Estructures Algebraiques

Xavier Povill Clarós

27 de juny de 2021

Índex

1 Introducció

En aquesta assignatura estudiarem les operacions i estructures elementals.

En un principi, l'operació més intuitiva és la suma en els nombres naturals. Més tard, per representar el concepte de deutes, es va necessitar la resta, i es van introduir els nombres enters per permetre la resta de qualsevol parella de nombres.

Per agilitzar la suma, sorgeix la multiplicació, i el seu invers la divisió. Per tal de poder dividir dos nombres qualssevol, s'introdueixen els nombres racionals.

A partir d'aquestes estructures bàsiques es poden obtenir estructures més complexes. Per exemple, es poden completar els racionals per obtenir els reals, però també es poden obtenir altres cossos complets com els nombres p-àdics. A partir dels reals, s'obtenen els complexos, que es corresponen a la seva clausura algebraica.

Altres maneres de generar noves estructures són el pas al quocient (per passar de $\mathbb{Z}$ a $\mathbb{Z}/p\mathbb{Z}$), o els anells de polinomis, com $\mathbb{Z}[x]$ o $\mathbb{R}[x]$. A partir d'un anell qualsevol també es poden obtenir altres tipus d'estructures, com les fraccions polinòmiques ($A(x)$), les sèries de potències ($A[[x]]$) o les sèries de Laurent ($A\{\{x\}\}$).

En aquest curs també treballarem amb els mòduls, que són una espècie d'anàleg dels espais vectorials però amb els escalars en un anell.

1.1 Propietats de $\mathbb{Z}$

- És Abelià
- És íntegre ($ab = 0 \implies a = 0 \vee b = 0$)
- Té elements primers
- És factorial (qualsevol enter es pot descomposar com a producte de primers de manera

única)

- Té divisió euclidiana
- Hi falten inversos (per la multiplicació)
- Falten arrels de polinomis
- No és complet

1.2 Operacions i les seves propietats

Totes les estructures algebraiques es defineixen a partir d'operacions en conjunts. Per tant, té sentit preguntar-se primer què és una operació en abstracte i quines propietats pot satisfer.

Definició 1.2.1 (Operació)**.** Una *operació* en un conjunt A és una aplicació $\varphi : A \times A \longrightarrow A$

Una operació pot satisfer algunes de les següents propietats:

- Propietat commutativa: $\forall a, b \in A$, $\varphi(a, b) = \varphi(b, a)$
- Propietat associativa: $\forall a, b, c \in A$, $\varphi(a, \varphi(b, c)) = \varphi(\varphi(a, b), c)$
- Element neutre: $\exists e \in A$ tal que $\forall a \in A$, $\varphi(e, a) = \varphi(a, e) = a$
- Element invers: $b \in A$ és invers de $a \in A$ si $\varphi(a, b) = \varphi(b, a) = e$
- Propietat de l'invers: Es diu que φ en A té la propietat de l'invers si tot element de A té element invers per φ.

Proposició 1.2.1. *Si existeix element neutre, aquest és únic.*

Demostració. Siguin e i e' elements neutres de l'operació φ. Aleshores, $e = \phi(e, e') = e'$ □

Proposició 1.2.2. *Si existeix element invers d'un $a \in A$, aleshores aquest element invers és únic.*

Demostració. Exercici. □

1.3 Estructures algebraiques bàsiques

- **Grup**: $(G, \star)$ amb EN, PA, PI.
- **Semigrup**: $(G, \star)$ amb EN, PA.
- **Grup Abelià**: Grup amb PC.
- **Anell**: $(A, +, \star)$ on $(A, +)$ és un grup Abelià, $(A, \star)$ és un semigrup, i $\star$ és distributiva per les dues bandes respecte $+$.

- **Anell commutatiu**: Anell on $\star$ té la PC. (*En aquest curs sovint ens referirem als anells commutatius simplement com anells.*)
- **Cos**: Anell $(K, +, \star)$ on $K \setminus \{0\}$ és un grup Abelià.
- **Mòdul**: $(M, +)$ és un mòdul sobre l'anell A si $(M, +)$ és un grup Abelià i existeix una multiplicació per escalars $A \times M \longrightarrow M$.
- **Espai vectorial**: Mòdul sobre un cos (en lloc d'un anell).

