mathbb{Q}$, definim $I = \{f(x) \in Q$, llavors $I = \{f(x) \in \mathbb{Q}[x] : f(x) = 0\}$ és un ideal de $\mathbb{Q}[x]$ i coincideix amb el generat per $(x - \alpha) = I$
5. $I = \{f(x, y) \in \mathbb{Q}[x, y] : f(0, 0) = 0\}$ ideal de $\mathbb{Q}[x, y]$. Coincideix amb $(x, y) = I$.

Proposició 2.3.4. *$I, J \subset A$ ideals*

1. *$I + J = \{a + b : a \in I, b \in J\}$ és un ideal i és el menor que conté I i J.*
2. *$I \cdot J = \{\sum_{j<\infty} a_jb_j : a_j \in I, b_j \in J\}$ és un ideal*

Demostració.

1. Primer comprovem que és un ideal. Siguin $a_1, a_2 \in I$, $b_1, b_2 \in J$ i $u = a_1 + b_1, v = a_2 + b_2 \in I + J$, $\alpha, \beta \in A$, llavors $\alpha u + \beta v = \alpha(a_1 + b_1) + \beta(a_2 + b_2) = (\alpha a_1 + \beta a_2) + (\alpha b_1 + \beta b_2)$ que pertany a $I + J$, ja que $(\alpha a_1 + \beta a_2) \in I$ i $(\alpha b_1 + \beta b_2) \in J$.

   I és el menor que conté els I i a J, perquè si un ideal K els conté, com que $\forall a \in I \subset K$, $\forall b \in J \subset K$ aleshores, com que K ha de ser tancat per la suma, segur que $a + b \in K$.
2. Siguin $a_j, a_i \in I$, $b_j, b_i \in J$ i $u = \sum_j a_j \cdot b_j, v = \sum_i a_i \cdot b_i \in I \cdot J$, $\alpha_1, \alpha_2 \in A$, llavors, $\alpha_1 u + \alpha_2 v = \alpha_1 \sum_j a_j \cdot b_j + \alpha_2 \sum_i a_i \cdot b_i =$ [PD i PA] $= \sum_j (\alpha_1 a_j) \cdot b_j + \sum_i (\alpha_2 a_i) \cdot b_i = \sum_{k=i,j} (\alpha a_k) b_k \in I \cdot J$, perquè $\alpha_1 a_j, \alpha_2 a_i \in I$.

□

Proposició 2.3.5. *En un anell, $a \in A$, $u \in A^*$, aleshores $(a) = (ua)$, és a dir, l'ideal generat per a i per ua son el mateix.*

Demostració.

$\subseteq$) Sigui $b \in (a)$, aleshores $b \in (ua)$ perquè b ha de ser de la forma $b = ax$ llavors, podem escrire b de la forma $b = au(u^{-1}x)$, el qual, clarament és un element de (ua).

$\supseteq$) Sigui $b \in (ua)$ aleshores b és de la forma $b = uax$ llavors també és de la forma $b = uau^-1ux = a(ux)$, per la qual cosa b és un element de (a). □

Proposició 2.3.6. *A és un cos $\iff$ els seus únics ideals són 0 i A.*

Demostració.

$\implies$) Sigui $I \subset A$ un ideal no nul. Sigui $x \in I$, $x \neq 0$, A cos $\implies \exists x^{-1}$, i com $x \in I \implies 1 = xx^{-1} \in I \implies \forall a \in A\ a = a \cdot 1 \in I \implies I = A$.

$\impliedby$) Sigui $x \in A$, $x \neq 0$ si $0 \neq (x) \implies (x) = A \implies 1 \in (x) \implies \exists y \in A$ tal que $1 = xy$ per tant, $y = x^{-1}$. □

Teorema 2.3.7. *Tots els ideals de l'anell de $\mathbb{Z}$ son principals.*

Demostració. Sigui $I \subset \mathbb{Z}$ un ideal. Si $I = (0)$ és principal clarament. Suposem que $\exists x \in I$ amb $x \neq 0$ llavors $x \in I \iff -x \in I$. Per tant, $I^+ = \{x \in I : x > 0\} = I \bigcap \mathbb{N} \neq 0$. Pel principi de bona ordenació de $\mathbb{N}$, $\exists m = \min I^+$.

Aleshores, suposem que hi ha un element y que no és de la forma mk. Li fem la divisio euclidiana i escrivim $y = mk + r$ per algun r (el qual pertany a I perquè I és tancat per la suma) entre m i 0 no inclosos. Aleshores, hem arribat a contradicció, perquè abans haviem dit que m era el mínim i ara hem vist que n'existeix un element positiu més petit. □

Proposició 2.3.8. *Sigui k un cos. Tots els ideals de $k[x]$ són principals.*

Demostració. Semblant amb la demostració anterior, només cal canviar el mínim pel polinomi del mínim grau. La contradicció és la mateixa. □

Definició 2.3.9. Un anell principal és un anell que tots els seus ideals son principals.

2.4 Morfisme d'anells

Definició 2.4.1. Siguin A, B dos anells. Una apliacació $f : A \to B$ és un morfisme d'anells si preserva les operacions en A i B.

1. $f(1_A) = 1_B$
2. $\forall x, y \in A\ f(x + y) = f(x) + f(y)$
3. $\forall x, y \in A\ f(xy) = f(x)f(y)$

Anomenarem Monomorfisme al morfisme injectiu, Epimorfisme al morfisme exhaustiu i isomorfisme al morfisme bijectiu.

Observació 2.4.2. *Sigui A un anell qualsevol. $\varphi : \mathbb{Z} \to A$ amb $\varphi(m) = m \cdot 1_A$. Aquest morfisme és injectiu si $char(A) = 0$, i es compleix que $\varphi^{-1}(0) = char(A)$.*

Proposició 2.4.3. *Propietats bàsiques dels anells . Siguin A i B dos anells i f un morfisme d'anell.*

1. $f(a^n) = f(a)^n$
2. $a \in A^* \implies f(a) \in B^*,\ f(a)^{-1} = f(a^{-1})$
3. *Sigui $J \subset B$ un ideal, llavors $f^{-1}(J) \subset A$ és un ideal*
4. *En general, la imatge d'un ideal d'A no és un ideal de B.*
5. *Si f és exhaustiva, llavors $I \subset A$ ideal $\implies f(I) \subset B$ també és un ideal.*
6. $\ker f := \{a \in A : f(a) = 0\} = f^{-1}((0))$ *és un ideal d'A.*
7. $Imf := \{f(a) : a \in A\} \subset B$ *subanell de B.*
8. *f injectiva* $\iff \ker f = 0$.
9. *A cos* $\implies f = 0$ *o f injectiu.*

Demostració.

1. Per inducció, es poden treure potencies una per una.
2. Per la propietat del producte dels morfirmes i envia l'element neutre a l'element neutre $1_B = f(1_A) = f(aa^{-1}) = f(a)f(a^-1)$.
3. Siguin $a_1, a_2 \in f^{-1}(J)$ i $\lambda, \mu \in A$, llavors $\lambda a_1 + \mu a_2 \in f^{-1}(J)$? Sí, perquè $f(\lambda a_1 + \mu a_2) = f(\lambda)f(a_1) + f(\mu)f(a_2) \in J$ perquè és combinació d'elements de J. Per tant, és un ideal.
4. Contraexemple, Si $A = \mathbb{Z}$ i $B = \mathbb{Q}$ i f és la inclusió. Un ideal de A és per exemple (2) però $f((2))$ no és un ideal perquè $2\frac{1}{3} \notin f((2))$.

5. Siguin $f(a), f(b) \in f(I)$ i $\lambda, \mu \in B$, llavors $\lambda f(a) + \mu f(b) \in f(I)$, sí, perquè al ser exhaustiva, $\exists x_\lambda, x_\mu$ tal que $f(x_\lambda) = \lambda$ i $f(x_\mu) = \mu$. Per tant, $\lambda f(a) + \mu f(b) = f(x_\lambda)f(a) + f(x_\mu)f(b) = f(x_\lambda a + x_\mu b) \in f(I)$.
6. L'element neutre hi és perquè $f(1_A) = 1_B$, la resta i el producte de dos elements hi són perquè f està tancat per la suma (i resta) i pel producte.
7. Que f sigui injectiva fa que només el 0 pugui anar al 0. Ja que, en qualsevol cas $f(0+0) = f(0)+f(0) \implies f(0) = 0$. I que $\ker f = 0$ implica que si dos elements tiguéssin la mateixa imatge $f(a) = f(b) \implies f(a) - f(b) = 0 \implies f(a-b) = 0$ i com que només el 0 va al 0, $a = b$.
8. Suposem que A és un cos i que dos elements diferents tenen la mateixa imatge $f(a) = f(b) \implies f(a-b) = 0$. Aleshores, $f(x) = f(x)f(1) = f(x(a-b)^{-1}(a-b)) = f(x(a-b)^{-1})f(a-b) = 0$. Llavors, f és la funció que va tot a 0. (I sembla que $0_B = 1_B$). Altrament f és injectiva.

□

2.5 Anell quocient

Definició 2.5.1. Anell quocient. Sigui A un anell i $I \subset A$ un ideal. Definim la relació d'equivalència $\sim$ com (per $a, b \in A$) $a \sim b \iff a - b \in I$. El corresponent conjunt quocient l'anotarme com A/I.