Propietats de la multiplicació per escalars en un mòdul:

i) $a(m_1 + m_2) = am_1 + am_2$

ii) $(a + b)m = am + bm$

iii) $a(bm) = (ab)m$

iv) $1_A m = m$

2 Anells

La definició d'anell s'ha donat en el capítol anterior. D'ara endavant farem servir la notació $(A, +, \cdot)$ per representar un anell, i ens referirem a l'element neutre de la suma com 0_A i a l'element neutre del producte com 1_A.

Per representar l'element invers de $a \in A$ respecte a la suma (l'oposat), utilitzarem la notació $-a$, i per representar l'element invers respecte al producte utilitzarem a^{-1}. En general, denotarem per A^* el conjunt d'elements d'A que tenen invers (les *unitats* d'A). Observem que $(A^*, \cdot)$ sempre és un grup Abelià.

2.1 Propietats dels anells

Començarem demostrant una sèrie de propietats bàsiques dels anells:

Proposició 2.1.1. *1.* $\forall a, b \in A, \quad a + b = a + c \implies b = c$

2. $\forall a \in A, \quad 0_A \cdot a = 0_A$

3. $\forall a \in A, \quad (-1_A)(-a) = a$

4. $\forall a \in A, \quad (-1_A)a = -a$

Demostració. 1. $a+b = a+c \implies -a+(a+b) = -a+(a+c) \implies 0_A+b = 0_A+c \implies b = c$

2. $0_A \cdot a = (0_A + 0_A) \cdot a = 0_A \cdot a + 0_A \cdot a \underset{(1)}{\implies} 0_A = 0_A \cdot a$

3. Exercici.

4. Exercici.

□

Alguns exemples d'anells són $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $M_{n\times n}(A)$ amb A anell, $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 : a \in \mathbb{Z},\ \zeta := e^{2\pi i/5}\}$, $\mathbb{Z}/n\mathbb{Z}$, etc.

Observem que els elements neutres de les dues operacions han de ser diferents si volem que l'anell no sigui trivial:

Proposició 2.1.2. *Sigui A un anell. Si $0_A = 1_A$, aleshores $A = \{0_A\}$.*

Demostració. Exercici. □

Definició 2.1.1. Si $n \in \mathbb{Z}$ i $a \in A$, definirem

$$na := \begin{cases} \underbrace{a + \cdots + a}_{n \text{ cops}}, & \text{si } n > 0 \\ \underbrace{-a + \cdots + -a}_{|n| \text{ cops}}, & \text{si } n < 0 \\ 0_A, & \text{si } n = 0 \end{cases}$$

Anàlogament, per representar el producte repetit definim

$$a^n := \begin{cases} \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ cops}}, & \text{si } n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{|n| \text{ cops}}, & \text{si } n < 0 \\ 1_A, & \text{si } n = 0 \end{cases}$$

Definició 2.1.2 (Característic)**.** Diem que l'anell A té característic 0 si $n1_A \neq 0_A$ per tot $n \in \mathbb{Z}^+$. En cas contrari, direm que A té característic m si m és el menor nombre enter positiu tal que $m1_A = 0_A$.

Observació. Per qualsevol $a \in A$, es compleix que $\text{char}(A)a = 0_A$ (ja que podem expressar a com $1_A \cdot a$).

Definició 2.1.3 (Subanell)**.** Un *subanell* d'un anell A és un subconjunt $S \subseteq A$ tal que

- $1_A \in S$
- $\forall a, b \in S, \quad a - b \in S$
- $\forall a, b \in S, \quad a \cdot b \in S$

Observació. Donat un $S \subseteq A$, podria semblar que S és subanell de $A \iff S$ és un anell. Observem que això és fals en general, ja que S pot ser un anell i no contenir 1_A (condició necessària per ser subanell de A). Per exemple, podem prendre $A = \mathbb{Z}/6\mathbb{Z}$ i $S = \{0, 3\} \subset A$. Observem que S és un anell, ja que podem prendre $1_S = 3_A$, però en canvi $1_A \notin S$.

Exemple 2.1.1.

- $\mathbb{Z}$ és subanell de $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ que és subanell de $\mathbb{C}$.
- $2\mathbb{Z}$ no és un subanell de $\mathbb{Z}$ perquè no conté el $1_{\mathbb{Z}}$.