En el conjunt quocient A/I definim dues operacions:

1. $\overline{a} + \overline{b} := \overline{a+b}$
2. $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$

Hem de veure que estan ben definides:

Suposem que $a' \in \overline{a}, b' \in \overline{b}$, cal veure que $\overline{a'+b'} = \overline{a+b}$ i $\overline{a'b'} = \overline{ab}$. Aleshores, hem de veure que la seva diferencia pertany a l'ideal. Així que fem $(a+b) - (a'+b') = (a-a') + (b-b') \in I$ perquè cada una de les diferencies pertany a l'ideal. I $ab - a'b' = b'(a-a') - a(b-b') \in I$, perquè l'ideal és tancat per la multiplicació.

Exercici 2.5.2. *Coproveu que aquestes dues operacions tenen totes les propietats necessàries per a què A/I sigui un anell. En direm anell quocient d'A per I.*

Solució. La classe del 0, és l'element neutre de la suma, perquè $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$. La suma commutativa, associativa i té invers perquè el propi anell A ho és i s'hereda. El mateix passa amb la multiplicació, la classe de l'1 és l'element neutre i les propietats s'hereden. □

Exemple 4.

1. $A = \mathbb{Z}$ i $I = (m)$ i $A/I = \mathbb{Z}/m\mathbb{Z}$
2. $A = K[x]$, $\alpha \in K$ i $I = (x - \alpha)$.

$$A/I = K[x]/(x-\alpha) \to K$$
$$\bar{p}(x) \to p(\alpha)$$

Està ben definit, si $q(x) \in \bar{p}(x)$, llavors $q(x) - p(x) \in (x-\alpha) \implies q(x) - p(x) = (x-\alpha)h(x) \implies q(\alpha) - p(\alpha) = 0$.

3. $A = \mathbb{R}[x]$ i $I = (x^2+1)$ llavors el seu quocient és isomorf a C. Enviant $\bar{p}(x)$ a $p(i)$.

Proposició 2.5.3. *L'aplicació natural*

$$\pi : A \to A/I$$
$$a \to \overline{a}$$

és un morfisme d'anells.

Demostració. La definició de les operacions A/I ho garanteix. □

Proposició 2.5.4. *(a) Sigui $J \subset A$ ideal tal que $J \supset I$, llavors $J/I := \pi(J) \subset A/I$ és un ideal. (b) Sigui $U \subset A/I$ ideal, existeix un únic ideal $J \subset A$ tal que $J \supset I$ i $J/I = U$.*

Demostració. (a) L'aplicació π és exhaustiva perquè $\ker \pi = \{a \in A, \overline{a} = \overline{0}\} = \{a \in A : a \in I\} = I$, llavors per una propietat anterior la imatge d'un ideal és un ideal.

(b) Sigui $J = \pi^{-1}(U) \subset A$ un ideal (perquè l'antiimatge d'un ideal és un ideal), notem que $\pi(J) = \pi(\pi^{-1}(U)) = [exh] = U$. Aleshores, com que U és ideal, $\overline{0} \in U \implies I = \pi^{-1}(0) \subset \pi^{-1}(U) = J$

Suposem que J' també satisfà $\pi(J') = U$ i $J' \supset I$. $\pi(J') = U \implies J' = \pi^{-1}(\pi(J')) \supset \pi^{-1}(U) = J$ i $a \in J' \implies \pi(a) \in U \implies a \in \pi^{-1}(U) = J$. Llavors $J = J'$. □

Proposició 2.5.5. *Propietat universal del quocient. Sigui $f : A \to B$ un morfisme d'anells $I \subset A$ ideal tal que $I \subset \ker f$. Existeix un únic morfisme $\varphi : A/I \to B$ tal que $\varphi \circ \pi = f$*

Demostració. Comencem definint $\varphi(\overline{a}) := f(a)$. Anem a veure que està ben definida i compleix que $\varphi \circ \pi = f$. Que compleix la segona condició està clar perquè $\varphi \circ \pi(a) = \varphi(\overline{a}) = f(a)$. Aleshores, està ben definida perquè si tenim que $\overline{a} = \overline{b}$, vol dir que $a - b \in I$, llavors, per condició de l'enunciat $f(a - b) = 0$ i, per tant, $f(a) = f(b)$, que és el que ens cal perquè $\varphi(\overline{a}) = \varphi(\overline{b})$.

Suposem que existeix una $\varphi' \neq \varphi$ que comleix la mateixa propietat. Aleshores, sigui $x \in A$ un element el qual es compleixi que $\varphi(\overline{x}) \neq \varphi'(\overline{x})$, al ser π exhaustiva, sempre existeix. Però sabem que $\varphi(\overline{x}) = \varphi(\pi(x)) = f(x) = \varphi'(\pi(x))$ llavors són la mateixa funció. Per tant, hem acabat, només n'hi ha una. □

Teorema 2.5.6. *(Teorema d'isomorfisme d'anells) Sigui $f : A \to B$ un morfisme d'anells. Hi ha un morfisme canònic $\overline{f} : A/\ker f \to Imf$.*

Demostració. Definim $\overline{f}(\overline{a}) = f(a)$, aplicant la proposició anterior al morfisme $\tilde{f} : A \to \mathrm{Im}(f) \subseteq B$ (vam veure que la imatge era un subanell) com a ideal triem $I = \ker f$ (ho vam comprovar en proposicions anteriors). Llavors tenim: $\overline{f} := \varphi$. φ és exhaustiu perquè $\tilde{f}$ ho és i és injectiu perquè $\ker \varphi = \{\overline{a} : \varphi(\overline{a}) = 0\} = \{\overline{a} : \tilde{f}(\overline{a}) = 0\} = \{\overline{a} : f(a) = 0\} = \overline{0}$, perquè els elements a tals que $f(a) = 0$ pertanyen al nucli i, per tant, en aquest cas, en el $\overline{0}$. □

2.6 Ideals íntegres, primers i maximals

Definició 2.6.1. Un divisor de zero en un anell A és un element $a \in A$, $a \neq 0$ tal que $ab = 0$ per algun $b \in A$, $b \neq 0$.

Definició 2.6.2. Un anell íntegre és un anell sense divisors de zero.

Definició 2.6.3. Un ideal $\mathfrak{p} \subset A$ d'un anell qualsevol s'anomena primer si $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Anomenarem l'espectre de A $\mathrm{Spec}(A) = \{\mathfrak{p} \subset A; \mathfrak{p} \text{ primer}\}$

Proposició 2.6.4. *Sigui $\mathfrak{p} \subset A$ un ideal. Llavors $\mathfrak{p}$ primer $\iff$ $A/\mathfrak{p}$ és un anell íntegre.*

Demostració. $\implies$ Siguin $\overline{a}, \overline{b} \in A/\mathfrak{p}$ tal que $\overline{a}, \overline{b} \neq \overline{0}$. Suposem que $\overline{a}\overline{b} = \overline{0} \implies \overline{ab} = \overline{0} \implies ab \in \overline{0} = \mathfrak{p} \implies a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Però això voldria dir que o a o b pertanyen a la classe del 0, contradicció amb el que hem suposat.

$\impliedby$ Suposem que $ab \in \mathfrak{p} \implies \overline{a}\overline{b} = \overline{ab} = \overline{0} \implies$ per ser $A/\mathfrak{p}$ íntegre, o a o b són de la classe del 0, per tant, o un o l'altre pertanyen a $\mathfrak{p}$. □

Definició 2.6.5. Un ideal $m \subset A$ s'anomena maximal si no està contingut en cap altre ideal propi d'A.

Proposició 2.6.6. *$m \subset A$ és un ideal. Llavors, m maximal $\iff$ A/m és un cos.*

Demostració. $\Longleftarrow$ Suposem $m \subsetneq J$ ideal, per tant, $\exists x \in J \setminus m$ per tant, $x \notin m \implies \bar{x} \neq 0 \implies \exists \bar{y} \neq 0$ tal que $\bar{x}\bar{y} = 1 \implies u = 1 - xy \in J$, llavors $1 = u + xy$, com és suma de dos elements de J, $1 \in J \implies A = J$.

$\implies$ Els ideals de A/m són de la forma J/m amb $m \subset J$ ideal d'A. Com que m és maximal, o $J = m$ o bé, $J = A$, en el primer cas $J/m = (J)$ i, en el segon, $J/m = A/m$. Per tant, els únics ideals de A/m són el zero i el total $\implies$ A/m és un cos (propietat dels cossos que vam veure). □

Corol·lari 2.6.7. *m maximal $\implies$ m primer.*

2.7 Anell de fraccions

Definició 2.7.1. Sigui A un anell íntegre, $F = A \times (A \setminus \{0\}) = \{(a, s) : a, s \in A, s \neq 0\}$. Definim en F una relació $\sim$ amb $(a, s) \sim (b, t) \iff at - bs = 0$.

Proposició 2.7.2. *La relació $\sim$ és una relació d'equivaléncia.*

Demostració. És reflexiva perquè sempre passa que $at - at = 0$, llavors $(a, t) \sim (a, t)$. És simétrica perquè si $(a, s) \sim (b, t)$ llavors $at - bs = 0$, per tant, $bs - at = 0$ així que $(b, t) \sim (a, s)$. És transitiva perquè si $(a, r) \sim (b, s)$ i $(b, s) \sim (c, t)$, llavors com multipliquem la primera per t i la segona per r (que son diferent de 0). Tenim, $ast - rbt = 0$ i $btr - scr = 0$, que summant-los ens queda $0 = ast - scr = s(at - cr)$, com que $s \neq 0$, ha de ser $at - cr = 0$, per tant, $(a, r) \sim (c, t)$. □

Definició 2.7.3. Sigui $Fr(A) =$ conjunt de classes d'equivaléncia segons aquesta relació i l'anomenarem *fraccions d'A*. $\frac{a}{s} := \overline{(a, s)}$. En $Fr(A)$ definim dues operacions:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Proposició 2.7.4. *Les operacions anteriors estan ben definides.*

Demostració. Per a la suma, com que és simètrica anem a veure només que escollint un representant diferent de la mateixa classe de $\frac{a}{s}$ dona el mateix resultat. Sigui $\frac{c}{r} = \frac{a}{s}$, aleshores, $\frac{c}{r} + \frac{b}{t} = \frac{ct+br}{rt}$, així que sabent que $ar = cs$, volem veure que $st(ct + br) = rt(at + bs)$, aplicant la propietat distributiva ens queda $stct + stbr = rtat + rtbs$ llavors volem veure que $stct = rtat$ i així és perquè subsituint $ar = cs$ ens queda dos termes iguals. Llavors, la suma està ben definida.