Definició 2.1.4 (Anell producte)**.** Donats dos anells A, B, el seu *anell producte* és el conjunt $A \times B$ amb les operacions

$$(a_1, b_1) + (a_2, b_2) \mapsto (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \cdot (a_2, b_2) \mapsto (a_1 \cdot a_2, b_1 \cdot b_2)$$

Es pot comprovar que amb aquestes operacions $A \times B$ és efectivament un anell.

Per productes finits, es pot aplicar la operació anterior repetidament, però per productes infinits s'ha d'anar en compte perquè podria no convergir.

A continuació veurem una de les definicions més interessants del capítol:

Definició 2.1.5 (Ideal)**.** Sigui A un anell. Un subconjunt $I \subseteq A$ es diu que és un *ideal* si

- $u \in I, \alpha \in A \implies \alpha u \in I$
- $u, v \in I \implies u + v \in I$

Aquestes dues condicions són equivalents a dir que

$$\forall u, v \in I, \forall \alpha, \beta \in A, \quad \alpha u + \beta v \in I$$

El concepte d'ideal va ser desenvolupat per Krönecker quan intentava provar el teorema de Fermat, ja que es va adonar que la propietat de factorització en primers estava relacionada amb aquest tipus de conjunts, que ell va denominar *nombres ideals*.

Alguns exemples d'ideals són

- $\{0_A\}$ (o *ideal zero*) i A (o ideal total)
- $2\mathbb{Z} \subset \mathbb{Z}$, o en general $m\mathbb{Z}$.
- *Ideal generat per* $a \in A$: $(a) := \{am : m \in A\}$
- *Ideal generat per* $a_1, \ldots, a_n \in A$: $(a_1, \ldots, a_n) := \{a_1 m_1 + \cdots + a_n m_n : m_i \in A\}$
- Donat $\alpha \in \mathbb{Q}$, $I = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\}$, que és l'ideal de $\mathbb{Q}[x]$ generat pel polinomi $x - \alpha$.
- $I = \{f(x, y) \in \mathbb{Q}[x][y] : f(0, 0) = 0\}$, ideal de $\mathbb{Q}[x, y]$ generat per (x, y).

Proposició 2.1.3. *Donats dos ideals* $I, J \subseteq A$*,*

1. $I + J := \{a + b : a \in I, b \in J\}$ *és un ideal i és el menor ideal que conté* I *i* J*.*
2. $I \cdot J := \{\sum_{i=1}^{k} a_i b_i : k < \infty, a_i \in I, b_i \in J\}$ *és un ideal.*

Demostració. Exercici. □

Observació. En general, $I \cup J$ no és un ideal.

Proposició 2.1.4. *Sigui $a \in A$ anell, i $u \in A^*$. Aleshores, $(a) = (u \cdot a)$.*

Demostració. Exercici. □

Exemple 2.1.2. Observem que, a $\mathbb{R}[x]$, $(x) = (3x)$, però a $\mathbb{Z}[x]$ no, ja que 3 no és una unitat.

Proposició 2.1.5. *A és un cos sii els seus únics ideals són 0 i A.*

Demostració. Sigui $I \subset A$ un ideal no nul. Sigui $x \in I$, $x \neq 0$. Si A és un cos, $\exists x^{-1} \in A$, i per tant $1 = x^{-1}x \in I$ i aleshores I és el total.

Per veure la implicació contrària, suposem que tot ideal és o bé el zero o el total. Aleshores, sigui $x \in A$ amb $x \neq 0$, tenim que $(x) = A$. Per tant, $1 \in (x) \implies \exists\, y \in A$ tal que $yx = 1$ i, per tant, $x \in A^*$. Com que aquest argument val per qualsevol $x \in A \setminus \{0\}$, A és un cos. □

Definició 2.1.6 (Ideal principal)**.** Direm que un ideal I de l'anell A és *principal* si existeix un $m \in A$ tal que $I = (m)$ (és a dir, I és l'ideal generat per m).