Per a la multiplicació igual. Sigui $\frac{c}{r} = \frac{a}{s}$, aleshores, $\frac{c}{r} \times \frac{b}{t} = \frac{bc}{rt}$ i volem veure que $rt(ab) = st(bc)$ però sabent que $cs = ar$ i subsitituint ens queda que la igualtat és certa. □

Aquestes operacions compleixen totes les propietats necessàries per tal que $Fr(A)$ sigui un anell. On el $0_{Fr(A)} = \frac{0}{1}$ i $1_{Fr(A)} = \frac{1}{1}$.

En aquest anell, tot element no nul té invers. Si $\frac{a}{s} = \frac{0}{1}$, llavors $a1 = 0s = 0 \implies a = 0$. Llavors si $\frac{a}{s} \neq \frac{0}{1} \implies a \neq 0$, el seu element invers és $\frac{s}{a}$ ja que $\frac{a}{s}\frac{s}{a} = \frac{1}{1}$, per tant $Fr(A)$ és un cos.

Observació 2.7.5. *Tenim un morfisme natural*

$$i : A \longrightarrow Fr(A)$$
$$a \mapsto i(a) = \frac{a}{1}$$

Aquesta aplicació és un morfisme d'anells (per la definició, l'1_A va a l'$1_{Fr(A)}$, la suma $i(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$ i el producte exactament igual $i(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a) \cdot i(b)$) i és injectiva (perquè si $i(a) = i(b)$ llavors $\frac{a}{1} = \frac{b}{1}$, per tant, $a = b$).

Exemple 5. $\mathbb{Q} := Fr(\mathbb{Z})$ o $Q(x) := Fr(\mathbb{Z}[x])$ o també $Q(x) = Fr(\mathbb{Z}[x])$

Proposició 2.7.6. *(propietat universal del cos de fraccions) Sigui A un anell íntegre.*

(a) Si $f : A \to B$ és un morfisme d'anells tal que $f(A \setminus \{0\}) \subset B^*$ llavors existeix un únic morfisme $\varphi : Fr(A) \to B$ tal que $\varphi \circ i = f$.

(b) Si $i' : A \to F$ és una injecció d'A en un altre cos F tal que satisfà la mateixa la mateixa propietat que $Fr(A)$ de l'apartat (a), és a dir, que si tenim un morfisme d'anells $f : A \to B$ amb imatge a les unitats de B, llavors existeix una única funció ψ tal que $\psi \circ i' = f$. Si això passa, llavors $F' \simeq Fr(A)$.

Demostració. (a) Anem a deduir què ha de ser φ: $\varphi(\frac{a}{b}) = \varphi(\frac{a}{1}\frac{1}{s}) = \varphi(\frac{a}{1})\varphi(\frac{1}{s}) = \varphi(i(a))\varphi(i(s)^{-1}) = f(a)f(s)^{-1}$. Llavors definim $\varphi(\frac{a}{s}) := f(a)f(s)^{-1}$. Cal veure que φ està ben definida, que és un morfisme i és única.

Està ben definida perquè si $\frac{a}{s} = \frac{b}{t}$ llavors volem veure que $f(a)f(s)^{-1} = \varphi(\frac{a}{s}) = \varphi(\frac{b}{t}) = f(b)f(t)^{-1}$. Sabent que f és un morfismes i que $at = bs$, tenim que $f(a)f(t) = f(b)f(s)$. Ara, per hipotesi tenim que tots els elements de la imatge excepte el 0 tenen invers i que tant s com t no poden ser el 0, tenim que $f(a)f(s)^{-1} = f(b)f(t)^{-1}$, que és el que volíem veure.

És un morfisme perquè l'1 va a l'1 ($\varphi(\frac{1}{1}) = f(1)f(1)^{-1} = 1$), la suma a la suma: $\varphi(\frac{a}{s} + \frac{b}{t}) = f(at + bs)f(st)^{-1} = f(at)f(st)^{-1} + f(bt)f(st)^{-1} = f(a)f(t)f(t)^{-1}f(s) + f(b)f(t)f(t)^{-1}f(s) = f(a)f(t)^{-1} + f(b)f(s)^{-1} = \varphi(\frac{a}{t}) + \varphi(\frac{b}{s})$. I el producte al producte: $\varphi(\frac{a}{s} \cdot \frac{b}{t}) = f(ab)f(st)^{-1} = f(a)f(s)^{-1}f(b)f(t)^{-1} = \varphi(\frac{a}{s})\varphi(\frac{b}{t})$.

Ara, suposem que existeix un altre morfisme ψ diferent de φ tal que $f = i \circ \psi$. Per ser diferents, existeix una fracció tal que $\psi(\frac{a}{s}) \neq \varphi(\frac{b}{t})$. Però, per ser morfismes, tant una com l'altra les podem escriure com $\psi(\frac{a}{s}) = \psi(\frac{a}{1} \cdot \frac{1}{s}) = \psi(\frac{a}{1})\psi(\frac{1}{s})$. Aquí, cal fer un incís, $1_B = \psi(\frac{1}{1}) = \psi(\frac{s}{1}\frac{1}{s}) = \psi(\frac{s}{1})\psi(\frac{1}{s})$, d'aquets dos últims factors, sabem que el primer té invers perquè és igual a $f(s)$, aleshores: $\psi(\frac{s}{1})^{-1} = \psi(\frac{1}{s})$. Retornant a l'igualtat que ens haviem deixat, $\psi(\frac{a}{s}) = \psi(\frac{a}{1})\psi(\frac{s}{1})^{-1} = f(a)f(s)^{-1} = \varphi(\frac{a}{s})$, per tant, les dues funcions són la mateix i sempre tenen la mateixa imatge.

(b) Com que tant i com i' són dos morfismes amb imatge a les unitats, tenim que existeixen unes úniques funcions $\varphi : Fr(A) \to F$ i $\psi : F \to Fr(A)$ tal que $\varphi \circ i = i'$ i al revés, $\psi \circ i' = i$. Llavors, fixem-nos que $\psi \circ \varphi \circ i = i$ (substituint). Però fixem-nos també que la propietat universal també la podem aplicar amb dues vegades el mateix conjunt $Fr(A)$ i la seva inclusió, aleshores, la funció $\psi \circ \varphi$ és l'única que compleix la propietat que $\psi \circ \varphi \circ i = i$, però triviament la identitat també, així que son la mateix funció ($\psi \circ \varphi = \mathrm{Id}_{Fr(A)}$). Similarment escollint F dues vegades, tenim que $\varphi \circ \psi = \mathrm{Id}_F$. Amb això i sabent que composició de morfismes és morfisme tenim que $Fr(A) \simeq F$. □

2.8 Anell factorial

La motivació d'aquesta secció és la de veure en quins anells tenim un teorema fonamental de l'aritmètica com tenim en els enters. El teorema fonamental de l'aritmètica diu el següent: tot nombre enter $m \in \mathbb{Z}$ diferent de 0 té una única factorització com a producte de factors primers. $m = \pm p_1^{e_1} \cdots p_r^{e_r}$ amb p_i primers i $e_i > 0$, llevat d'ordre i signe.

Definició 2.8.1. Un element $a \neq 0 \in A$ és irreductible si

(1) a no és una unitat ($a \notin A^*$).

(2) Si podem escriure $a = bc$ llavors b o c son unitats ($\in A^*$)

Definició 2.8.2. Un element $a \neq 0 \in A \setminus A^*$ és primer si (a) és un ideal primer.

Proposició 2.8.3. *Si A és un anell íntegre: a primer $\implies$ a irreductible.*

Demostració. Suposem que $a = bc$ llavors $bc \in (a)$ llavors, per ser (a) un ideal primer, o bé b, o bé c pertanyen a (a). Sense pérdua de generalitat, suposem $b \in (a)$, llavors existeix $d \in A$ tal que $b = ad$, llavors $a = adc$, per tant, $a(1 - dc) = 0 \implies dc = 1$, llavors $c \in A^*$. □

Exemple 6. Considerem l'anell $A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. En aquest anell 2 és irreductible. Suposem que $2 = (\alpha+\beta\sqrt{-5})(\gamma+\delta\sqrt{-5})$, llavors $2 = (\alpha-\beta\sqrt{-5})(\gamma-\delta\sqrt{-5})$, per tant, $4 = (\alpha^2+5\beta^2)(\gamma^2+5\delta^2)$, que és una igualtat entre enters positius llavors els divisors son 1,2 o 4. Fixem-nos que 2 no es pot escriure de la forma $1 \leq \alpha^2 + 5\beta^2 \leq 4$, per tant, els factors son 4 i 1, com que $1 \in \mathbb{Z}[\sqrt{-5}]^*$ és una unitat, 2 és irreductible. En canvi, 2 no és primer, perquè $2|6$ però com $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, però 2 no divideix a cap dels dos perquè 2 no divideix a 1.

Definició 2.8.4. Un anell factorial (o domini de factorització única - DFU, UFD) és un anell íntegre en el qual cada element no nul admet una factorització única en producte d'elements irreductibles, llevat d'ordre i de producte per unitats.

Definició 2.8.5. Dos elements $a, b \in A$ són associats si $\exists n \in A^*$ tal que $a = nb$.

Proposició 2.8.6. *A factorial, $p \in A$ primer $\iff$ p irreductible.*

Demostració. Com hem vist en la proposició anterior, la implicació cap a la dreta és certa per qualsevol anell íntegre. Ara, suposem que tenim p irreductible i que $p|ab$ llavors existeix $d \in A$ tal que $pd = ab$, com que A és factorial, p és un dels irreductible en la factorització d'ab i, la factorització d'ab és la que s'obté ajuntant les d'a amb b (perquè és única). Per tant, p apareix en la factorització d'a o de b, per tant, divideix un o l'altre. □

Proposició 2.8.7. *Siguin A un anell factorial, p, q irreductibles no associats $a \in A$. Si $p|a$ i $q|a$, llavors $pq|a$. En general, si $p_1, \cdots, p_n$ irreductibles no associats dos a dos, si tots divideixen a a ($p_i|a$), llavors la multiplicació de tots divideix a a.*

Demostració. La mateixa demostració serveix en tots dos casos. Tenim que A és un anell factorial, aleshores a té una factorització única en elements irreductibles, com que p_1 és irreductible i divideix a a, ha de ser un d'aquests elements. Ara, això passa per tots, com que no són associats entre ells, si $p_2|a = p_1a_1$, tenim que (per ser p_2 primer que no divideix a p_1) $p_2|\frac{a}{p_1} = a_1$, repetint el mateix argument per inducció tenim que $p_n|\frac{a}{\prod p_1\cdots p_{n-1}} = a_{n-1}$, llavors finalment, podem escriure que $a = a_n \prod p_1 \cdots p_n$, és a dir, que la multiplicació divideix a a. □

Definició 2.8.8. $a, b \in A$, direm que $m \in A$ és màxim comú divisor (mcd, gcd) d'a i b si

1. $m|a$ i $m|b$.
2. Si $c|a$ i $c|b$, llavors $c|m$.

Exemple 7. No sempre existeix. Per exemple, en l'anell $A = \mathbb{Z}[\sqrt{-5}]$, $2|6$, $2|2+2\sqrt{-5}$ i $1+\sqrt{-5}|6$ i $1+\sqrt{-5}|2+2\sqrt{-5}$ i tant 2 com $1+\sqrt{-5}$ són irreductibles i, per tant, no es divideixen entre ells. Llavors el $\gcd(6,2+2\sqrt{-5})$ no existeix.

Definició 2.8.9. Un element $M \in A$ és mínim comú multiplie (MCM, LCM) d'a i b si

1. $a|M$, $b|M$.
2. Si $a|c$, $b|c$, llavors $M|c$.

Proposició 2.8.10. *Sigui A un anell principal, $a, b \in A$.*

a) Sigui $(a) + (b) = (m)$, llavors m és mcd d'a i b.

b) Sigui $(a) \cap (b) = (M)$, llavors M és MCM d'a i b.

Demostració.

a) Tenim que $a, b \in (m)$, llavors $m|a$ i $m|b$. Suposem que tenim c tal que $c|a$ i $c|b$, llavors $a, b \in (c)$, per tant, $(m) = (a) + (b) \subset (c)$, aleshores, $m \in (c) \implies c|m$.

b) Tenim que $M \in (a)$ i $M \in (b)$, llavors $M = ak = bl$, per tant, $a|M$ i $b|M$. Ara, suposem que $a|c$ i $b|c$ llavors $c \in (a) \cap (b) = (M)$, llavors $c = Mn$, per tant, $M|c$.

□

Definició 2.8.11. Dos ideals I, J d'un anell A s'anomenen coprimeres si $I + J = A$. Dos elements $a, b \in A$ s'anomenen coprimers si $(a) + (b) = (1) = A$.

En aquest cas tindrem una identitat de Bézout.

$$\exists \lambda, \mu \quad \lambda a + \mu b = 1$$

En general, si $(a) + (b) = (m)$, $\exists \lambda, \mu \in A$ tal que $\lambda a + \mu b = m$.

Lema 2.8.12. *Sigui A DIP (un anell íntegre i principal) i $a \in A$. Aleshores*

$$a \text{ irreductible} \iff a \text{ primer}$$

Demostració. Només cal veure $\implies$ perquè el recíproc és sempre cert per anells íntegres.

Suposem que $a|bc$ i a no divideix a b. Tenim $(a) + (b) = (d)$, llavors $a \in (d) \implies d|a \implies d \in A^*$ o bé que $d = au$ amb $u \in A^*$, perquè a és irreductible. Però com que $b \in (d) \implies d|b$, però $au = d|b$ llavors $a|b$ cosa que contradiu amb la hipotesi que a no divideix a b.

Per tant, $d \in A^* \implies (d) = A = (1)$, podem suposar que $d = 1$. Per la identitat de Bézout, $\exists \lambda, \mu \in A$ tal que $\lambda a + \mu b = 1$. Llavors, $\lambda ac + \mu bc = c$, ara, com que $a|bc$ per hipotesi i $a|ac$ tenim que $a|c$. □

Proposició 2.8.13. *A DIP. Aleshores*

$$a \text{ irreductible} \iff a \text{ primer} \iff (a) \text{ maximal}$$

Demostració. $\impliedby$) Suposem (a) maximal *implies* $A/(a)$ és un cos, com que tot cos és íntegre, (a) és primer.

$\implies$) Suposem que a és irreductible i suposem que existeix un element b tal que $(a) \subsetneq (b) \subsetneq A$, llavors $a \in (b)$ que implica que existeix un element k tal que $a = bk$, però com que a és irreductible, o bé $k \in A^*$, que voldria dir que $(a) = (b)$ o bé $b \in A^*$ que voldria dir que $(b) = A$. Llavors hem arribat a contradicció i (a) és maximal. □

Teorema 2.8.14. *A DIP $\implies$ A DFU*

Demostració. Sigui $a \in A \setminus A^*$. Hem de veure que a té una única factorització en producte d'irreductibles. Si a és irreductible, ja estem.

Si a no és irreductible, llavors $a = a_1 a_1'$ amb $a_1, a_1' \notin A^*$ (aleshores $(a) \subsetneq (a_1)$ i $(a) \subsetneq (a_1')$). Suposem que a_1 no és irreductible, llavors $a_1 = a_2 a_2'$ amb $a_2, a_2' \notin A^*$. Repetim aquest procés per tots els elements no irreductibles que vagi trobant. Si en algun moment elements són irreductibles, ja tindrem la factorització d'a.

Podria passar que no acabèssim mai? Llavors tindriem elements $a, a_1, \cdots$ tal que

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_r) \subsetneq \cdots$$

que és una cadena infinita ascendent d'ideals. Considerem $I = \cup_i (a_i)$ sí que és ideal en aquest cas. A principal, $I = (b)$, llavors $b \in I = \cup_i (a_i) \implies \exists i_0$ tal que $b \in (a_{i_0}) \implies (b) \subset (a_{i_0}) \subset \cup (a_i) = b$ per tant, $(b) = (a_{i_0}) \subsetneq (a_{i_0+1}) \subset I = (b)$, contradicció perquè la inclusió no és estricte. Aleshores, les cadenes sempre són finites i a té almenys una factorització.

Unicitat de la factorització: suposem que $p_1, \cdots, p_r = q_1 \cdots q_s$ amb p_i, q_j irreductibles. $p_1 | p_1 \cdots p_r = q_1 \cdots q_s$, com que estem en un DIP, p_1 és primer, llavors $p_1 | q_j$ per algun j, per ser q_j irreductible $p_i = u q_j$ amb $u \in A^*$. Cancel·lem p_1 i q_j i repetim el procés fins a veure que cada p_i és igual a un altre q_j excepte per unitats (i que $r = s$). □

2.9 Anell euclidià

Definició 2.9.1. A és una anell euclidià si tenim una funció $\delta : A \setminus \{0\} \to \mathbb{N}$ tal que

1. $\delta(a) \leq \delta(ab)$ $\forall a, b \in A \setminus \{0\}$
2. $\forall a, b \in A$ $b \neq 0$ $\exists q, r \in A$ tal que $a = bq + r$ i $r = 0$ o bé $\delta(r < \delta(b)$.

Aleshores, δ és una norma d'A.

Exemple 8. En el enters podem fer valor absolut i en el anell de polinomis sobre un cos, la funció que retorna el grau del polinomi. Per cossos, simplement la funció 0 compleix els requisits.

Teorema 2.9.2. *Un anell euclidià és principal i, per tant, factorial.*

Demostració. Sigui $I \subset A$ un ideal no nul. Sigui $m = \min\{\delta(a) : a \in I\} = \min \delta(I) \subset \mathbb{N}$, per tant, aquest mínim existeix. Sigui $c \in I$ tal que $\delta(c) = m$, veurem que $I = (c)$. Donat $a \in I$ qualsevol, $\exists q, r \in A$ tal que $a = cq + r$ amb $\delta(r) < \delta(c)$ o $r = 0$. En el primer cas, com que $r = a - cq \in I$ llavors $\delta(r) \geq \delta(a)$, per ser mínim, però això contradiu l'algoritme de la divisió, per tant, no pot ser. En el segon cas, $r = 0$, $a \in (c)$, és a dir, $(c) = I$. □

Corol·lari 2.9.3. $\mathbb{Z}[\sqrt{-5}]$ *no és euclidià. La gran majoria d'anells quadràtics no són euclidians.* $\mathbb{Z}[\sqrt{d}]$, *amb* $d \equiv 2, 3(4)$ *i* $d \in \mathbb{Z}$, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *i* $d \equiv 1(4)$.