Proposició 2.1.6. *Tots els ideals de $\mathbb{Z}$ són principals.*

Demostració. Sigui $I \subset \mathbb{Z}$ un ideal. (0) és òbviament principal. Podem suposar per tant que $I \neq (0) \implies \exists\, x \in I$ tal que $x \neq 0$. Observem que $x \in I$ sii $-x \in I$, de manera que

$$I^+ := \{x \in I : x > 0\} = I \cap \mathbb{N} \neq \emptyset$$

Pel principi de bona ordenació dels naturals, tot subconjunt de $\mathbb{N}$ té un element mínim. Sigui $m = \min I^+$. $m \in I \implies \forall\, k \in \mathbb{Z}$, $mk \in I$. Per tant, $(m) \subseteq I$.

En tindríem prou amb veure la inclusió contrària (que $I \subseteq (m)$). Sigui $y \in I$ tal que $y > 0$. Definim

$$T := \{y - km \geq 0, k \in \mathbb{N}\} \subset \mathbb{N}$$

El conjunt T no és buit, ja que $y \in T$. Aleshores pel principi de bona ordenació també té un mínim. Sigui $r = y - mk_0 = \min T$. Tant y com mk_0 pertanyen a I, de manera que $r \in I$. Si tinguéssim $r \geq m$, llavors $0 \leq y - (k_0 + 1)m < r$, de manera que r no seria el mínim de T. Per tant, tenim que $0 \leq r < m$, i com que $m = \min I^+$, $r = 0$. Això implica que y és múltiple de m, de manera que $y \in (m)$. Com que y era un element qualsevol de I, $I \subseteq (m)$.

Havent vist les dues inclusions, tenim que $I = (m)$ per un cert $m \in \mathbb{Z}$, tal i com volíem demostrar. □

Observació. Observem que la base de la demostració és el fet que a $\mathbb{Z}$ podem dividir per m obtenint un residu r únic. Això ens permet extendre la demostració anterior per tots els anells en els quals es pugui "dividir bé" (els anells que més endavant anomenarem *anells euclidians*). En particular, tenim la següent proposició pels polinomis:

Proposició 2.1.7. *Sigui K un cos. Aleshores tots els ideals de $K[x]$ són principals.*

Demostració. Exercici. S'ha d'adaptar la demostració anterior utilitzant la divisió de polinomis. □

Definició 2.1.7 (Anell principal)**.** Un *anell principal* és un anell on tots els ideals són principals. Per exemple, segons les proposicions anteriors, $\mathbb{Z}$ o $K[x]$ són anells principals.

2.2 Morfismes d'anells

Definició 2.2.1 (Morfisme d'anells)**.** Siguin A i B anells. Una aplicació $f : A \longrightarrow B$ és un *morfisme d'anells* si preserva les operacions de A i B:

- $f(1_A) = 1_B$
- $\forall x, y \in A, \quad f(x + y) = f(x) + f(y)$
- $\forall x, y \in A, \quad f(x \cdot y) = f(x) \cdot f(y)$.

Definició 2.2.2 (Tipus de morfismes)**.**

- *Monomorfisme*: morfisme injectiu.
- *Epimorfisme*: morfisme exhaustiu.
- *Isomorfisme*: morfisme bijectiu.

Exemple 2.2.1. Alguns exemples de morfismes entre anells són els següents:

1. $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ tal que $f(m) = m \cdot 1_{\mathbb{Q}}$
2. En general, per un anell A qualsevol, tenim el morfisme $\phi : \mathbb{Z} \longrightarrow A$ tal que $\phi(m) = m \cdot 1_A$. Aquest morfisme és important, perquè ϕ injectiu sii $\mathrm{char}A = 0$, i $\phi^{-1}(0) = (\mathrm{char}A)$. A més, $\phi(\mathbb{Z})$ és un subanell.
3. Sigui K un cos, $\alpha \in K$, $\phi_\alpha : K[x] \longrightarrow K$ tal que $\phi_\alpha(p(x)) = p(\alpha)$
4. $\mathbb{C} \longrightarrow M_2(\mathbb{R})$ donat per $a + bi \mapsto a\mathrm{Id} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
5. La conjugació complexa (morfisme de $\mathbb{C}$ a $\mathbb{C}$).
6. L'anàleg de la conjugació complexa a $\mathbb{Z}[\sqrt{d}]$ (on $a + b\sqrt{d} \mapsto a - b\sqrt{d}$), demanant que $d \in \mathbb{Z}$ i $d \neq 0$.
7. Sigui $\zeta = e^{2\pi i/5}$ i $k \neq 0 \mod 5$, el morfisme de $\mathbb{Z}[\zeta]$ a $\mathbb{Z}[\zeta]$ donat per $\sum \alpha_i \zeta^i \mapsto \sum \alpha_i \zeta^{ki}$.