Proposició 2.9.4. *Propietats bàsiques de* $K[x]$, K *un cos*

1. $f, g \in K[x]$, *amb* $f, g \neq 0$ *llavors* $\deg(fg) = \deg f + \deg g$
2. $f \in K[x]$ $n = \deg f$ *llavors* f *té com a molt* n *arrels diferents,*
3. *Identitat de Bezout. Donats* $f, g \in K[x]$ *existeix un únic polinomi mónic* $h(x) \in K[x]$ *i polinomis* $\lambda(x), \mu(x) \in K[x]$ *tal que*

$$h(x) = mcd(f(x), g(x)) = \lambda(x)f(x) + \mu(x)g(x)$$

Demostració.

1. Això és degut a que tot cos és íntegre i si $f = ax^n + \cdots$ (amb $a \neq 0$) i $g = bx^m + \cdots$ (amb $b \neq 0$), és a dir, $\deg f = n$ i $\deg g = m$. Tenim que $fg = abx^{n+m} + \cdots$, amb $ab \neq 0$. Així que almenys té grau igual a la suma de graus. No té grau més gran perquè ha de venir de la suma de dos nombres menors o iguals que n i m respectivament.
2. Anem a veure primer el lema següent:

   Lema 2.9.5. $f(\alpha) = 0 \iff x - \alpha | f(x)$
   Demostració. $\Longleftarrow$) Si $f(x) = (x - \alpha)g(x)$ llavors $f(\alpha) = 0g(\alpha) = 0$.
   $\Longrightarrow$) Ara, com que $K[x]$ és euclidià amb $\delta(f) = \deg(f)$. Tenim que $f(x) = (x - \alpha)q(x) + r(x)$, amb $r(x) = c$ un sol terme de grau 0. I com que $f(\alpha) = (\alpha - \alpha)q(\alpha) + c \implies c = 0$. Per tant, $x - \alpha | f(x)$. □

   Ara, siguin $\alpha_1, \ldots, \alpha_m$, m arrels diferents, llavors no són associats i totes divideixen a f, per una proposició anterior, la multiplicació de totes divideix a f. Ara, com que $\prod(x - \alpha_i) | f(x)$, tenim que $f(x) = g(x) \prod(x - \alpha_i)$, per l'apartat anterior, $n = \deg(f) = \deg(g) + \deg(\prod(x - \alpha_i)) = \deg(g) + m$, per tant, $m \leq n$.
3. El ser $K[x]$ euclidià, és factorial i per tant, tot element no nul té una factorització única en irreductibles (o primers). Llavors el mínim comú divisor sempre existeix i és únic, ja que és el la unió de tots els primers compartits (amb la multiplicitat compartida més gran que tinguin els dos alhora). Llavors, com és principal $(h(x)) = (f(x)) + (g(x))$ i per tant, $h \in (f(x)) + (g(x))$, és a dir, h es pot escriure com a suma de dos elements, un de $(f(x))$ i un de $(g(x))$.

□

Nota. Podem trobar $\lambda(x), \mu(x)$ amb $\deg(\lambda(x)) \leq \deg(g(x))$ i $\deg(\mu(x)) \leq \deg(f(x))$.

2.10 Polinomis amb coeficients en un anell factorial

Sigui A un anell factorial $K = Fr(A)$ el cos de fraccions.

Definició 2.10.1. El *contingut* d'un polinomi $f(x) = \sum a_i x^i \in A[x]$ és

$$c(f) := \text{mcd}(a_0, a_1, \cdots, a_n)$$

Observació 2.10.2. *Està determinat llevat d'unitats.*

Definició 2.10.3. Direm que $f(x) \in A[x]$ és primitiu si $c(f)$ és una unitat.

Lema 2.10.4. *Lemma de Gauss. Si $f, g \in A[x]$ són primitius, llavors fg és primitiu.*

Demostració. Tenim que $f(x) = \sum_{j=0}^{m} a_j x^j$ i que $g(x) = \sum_{j=0}^{n} b_j x^j$, llavors $f(x)g(x) = \sum_{j=0}^{m+n} c_j x^j$ on $c_j = \sum_{k=0}^{j} a_k b_{j-k}$.

Si $p(x)q(x)$ no fos primitiu, existiria $p \in A$ irreductible tal que $p|c(fg)$. Llavors $p|c_0$, $p|c_1$, $\cdots$, $p|c_{m+n}$. $r = \min\{j : p \nmid a_j\}$ i $s = \min\{j : p \nmid b_j\}$. Aleshores, $c_{r+s} = a_0 b_{r+s} + \cdots + a_r b_s + \cdots + a_{r+s} b_0$. Els primers són dividits per p perquè $p|a_{j<r}$ i els últims també perquè $p|b_{j<s}$. Per tant, p sí divideix a $a_r b_s$ i per tant, o bé divideix a a_r o a b_s, contradicció. □

Proposició 2.10.5. *Tot polinomi $f(x) \in K[x]$ es pot escriure de manera única (llevat d'unitat d'A) com*

$$f(x) = c f_0(x) \; c \in K \; f_0(x) \in A[x] \text{ primitiu}$$

Demostració. (Obviant l'abús de notació) Sigui $d \in A$ tal que $g(x) = df(x) \in A[x]$ (ha d'existir, almenys multiplicant tots el denominadors). Sigui $k = c(g(x))$, llavors $g_0(x) = \frac{1}{k} g(x) \in A[x]$ és primitiu, i $f(x) = \frac{k}{d} g_0(x) = \frac{k}{d} \left(\frac{d}{k} f(x)\right)$.

Unicitat: Suposem que $c_1 f_1(x) = c_2 f_2(x)$ amb $c_1, c_2 \in K$, $f_i(x) \in A[x]$ primitiu. Podem suposar que $c_1, c_2 \in A$ i que són coprimers (si tenen factors comuns, els podem simplificar). Sigui $p \in A$ irreductible tal que $p|c_1$

$$p|c_1 \implies p|c_2 f_2(x) \implies p|c(c_2 f_2(x)) = c_2 c(f_2(x)) = c_2$$

Per tant, $c_1 \in A^*$. Simétricament $c_2 \in A^*$. Llavors, si les dues són la mateixa factorització. Naturalment, si $f(x) \in A[x]$ la descomposició serà

$$f(x) = c(f(x)) \left(\frac{1}{c(f(x))} f(x) \right)$$

□

Corol·lari 2.10.6. *$f(x), g(x) \in A[x]$ i $c(f(x)g(x)) = c(f(x))c(g(x))$.*

Demostració. $f(x) = a f_0(x)$ i $g(x) = b g_0(x)$, on $a = c(f)$ i $b = v(g)$, $f_0, g_0 \in A[x]$ primitius. Per tant, $f(x)g(x) = (ab)(f_0(x)g_0(x)) \implies ab = c(f(x)g(x))$ (per unicitat). □

Proposició 2.10.7. *$f(x) \in A[x]$ primitiu, llavors $f(x)$ és irreductible en $A[x]$ si i només si $f(x)$ irreductible en $K[X]$.*

Demostració. $\Longleftarrow$) Trivial per subconjunt.

$\Longrightarrow$) Suposem $f(x) = a(x)b(x)$ amb $a(x), b(x) \in K[x]$ (amb els graus menors o iguals que 1), llavors $a(x) = \alpha a_0(x)$ i $b(x) = \beta b_0(x)$, $\alpha, \beta \in K$ i $a_0(x), b_0(x) \in A[x]$ primitius. $f(X) = \alpha\beta a_0(x) b_0(x)$, posem $\alpha\beta = \frac{\gamma}{\delta}$ amb $\gamma, \delta \in A$ coprimers, llavors $\delta f(x) = \gamma a_0(x) g_0(x)$, com que la banda de l'esquerra està a $A[x]$ la dreta també. $\delta = c(\delta f(x)) = c(\gamma a_0(x) b_0(x)) = \gamma$. Per tant, $f(x) = a_0(x) b_0(x)$ i f irreductible en $A[x]$, llavors o bé, $a_0(x) \in A[x]^* = A^*$ (llavors el grau de a_0 és 0), o bé $b_0(x) \in A[x]^* = A^*$ (llavors el grau de b_0 és 0). □

Teorema 2.10.8. *A és un anell factorial, aleshores $A[x]$ és factorial.*

Demostració. Sigui $f(x) \in A[x]$ qualsevol. $f(x) = c(f(x))f_0(x)$ (descomposició única) i $f_0(x) \in A[x]$ primitiu. Per una banda, $c(f) = p_1^{e_1} \cdots p_r^{e_r}$ descomposició en irreductibles en A. $f_0(x) \in A[x] \subset K[x] \implies f_0(x) = h_1(x)^{n_1} \cdots h_s(x)^{n_s}$, $h_i(x) \in K[x]$ irreductible ($K[x]$ és euclidià i, per tant, factorial). Però cada $h_i \in K[x]$ es pot escriure com $kg_i(x)$, amb $k \in K$ i $g_i(x) \in A[x]$ primitiu i irreductible en $K[x]$, per tant, també en $A[x]$. A més, podem escriure $mf_0(x) = lg_1(x)^{n_1} \cdots g_s(x)^{n_s}$, amb $l, m \in A$, però veient el contingut dels polinomis a banda i banda, com són primitius tots ens queda que $l = m$, aleshores hem descomposat $f_0(x)$ de manera única en $A[x]$, llevat d'ordre i unitats. Finalment, $f(x) = p_1^{e_1} \cdots p_r^{e_r} g_1(x)^{n_1} \cdots g_s(x)^{n_s}$. La unicitat ve donada per la unicitat de les dues composicions. □

Corol·lari 2.10.9. *A factorial, llavors $A[x_1, \cdots, x_n]$ és factorial*

Demostració. $A[x_1, \cdots, x_n] = A[x_1, \cdots, x_{n-1}][x_n]$ i inducció. □

2.11 Criteris d'irreductibilitat.

Sigui A un anell factorial i $K = Fr(A)$.

Proposició 2.11.1. *Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ i suposem que $\alpha = \frac{u}{v} \in K$ és una arrel, amb u i v coprimers, llavors $u|a_0$ i $v|a_n$.*

Demostració. Tenim que $f(\alpha) = 0 \implies a_0v^n + a_1v^{n-1}u + \cdots + a_{n-1}vu^{n-1} + a_nu^n = 0$. Com que $v|a_0v^n + \cdots + a_{n-1}vu^{n-1}$ i $a_nu^n = a_0v^n + \cdots + a_{n-1}vu^{n-1}$, llavors $v|a_nu^n$ i com que u, v son coprimers $v|a_n$.

Anàlogament s'obté $u|a_0$. □

Teorema 2.11.2. *Criteri d'irreductibilitat d'Eisenstein. Sigui $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ $p \in A$ primer, si $p|a_0$, $p|a_1$, $\cdots$, $p|a_{n-1}$, si $p \nmid a_n$ i $p^2 \nmid a_0$, llavors $f(x)$ és un polinomi irreductible en $K[X]$.*

Demostració. Podem suposar que $f(x)$ és primitiu i demostrarem que és irreductible en $A[x]$. Suposem que $f(x) = q(x)h(x)$ amb $q(x) = \sum_{i=0}^{r} b_ix^i$ i $h(x) = \sum_{i=0}^{s} c_ix^i$ amb $r \geq 1$ i $s \geq 1$. Com que f primitiu, g i h son primitius.

Tenim que $a_0 = b_0c_0$ i $p|a_0$ i $p^2 \nmid a_0$. Llavors podem suposar que $p|c_0$ però $p \nmid b_0$. Com que $p \nmid a_n$ tenim que $p \nmid c_s$. Ara sigui $t = \min\{j : p \nmid c_j\} < s < r + s = n$. $a_t = b_0c_t + b_ic_{t-1} + \cdots + b_tc_0$ (ha d'existir perquè h és primitiu). Com que tenim $a_t = b_0c_t + b_1c_{t-1} + \cdots + b_tc_0$, amb p que divideix a a_t i divideix a $c_0, \cdots, c_{t-1}$, per tant, divideix a b_0c_t però com que no divideix a b_0 ha de dividir a c_t, contradicció amb que t és el mínim tal que $p \nmid c_t$, per tant, $f(x)$ no és irreductible. □

Lema 2.11.3. *(extensió de morfismes a l'anell de polinomis). A, B anells qualssevol. Sigui $f : A \to B$ un morfisme.*

$$\tilde{f} : A[x] \to B[x]$$
$$\sum a_ix^i \mapsto \sum f(a_i)x^i$$

és un morfisme d'anells

Demostració. Tenim que $\tilde{f}(1_A) = f(1_A) = 1_B$ que és l'element neutre de $B[x]$.

Sigui $p = a_0 + a_1x + \ldots + a_nx^n$ i $q = b_0 + b_1x + \ldots + b_mx^m$. Ara

$$\tilde{f}(p + q) = \sum f(a_i + b_i)x^i = \sum f(a_i)x^i + \sum f(b_i)x^i = \tilde{f}(p) + \tilde{f}(q)$$

I

$$\tilde{f}(pq) = \tilde{f}\left(\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right)\right) = \sum_{k=0}^{n+m} f\left(\sum_{l=0}^{k} a_l b_{k-l}\right) x^k =$$

$$= \sum_{k=0}^{n+m}\left(\sum_{l=0}^{k} f(a_l) f(b_{k-l})\right) x^k = \left(\sum_{i=0}^{n} f(a_i) x^i\right)\left(\sum_{j=0}^{m} f(b_j) x^j\right) = \tilde{f}(p)\tilde{f}(q)$$

Aleshores, és un morfisme d'anells. □

Teorema 2.11.4. *Criteri de reducció. A, B anells amb A factorial. I sigui $\varphi : A \to B$ un morfisme (directament tenim també $\tilde{\varphi}$). $f(x) \in A[x]$ tal que*

1. $\deg \tilde{\varphi}(f) = \deg f$.
2. *$\tilde{\varphi}(f)$ irreductible.*

Demostració. Suposem que $f(x) = a(x)b(x)$ en $A[x]$. Llavors

$$\tilde{\varphi}(f(x)) = \tilde{\varphi}(a(x))\tilde{\varphi}(b(x))$$

Com que $\tilde{\varphi}(f(x))$ irreductible tenim que el grau de $\tilde{\varphi}(a(x)) = 0$ o el grau de $\tilde{\varphi}(a(x)) = 0$. Com que $\deg \tilde{\varphi}(f(x)) = \deg f(x)$, llavors, com que el graus dels polinomis no poden creixer, $\deg \tilde{\varphi}(a(x)) = \deg a(x)$ i $\deg \tilde{\varphi}(b(x)) = \deg b(x)$. Per tant, $\deg a(x) = 0$ o bé $\deg b(x) = 0$ que és el que volíem veure per tal que $f(x)$ fos irreductible. □

Exemple 9. Tenim $f(x) = x^5 + 2x + 6$, modul 5 és $f(x) \equiv (x^4 + 3x^3 + 4x^2 + 2x + 3)(x + 2)$ i módul 11 $f(x) \equiv (x^3 + 8x^2 + 6x + 2)(x^2 + 3x + 2)$ son irreductibles respectivament. Llavors f és irreductible perquè les descomposicions son incompatibles per grau.

Capítol 3

Cossos

3.1 Motivació

Per agafar idees, abans de començar, anem a veure alguns exemples com a motivació del capítol.

Exemple 10. Sigui $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}\}$, aquest anell és un cos perquè és isomorf a $\mathbb{Q}[x]/(x^3 - 2)$, ja que $x^3 - 2$ és irreductible a $\mathbb{Q}$ (2-Einstein) i, per tant, l'ideal és maximal i el quocient és un cos. A més, podem veure-ho com un espai vectorial: $\mathbb{Q}\langle 1, \sqrt[3]{2}, \sqrt[3]{2}\rangle$, $3 = \dim Q[\sqrt[2]{3}$.

Sigui $J = e^{2\pi i/7}$, que és una solució de $x^7 - 1 = (x-1)(x^6 + \ldots + x + 1)$, però com que no és solució del primer factor, ho és del segon terme ($f(x)$). A més, aquest segon és irreductible a $\mathbb{Q}$, ja que, $f(x+1) = \frac{(x+1)^7 - 1}{x}$, tots els termes són múltiples de 7, excepte el terme dominant, i el terme independent és 7. Llavors és 7-Einstein. Llavors $\mathbb{Q}[J] = \mathbb{Q}\langle 1, J, \ldots, J^5\rangle = \mathbb{Q}[x]/f(x)$.

És $\mathbb{Q}(\pi)$ un cos? Ho és si, i només si $a \in \mathbb{Q}(\pi)$ tal que $a\pi = 1$, reordenant, només passa si existeix algun $f(x) \in \mathbb{Q}(\pi)$ tal que $f(\pi) = 0$.

3.2 Extensió d'un cos

Definició 3.2.1. Direm que el cos F és una extensió del cos K si $K \subset F$, és a dir, si K és un subcos de F. Ho denotarem com F/K.

En aquesta situació tenim una aplicació.

$$\begin{aligned} K \times F &\to F \\ (\lambda, \alpha) &\mapsto \lambda\alpha \end{aligned}$$

que li dona a F estructura de K-e.v.

Definició 3.2.2. Direm que F/K és una extensió finita si $\dim_K F < +\infty$ i, en aquest cas, anomenarem grau de l'extensió a aquesta dimensió

$$[F : K] := \dim_K F$$

Si $\dim_K F = +\infty$, diem que F és una extensió infinita de K.

Exemple 11. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{R}\langle 1, i\rangle$. Com que $1, i$ són $\mathbb{R}$-l.i. Llavors $[\mathbb{C}, \mathbb{R}] = 2$.

El cos $\mathbb{Q}(x_1, \ldots)$ (polinomis d'infinites variables) és una extensió infinita de $\mathbb{Q}$. Si hi hagués una base finita d'aquesta extensió involucra una quantitat finita de x.

Proposició 3.2.3. *F/K i H/F extensió de cossos ($K \subset F \subset H$). L'extensió H/K és finita $\iff$ H/F, F/K són extensions finites. I quan ho és $[H : K] = [H : F][F : K]$.*

Demostració. $\Longrightarrow$) Suposem H/K una extensió finita $F \subset H$ és un sub k-e.v. d'H. Llavors com que $\dim_K F \leq \dim_K H < +\infty$ tenim que F/K és una extensió finita. Siguin $w_1, \ldots, w_n$ una K-base d'H. $H = K\langle w_1, \ldots, w_n\rangle \subseteq F\langle w_1, \ldots, w_n\rangle \subseteq H$. $w_1, \ldots, w_n$ són generadors d'H (encara que siguin F-l.d.) llavors $\dim_F H \leq n < +\infty$.