Proposició 2.2.1. *Sigui $f : A \longrightarrow B$ un morfisme entre anells. Aleshores,*

1. $f(a^n) = f(a)^n$
2. $a \in A^* \implies f(a) \in B^*$
3. *Sigui J un ideal de B, llavors $f^{-1}(J)$ és un ideal de A.*
4. *Si f és exhaustiu, I ideal de $A \implies f(I)$ ideal de B.*
5. $\ker f$ *és un ideal de A.*

6. $\operatorname{Im} f$ *és un subanell de* B.

7. f *injectiu* $\iff \ker f = 0$

8. *Si* A *és un cos, l'únic morfisme* $f : A \longrightarrow B$ *no injectiu és el morfisme zero.*

Demostració. 1. Exercici.

2. Exercici.

3. Siguin $a_1, a_2 \in f^{-1}(J)$, $\lambda, \mu \in A$. Hem de veure que $\lambda a_1 + \mu a_2 \in f^{-1}(J)$.

$$f(\lambda a_1 + \mu a_2) = \lambda f(a_1) + \mu f(a_2) \in J \implies \lambda a_1 + \mu a_2 \in f^{-1}(J)$$

4. Exercici.

5. Exercici.

6. Exercici.

7. Exercici.

8. Exercici.

□

Observació. En general, la imatge d'un ideal per un morfisme no és un ideal. Per exemple, tenim el morfisme $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$, $a \mapsto a/1$. Observem que $2\mathbb{Z}$ és un ideal de $\mathbb{Z}$ però que la seva imatge no és un ideal de $\mathbb{Q}$ (ja que, per exemple, $\frac{1}{3} \cdot 2 \notin 2\mathbb{Z}$).

2.3 Anell quocient

Definició 2.3.1 (Anell quocient)**.** Sigui A un anell i $I \subset A$ un ideal. A partir de I definim la següent relació d'equivalència: $a \sim_I b \iff a - b \in I$. (Exercici: comprovar que és relació d'equivalència.) Aleshores el conjunt $A/I := A/\sim_I$ juntament amb les dues operacions

$$\overline{a} + \overline{b} := \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

forma un anell, que anomenarem *anell quocient.*

Demostració. En primer lloc, veurem que les operacions estan ben definides. Siguin $a, a' \in \overline{a}$ i $b, b' \in \overline{b}$. Aleshores, $a - a', b - b' \in I$. Per tant,

$$\overline{a'} + \overline{b'} = \overline{a' + b'} = \overline{a + b - (a - a') - (b - b')} = \overline{a + b} = \overline{a} + \overline{b}$$

de manera que la suma no depèn dels representants que escollim. Com a exercici, es pot fer la mateixa comprovació pel producte i comprovar a més que el conjunt A/I amb aquestes dues operacions satisfà totes les propietats de la definició d'anell. □

Exemple 2.3.1. 1. Agafant $A = \mathbb{Z}$ i $I = (m)$, tenim que l'anell quocient A/I és $\mathbb{Z}/m\mathbb{Z}$.

2. Si $A = K[x]$ i $I = (x - \alpha)$ per $\alpha \in K$, aleshores $A/I = K[x]/(x - \alpha)$ és un anell quocient isomorf al cos K.

   Demostració. Sigui $f : K[x]/(x - \alpha) \longrightarrow K$ que envia $\overline{p(x)}$ a $p(\alpha)$. Aquesta aplicació està ben definida, ja que si $q(x) \in \overline{p(x)}$, aleshores $q(x) - p(x) \in (x - \alpha) \implies q(\alpha) - p(\alpha) = 0$. Falta veure que és un isomorfisme, cosa que es deixa com a exercici. □

3. Sigui $A = \mathbb{R}[x]$, $I = (x^2 + 1)$. Aleshores, l'anell quocient $R[x]/(x^2 + 1)$ és isomorf a $\mathbb{C}$. Com a exercici, es pot demostrar que $\overline{p(x)} \mapsto p(i)$ és un isomorfisme.