$\Longleftarrow$) Suposem que $r = [F : K] < +\infty$, $s = [H : F] < +\infty$. Agafem una K-base d'F, $\alpha_1, \ldots, \alpha_r \in F$ i una F-base $\beta_1, \ldots, \beta_s \in H$. Cal veure que $\{\alpha_i\beta_j\}_{ij}$ és una K-base d'H. Això implicarà que $[H : K] = rs < +\infty$. Suposem que son l.d.

$$\sum_{ij} \lambda_{ij}\alpha_i\beta_j = 0 \qquad \lambda_{ij} \in K$$

Podem escriure-ho com:

$$0 = \sum_j \left(\sum_i \lambda_{ij}\alpha_i \right) \beta_j$$

Com que el que hi ha dintre del parentesis és part de F i les β són F-l.i., els coeficient ha de ser 0. Per tant, per cada j.

$$\sum_i \lambda_{ij}\alpha_i = 0$$

I com que les λ son de K i les α són K-l.i. llavors són totes 0, que és el que volíem veure.

A més, fàcilment es veu que $\{\alpha_i\beta_j\}$ són generadors, ja que podem escriure qualsevol $a \in H$ com $a = a_1\beta_1 + \ldots + a_s\beta_s$, amb $a_i \in F$, per tant, podem escrire $a_i = a_{i1}\alpha_1 + \ldots + a_{ir}\alpha_r$, amb $a_{ij} \in K$. □

3.3 Algebraic i transcendent

Definició 3.3.1. Sigui L/K una extensió. Direm que $\alpha \in L$ és algebraic de K $(/K)$ si α és arrel d'un polinomi amb coeficients a K. En cas contrari direm que α és transcedent $/K$. Anotarem $\overline{K} = \{$ elements algebraics $/K\}$.

Exemple 12. $\sqrt{2}$ és algebraic sobre $\mathbb{Q}$ perquè $f(x) = x^2 - 2$ compleix que $f(\sqrt{2}) = 0$. π també és algebraic sobre $\mathbb{R}$ però no sobre $\mathbb{Q}$.

Definició 3.3.2. Si $\alpha \in F$ és un element algebraic $/K$ anomenarem polinomi irreductible d'α/K $Irr(\alpha, k, x)$ al polinomi mònic de $K[X]$ de menor grau que té α com arrel.

Observació 3.3.3. *El polinomi irreductible és únic.*

Demostració. Així és perquè si n'hi haguéssin dos, al fer-ne la resta tindriem un polinomi diferent de 0 amb grau menor (perquè al ser els dos mónics hem reduit almenys un grau) que té per arrel α llavors, cap dels dos seria el menor. □

Proposició 3.3.4. *Podem caracteritzar el polinomi irreductible d'una altra manera:*

$$\begin{aligned} \varphi_\alpha : K[X] &\to F \\ p(x) &\mapsto p(\alpha) \end{aligned}$$

Fixem-nos que φ_α és un morfisme d'anells. Llavors $p(x)$ és el polinomi irreductible $\mathrm{Irr}(\alpha, k, x)$ *si i només si* $\ker \varphi_\alpha = (p(x))$.

Demostració.

$\Longrightarrow$) Està clar que si $p(x)$ és el polinomi irreductible, qualsevol polinomi $D(x)$ tal que $D(\alpha) = 0$ és un múltiple seu. Ja que sinò, al estar en un anell euclidià podem fer la divisió de polinomis, dividim $p(x)$ a $D(x)$, ens queda que $D(x) = p(x)q(x) + r(x)$, on $r(x)$ és diferent de 0 i, per tant, de grau menor que $p(x)$ i fixem-nos que també és anul·lat per α $(0 = D(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha))$, aleshores hauriem arribat a contradicció amb que $p(x)$ era el polinomi irreductible d'α. Per tant, el nucli de l'aplicació φ_α són els múltiples de $p(x)$.

$\Longleftarrow$) Com que, pel primer teorema d'isomorfisme tenim que

$$K[x]/(p(x)) \simeq \operatorname{Im}\varphi_\alpha \subset F$$

i F és un cos, en particular, tenim que és íntegre, per tant, $\operatorname{Im}\varphi_\alpha$ és íntegre, llavors $p(x)$ és primer i com estem en $K[x]$ que és un euclidià, en particular, factorial, primer és el mateix que irreductible. □

Definició 3.3.5. Siguin K i L dos cossos tals que L/K i sigui $\alpha \in L$. El cos generat per α i per K és el menor que conté α i K. Se'l denota com:

$$K(\alpha) = \{\frac{p(\alpha)}{q(\alpha)} : p, q \in K[x], q(\alpha) \neq 0\}$$

I sigui $K[\alpha]$ l'espai vectorial sobre el cos K, generat amb $\langle 1, \alpha, \alpha^2, \ldots\rangle$.

Proposició 3.3.6. *Si α és algebraic $K(\alpha) \simeq K[x]/\operatorname{Irr}(\alpha, K, x)$. Si α és transcendent llavors $K[\alpha] \simeq K[x]$.*

Demostració. Al ser α algebraic podem escriure α^n com a combinació lineal en K de potencies inferiors de n, on n és el grau de $\operatorname{Irr}(\alpha, K, x)$. Llavors $K(\alpha) = K\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$. Que és el mateix que $K[x]/\operatorname{Irr}(\alpha, k, x)$.

Altrament, si no α no fos transcendent tindriem que $K[\alpha]$ és isomorf a $K[x]$ fent el canvi formal de x a α sense poder determinar cap valor perquè no s'anul·la mai. □

Proposició 3.3.7. *$\alpha \in L/K$. Llavors α és algebraic $/K \iff K(\alpha) = K[\alpha] \iff K(\alpha)/K$ és una extensió finita.*

Demostració.

(1) $\implies$ (2) Cal veure que si $q(x) \in K[x]$ tal que $q(\alpha) \neq 0$, llavors $\frac{1}{q(\alpha)} \in K[\alpha]$. Sigui $f(x) = \operatorname{Irr}(\alpha, k, x)$ $q(\alpha) \neq 0 \implies f(x) \nmid q(x) \implies \operatorname{mcd}(f(x), q(x)) = 1$ Llavors $\exists \lambda(x), \mu(x) \in K[x]$ tal que $\lambda(x)f(x) + \mu(x)q(x) = 1$ (per Bezout)

$$\lambda(\alpha)f(\alpha) + \mu(\alpha)q(\alpha) = 1 \implies \frac{1}{q(\alpha)} = \mu(\alpha) \in K[\alpha]$$

(2) $\implies$ (3) $\frac{1}{\alpha} \in K[\alpha] \implies \frac{1}{\alpha} = \sum_{i=0}^{n-1} a_i\alpha^i \implies 1 = \sum_{i=0}^{n-1} a_i\alpha^{i+1} \implies \alpha^n = \frac{-1}{a_{n-1}}(\sum_{i=0}^{n-1} a_i\alpha^i - 1)$. Per inducció, $\forall k \geq n$, $\alpha^k \in K\langle 1, \ldots, \alpha^{n-1}\rangle$. Llavors $K(\alpha) = K[\alpha] = K\langle 1, \ldots, \alpha^{n-1}\rangle \implies [K(\alpha) : K] < +\infty$.

(3) $\implies$ (1) Si $n = [K(\alpha) : K] < +\infty$. $1, \alpha, \alpha^2, \ldots, \alpha^n$ han de ser linealment dependents. Llavors existeix una combinació lineal que és 0 i aquest és el polinomi tal que $f(\alpha) = 0$. □

Lema 3.3.8. *$L/M/K$ extensió de cossos*

$$\alpha \in L \text{ algebraic } /K \implies \alpha \text{ algebraic } /M$$

Demostració. Els elements de K són també de M. Si tenim un polinomi en K que és anul·lat per α també el tenim en M. □

Proposició 3.3.9. *L/K extensió de cossos, si α, β algebraic sobre $/K$, llavors $\alpha \pm \beta$, $\alpha\beta$, α/β és algebraic sobre K*

Demostració. Fixem-nos que $K(\alpha)(\beta)$ és una extensió finita de K. Per una banda, perquè els coeficients ja són una extensió finita de K. Per altra, com que β anul·la un cert polinomi amb coeficient a K, el mateix polinomi està inclós a $K(\alpha)(\beta)$. Per tant, podem escriure un certa potencia de β com a combinació lineal en K de les anteriors. A més, com que $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$ (perquè és un cos i aquests elements apareixen), per tant $K()$ d'aquests elements sobre K és una extensió finita, per la proposició anterior, son algebraics. □

Definició 3.3.10. Fixem una K-base $w_1, \dots, w_r$ de L. Donat $\alpha \in L$ considerem l'aplicació

$$\begin{aligned} w_\alpha : L &\to L \\ x &\mapsto w_\alpha(x) := \alpha x \end{aligned}$$

w_α és una aplicació K-lineal del K-e.v. L en ell mateix. Per tant, es pot escriure com una matriu respecte la base $w_1, \dots, w_n$

$$w_\alpha(w_i) = \sum a_{ij} w_j \to M_\alpha = (a_{ij})_{ij}$$

és la representació matricial de x en la base $w_1, \dots, w_n$.

Proposició 3.3.11. *L'aplicació*

$$\begin{aligned} \mathbf{M} : L &\to \mathcal{M}_n(K) \\ \alpha &\mapsto M_\alpha \end{aligned}$$

és un morfisme injectiu d'anells (depèn de la base triada). Tenim que per $\alpha \neq 0$ $M_\alpha \in Gl_n(K)$ és inverible. Si $\alpha, \beta \in L$, tenim que $M_\alpha M_\beta = M_\beta M_\alpha$.

Demostració. Sigui $w_1, \dots, w_n$ una base, anem a veure que $\mathbf{M}$ és un morfisme. Si $\alpha = 1_L$, com que $w_\alpha(w_i) = w_i$, llavors $M_\alpha = \mathrm{Id}$. A cada columna de $(\alpha + \beta)$ tenim $w_{\alpha+\beta}(w_i) = (\alpha+\beta)w_i = \alpha w_i + \beta w_i = w_\alpha(w_i) + w_\beta(w_i)$, per tant, $\mathbf{M}(\alpha+\beta) = \mathbf{M}(\alpha) + \mathbf{M}(\beta)$. Semblant amb el producte, tenim que a la fila i-éssima de M_α hi ha els elements de la forma (a_{ik}) per $k = 1, \dots, n$ i a la columna j-éssima de M_β hi ha els elements (b_{kj}) per $k = 1, \dots, n$. Així que $M_\alpha M_\beta = (\sum_{k=1}^n a_{ik} b_{kj})_{ij}$. Mentre que a les columnes de $M_{\alpha\beta}$ hi ha:

$$w_i \alpha\beta = w_\beta(w_\alpha(w_i)) = w_\beta(\sum_{k=1}^n a_{ik} w_k) = \sum_{k=1}^n a_{ik}(w_\beta(w_k)) = \sum_{k=1}^n a_{ik}(\sum_{j=1}^n b_{kj} w_j) = \sum_{j=1}^n w_j(\sum_{k=1}^n a_{ik} b_{kj})$$

Fixant la fila i tenim que a la posició i, j de la matriu $M_{\alpha\beta}$ hi ha $(\sum_{k=1}^n a_{ik} b_{kj})$. Llavors hem vist que $\mathbb{M}(\alpha\beta) = \mathbb{M}(\alpha)\mathbb{M}(\beta)$ que és el que ens faltava per veure que és un morfisme.

Per veure que és injectiu, suposem que $\mathbb{M}(\alpha) = \mathbb{M}(\beta)$ llavors α per cada matriu de base dona el mateix que β per cada matriu de la base. En particular, $\alpha w_1 = \beta w_1$, llavors $\alpha = \beta$.

La inversa de M_α és $M_{\alpha^{-1}}$ perquè per morfisme tenim $M_\alpha M_{\alpha^{-1}} = M_{\alpha\alpha^{-1}} = M_1 = \mathrm{Id}$.

I tenim que el producte és comutatiu perquè $w_\alpha \circ w_\beta = w_{\alpha\beta} = w_\beta \circ w_\alpha$, llavors com que a cada columna de $M_\alpha M_\beta$ com a cada columna de $M_\beta M_\alpha$ tenim $w_{\alpha\beta}$ son iguals i el producte commuta. □

Corol·lari 3.3.12. *Si $\alpha = \sum \lambda_i w_i$ $M_\alpha = \sum \lambda_i M_{w_i}$.*

Demostració. Tenim que $\mathbf{M}$ és un morfisme. Llavors $\mathbf{M}(\alpha) = \mathbf{M}(\sum \lambda_i w_i) = \sum \lambda \mathbf{M}_{w_i}$. □

Proposició 3.3.13. *El polinomi $\mathrm{Irr}(\alpha, k, x)$ coincideix amb el polinomi mínim de M_α. En particular, els VAP's de M_α són les arrels de $\mathrm{Irr}(\alpha, k, x)$.*

Demostració. Sigui $p(x) = \mathrm{Irr}(\alpha, k, x)$, com que $\mathbf{M}$ és un morfisme, $0 = \mathbf{M}(0) = \mathbf{M}(p(\alpha)) = p(\mathbf{M}(\alpha))$. En particular, $p(x)$ és el mínim perquè si un polinomi és anul·lat per M_α és multiple del mínim, però $p(x)$ és irreductble i mónic.

Els VAP's de M_α són les arrels del polinomi mínim, per tant, les arrels de $\mathrm{Irr}(\alpha, k, x)$. □

3.4 Teorema de l'element primitiu

Aquest exemple dóna pas al teorema d'aquesta secció, el qual, per simplicitat, no farem la versió més general

Exemple 13. Tenim que $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$ i volem saber quin grau és $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Fixem-nos que $[\mathbb{Q}(\sqrt{3})(\sqrt{2}):\mathbb{Q}(\sqrt{3})] = 2$ perquè, per una banda no pot ser més gran de 2 perquè hi ha un polinomi irreductible x^2-2 que s'anul·la amb $\sqrt{2}$ i no pot ser de grau 1, perquè arrel de 2 no es pot escriure com combinació d'1 i $\sqrt{3}$. Llavors, com que els graus es multipliquen K té grau 4.

I $\mathbb{Q}(\sqrt{2}+\sqrt{3})$? Sigui $\alpha = \sqrt{2}+\sqrt{3}$, per una banda és fàcil veure que $\alpha^4 - 10\alpha^2 + 1$ és el polinomi irreductible α en $\mathbb{Q}$. Llavors $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ té grau 4. Però com que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}.\sqrt{3})$, per grau, tenim que els dos últims són iguals. Així que tenim un base per $\mathbb{Q}(\sqrt{2},\sqrt{3})$ que és $\mathbb{Q}\langle 1,\alpha,\alpha^2,\alpha^3\rangle$.

Lema 3.4.1. *Si* $\operatorname{char} K = 0$ *tot polinomi irreductible /*K *és separable (té totes les arrels diferents).*

Demostració. Si α fos arrel doble d'un factor $f(x) \in K[x]$ irreductible i $f'(x)$ la seva derivada. Tenim que

$$h(x) := \operatorname{mcd}(f(x), f'(x))$$

tindrà grau major o igual que 1 (perquè els dos tenen almenys una arrel en comú). Però com que f és irreductible, tenim que $h(x) = f(x)$ llavors $f(x)|f'(x)$. Però com que el grau de $f'(x)$ és més petit estricte que el grau de $f(x)$, la derivada ha de ser 0 i, per tant, per la característica k, $f(x)$ és una constant, així que no pot tenir una arrel doble. □

Teorema 3.4.2. *Teorema de l'element primitiu. Sigui* K *un cos amb* $\operatorname{char} K = 0$ *i sigui* L/K *una extensió finita. Llavors, existeix un element* $\gamma \in L$ *tal que* $L = K(\gamma)$*. És a dir,* L *és el cos generat per* K *i* γ*.*

Demostració. L/K finita $\implies$ $L = K(\alpha_1,\ldots,\alpha_n)$ per algunes $\alpha_i \in L$.

Raonarem per inducció, d'aquesta manera només caldria saber reduir de $K(a_1,a_2)$ a $K(b)$ $(a_1,a_2,b \in L)$. Així tindriem el cas base de la inducció, mentre que el cas general es demostra utilitzant que sempre podem escriure les extensions com a producte d'extensions, és a dir, $K(\alpha_1,\ldots,\alpha_n) = K(\alpha_1,\ldots,\alpha_{n-1})(\alpha_n)$ i, per hipotesi d'inducció $K(\alpha_1,\ldots,\alpha_{n-1}) = K(\beta)$ i pel cas base $K(\beta)(\alpha_n) = K(\gamma)$.

Suposem, doncs, que $L = K(\alpha,\beta)$ i busquem γ tal que $L = K(\gamma)$. És a dir, γ de la forma $\gamma = \alpha + c\beta$ per algun $c \in K$. Ho farem veient que $\beta \in K(\gamma)$, perquè llavors $\alpha = \gamma - c\beta \in K(\gamma)$ i, per tant, $K(\alpha,\beta) \subset K(\gamma)$.

Donat una γ així, siguin $f(x) = \operatorname{Irr}(\alpha,K,x) \in K[x]$, $g(x) = \operatorname{Irr}(\beta,K(\gamma),x) \in K(\gamma)[x]$ i $h(x) = f(\gamma - cx) \in K(\gamma)[x]$. Fixem-nos que $\deg g(x) = 1 \iff \beta \in K(\gamma)$. Suposem que $\beta \notin K(\gamma)$, és a dir, $\deg g(X) > 1$. Pel lema anterior, les altres arrels de $g(x)$ són diferents de β ($\beta' = \beta$ (*) amb $g(\beta') = 0$). A més tenim que $h(\beta) = (f(\gamma - c\beta) = f(\alpha) = 0 \implies g(x)|h(x)$ (perquè tots els polinomis que s'anul·len amb β són multiples de $g(x)$), per tant, també tenim que $h(\beta') = 0$. Així que $\alpha' = \gamma - c\beta'$ és una altra arrel de $f(x)$, substituint $\alpha' = \alpha + c\beta - c\beta'$, llavors ens queda que $c = \frac{\alpha'-\alpha}{\beta-\beta'}$. Per tant, si $\beta \notin K(\gamma)$, c ha de tenir aquesta forma (diferència d'arrels de f / diferència d'arrels de g), de les quals només n'hi ha un nombre finit. Fixem-nos ara que $\operatorname{char} K = 0$, llavors $\mathbb{Q} \subset K$, per tant, el cardinal de K és $+\infty$. Aleshores, segur que existeix alguna c que no és d'aquesta forma. El $\gamma = \alpha + c\beta$ corresponent satisfà $\beta \in K(\gamma)$.
□

Observació 3.4.3. *El teorema de l'element primitiu és vàlid en qualsevol extensió* L/K *finita i separable (tots els polinomis irreductibles d'*$\alpha \in L$ *són separables). Això inclou les extensions de cossos finits.*

Capítol 4

Grups

Capítol 5

Moduls