4. Sigui $I = A \times 0 \subset A \times B$, amb A, B anells. Aleshores $(A \times B)/I \simeq B$.

Proposició 2.3.1. *L'aplicació natural*

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ a &\mapsto \overline{a} \end{aligned}$$

és un morfisme d'anells.

Demostració. Segueix de la definició de les operacions a A/I. □

Per definició, π és exhaustiva, i $\ker \pi = \{a \in A : \overline{a} = \overline{0}\} = \{a \in A : a \in I\} = I$. A més, tenim la següent proposició:

Proposició 2.3.2.

1. *Sigui $J \in A$, un ideal tal que $I \subset J$. Aleshores,*

$$J/I = \pi(J) \subset A/I \text{ és un ideal}$$

2. *Sigui $U \subset A/I$ un ideal. Aleshores existeix un únic ideal $J \subset A$ tal que $J \supset I$ i $J/I = U$.*

Demostració. 1. El morfisme π és exhaustiu, i sabem que la imatge d'un ideal per un epimorfisme és sempre un ideal.

2. Prenem $J := \pi^{-1}(U) \subset A$, que és un ideal pel fet de ser antiimatge d'un ideal. Comprovem que aquest J satisfà les condicions necessàries. Tenim que $J/I = \pi(J) = \pi(\pi^{-1}(U)) = U$ (donat que π és exhaustiva). A més, com $\overline{0} \in U$, $I = \pi^{-1}(\overline{0}) \subset \pi^{-1}(U) = J$.

   Només ens falta demostrar la unicitat de J. Suposem que existeix un altre ideal J' que també satisfà $\pi(J') = U$ i $J' \supset I$. Aleshores, $\pi(J') = U \implies J' \subset \pi^{-1}\pi(J') = \pi^{-1}(U) = J$. Ens falta veure l'altra inclusió. Sigui $a \in J = \pi^{-1}(U)$, aleshores $\pi(a) \in U = \pi(J')$. Per tant, existeix un $x \in J'$ tal que $\pi(x) = \pi(a)$, és a dir, que $x - a \in I \subset J'$. Finalment, com que $a - x \in J'$ i $x \in J'$, tenim que $a \in J'$. Així doncs, $J \subset J'$.

   □

Proposició 2.3.3 (Propietat universal del quocient)**.** *Sigui $f : A \longrightarrow B$ un morfisme d'anells, i sigui $I \subset A$ un ideal tal que $I \subset \ker f$. Aleshores, existeix un únic morfisme $\phi : A/I \longrightarrow B$ tal que $\phi \circ \pi = f$ (és a dir, el diagrama és commutatiu).*

Demostració. Definim $\phi(\overline{a}) = f(a)$. Sigui $b \in \overline{a}$. Aleshores, $b = a + \lambda$, amb $\lambda \in I \subset \ker f$. Aleshores,

$$f(b) = f(a) + f(\lambda) = f(a)$$

i, per tant, $\phi(\overline{a})$ no depèn de l'elecció del representat de $\overline{a}$.

Per altra banda, ϕ és un morfisme, ja que $\phi(\overline{1}) = f(1) = 1$ i

$$\phi(\overline{a} + \overline{b}) = \phi(\overline{a + b}) = f(a + b) = f(a) + f(b) = \phi(\overline{a}) + \phi(\overline{b})$$
$$\phi(\overline{a} \cdot \overline{b}) = \phi(\overline{a \cdot b}) = f(a \cdot b) = f(a) \cdot f(b) = \phi(\overline{a}) \cdot \phi(\overline{b})$$

A més, per construcció, observem que $\phi \circ \pi = f$. Només ens falta demostrar la unicitat. Sigui $\varphi : A/I \longrightarrow B$ que també satisfaci que $\varphi \circ \pi = f$. Aleshores, per qualsevol $\overline{a} \in A/I$,

$$\varphi(\overline{a}) = (\varphi \circ \pi)(a) = f(a) = \phi(\overline{a})$$

de manera que $\varphi = \phi$. □

Amb aquesta proposició es pot demostrar fàcilment el teorema d'isomorfisme:

Proposició 2.3.4 (Teorema d'isomorfisme)**.** *Sigui $f : A \longrightarrow B$ un morfisme d'anells. Aleshores hi ha un isomorfisme canònic*

$$\begin{aligned} \overline{f} : & A/\ker f \longrightarrow \operatorname{Im} f \\ & \overline{a} \mapsto f(a) \end{aligned}$$

Demostració. Considerem el morfisme $f' : A \longrightarrow \operatorname{Im} f \subset B$, i prenem $I = \ker f' = \ker f$. A més, $\operatorname{Im} f = \operatorname{Im} f'$. Per la propietat universal del quocient, existeix un únic morfisme $\phi : A/\ker f' \longrightarrow \operatorname{Im} f'$ tal que $\phi \circ \pi = f'$. Tenim que ϕ és exhaustiu perquè f' ho és, i a més tenim que $\ker \phi = \overline{0}$, de manera que és injectiu. Per tant, ϕ és l'isomorfisme entre $A/\ker f \simeq \operatorname{Im} f$ que a l'enunciat anomenàvem $\overline{f}$. □

2.4 Ideals primers i ideals maximals

Definició 2.4.1 (Divisor de zero)**.** Un *divisor de zero* en un anell A és un element $a \in A$, $a \neq 0$, tal que per un cert $b \in A$, $a \cdot b = 0$.

Exemple 2.4.1. A $\mathbb{Z}/12\mathbb{Z}$, tenim que 3 és un divisor de zero, ja que $3 \cdot 4 = 0$.

Similarment, a $M_2(\mathbb{Q})$ la matriu $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ és un divisor de zero, ja que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

Habitualment ens interessaran els anells on no hi hagi divisors de zero:

Definició 2.4.2 (Anell íntegre)**.** Un *anell íntegre* és un anell sense divisors de zero.

Definició 2.4.3 (Ideal primer)**.** Un ideal $\mathfrak{p} \subset A$ qualsevol es diu que és *primer* si per tot $a, b \in A$, es té que $a \cdot b \in \mathfrak{p} \implies a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

Exemple 2.4.2. A l'anell $\mathbb{Z}$, l'ideal principal (p) generat per un p primer és un ideal primer. De la mateixa manera, a $K[x]$, l'ideal generat per un polinomi irreductible és un ideal primer.

Definició 2.4.4. L'espectre d'un anell A és el conjunt d'ideals primers de l'anell:

$$\operatorname{Spec}(A) = \{\mathfrak{p} \subset A : \mathfrak{p} \text{ ideal}\}$$

L'espectre d'un anell és important en geometria, ja que ens permet trobar les subvarietats de la varietat descrita per l'anell.

Proposició 2.4.1. *Sigui $\mathfrak{p} \subset A$ un ideal. Aleshores, $\mathfrak{p}$ primer $\iff$ $A/\mathfrak{p}$ íntegre.*

Demostració. $\underline{\implies}$ Siguin $\overline{a}, \overline{b} \in A/\mathfrak{p}$. Si $\overline{a} \cdot \overline{b} = \overline{0}$, aleshores $a \cdot b \in \overline{0} = \mathfrak{p} \implies a \in \mathfrak{p}$ o $b \in \mathfrak{p} \implies \overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$. Per tant, $A/\mathfrak{p}$ és íntegre.

$\underline{\impliedby}$ Suposem que $ab \in \mathfrak{p}$. Aleshores, $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{0}$, i com $A/\mathfrak{p}$ és íntegre, això implica que $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$. Per tant, un dels dos pertany a $\mathfrak{p}$, que és la condició que necessitem per dir que $\mathfrak{p}$ és un ideal primer. □

Exemple 2.4.3. Prenent $A = \mathbb{Z}[x]$, tenim que $\mathfrak{p} = (x)$ és primer, ja que $\mathbb{Z}[x]/(x) = \mathbb{Z}$ és íntegre.

Definició 2.4.5 (Ideal maximal)**.** Un ideal $\mathfrak{M} \subset A$ s'anomena *maximal* si no està contingut en cap altre ideal propi de A (és a dir, que si $\mathfrak{M} \subsetneq I$ ideal, $I = A$).

Exemple 2.4.4. A l'anell de polinomis $K[x]$, $\mathfrak{M} = (x)$ és maximal, ja que si $(x) \subsetneq I \implies \exists\, p(x) \in I$ tal que $p(x) \notin (x) \implies p(x) = a_0 + q(x)$ amb $a_0 \in K^*$ i $q(x) \in (x) \implies a_0 = p(x) - q(x) \in I \implies 1 = a_0^{-1} a_0 \in I \implies K[x] = (1, x) \subset I \implies I = K[x]$.

A $\mathbb{Z}[x]$, en canvi, (x) no és maximal. La demostració anterior no val perquè no sabem si existeix un $a_0^{-1} \in \mathbb{Z}$. Per exemple, $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

Com a exercici és interessant demostrar que $(2, x)$ sí que és maximal a $\mathbb{Z}[x]$.

De la mateixa manera que tenim una caracterització dels ideals primers a partir del seu quocient respecte l'anell, també tenim una caracterització del mateix estil pels ideals maximals:

Proposició 2.4.2. *Un ideal $\mathfrak{M} \subset A$ és maximal $\iff$ $A/\mathfrak{M}$ és un cos.*

Demostració. $\underline{\impliedby}$ Suposem $\mathfrak{M} \subsetneq J$ ideal. Aleshores, $\exists\, x \in J \setminus \mathfrak{M}$. Donat que $x \notin \mathfrak{M}$, tenim que $\overline{x} \neq \overline{0}$. Per tant, com que $A/\mathfrak{M}$ és un cos, $\exists\, \overline{y} \neq 0$ tal que $\overline{xy} = \overline{1}$. Aleshores, $u = 1 - xy \in J \implies 1 = u + xy \in J \implies J = A \implies \mathfrak{M}$ és maximal.

$\underline{\implies}$ Els ideals de $A/\mathfrak{M}$ són de la forma $J/\mathfrak{M}$, amb J ideal de A i $\mathfrak{M} \subset J$ (ja que l'aplicació $\pi : A \longrightarrow A/\mathfrak{M}$ és exhaustiva). Donat que $\mathfrak{M}$ és maximal, els únics ideals de $A/\mathfrak{M}$ seran o bé $\mathfrak{M}/\mathfrak{M} = \overline{0}$, o $A/\mathfrak{M}$ que és el total. Com que tot anell que té com a únics ideals el zero i el total és un cos, tenim que $A/\mathfrak{M}$ és un cos. □

Corol·lari 2.4.1. *$\mathfrak{M}$ maximal $\implies$ $\mathfrak{M}$ primer.*

Demostració. Sigui $\mathfrak{M}$ un ideal maximal. Segons la caracterització dels ideals primers donada a la proposició 2.4.1, hem de veure que $A/\mathfrak{M}$ és un anell íntegre.

$\mathfrak{M}$ maximal $\implies$ $A/\mathfrak{M}$ és un cos. Aleshores, donats $a, b \in A/\mathfrak{M}$ tals que $a \cdot b = 0$, o bé $a = 0$, o en cas contrari tenim que $\exists\, a^{-1} \in A/\mathfrak{M} \implies b = 0$. Per tant, $A/\mathfrak{M}$ no té divisors de zero i és un anell íntegre. □

Exemple 2.4.5.

1. (x^2+1) és un ideal maximal de $\mathbb{R}[x]$, ja que $\mathbb{R}[x]/(x^2+1) = \mathbb{C}$ que és un cos.
2. (x^3-2) és un ideal maximal de $\mathbb{Q}[x]$ (exercici), fet que implica que $\mathbb{Q}[x]/(x^3-2) = \mathbb{Q}[\sqrt[3]{2}]$ és un cos.

2.5 Anell de fraccions

Definició 2.5.1 (Anell de fraccions)**.** Sigui A un anell íntegre. Sigui $F = A \times (A \setminus \{0\})$. Definim una relació d'equivalència a F tal que $(a, s) \sim (b, t) \iff at = bs$ (Exercici: veure que és relació d'equivalència).

Aleshores, definim l'*anell de fraccions* de A, $\mathrm{Fr}(A)$ com el conjunt de classes d'equivalència de $F/\sim$. A més, definim la *fracció* $\frac{a}{s}$ com la classe $\overline{(a,s)} \in F/\sim$.

Les operacions d'aquest anell es defineixen com la suma i producte habituals de fraccions d'enters:

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

Per veure que estan ben definides, cal demostrar que el resultat de les operacions no depèn dels representants triats (Exercici). També caldria demostrar que $(\mathrm{Fr}(A), +, \cdot)$ compleix la resta de condicions necessàries per ser un anell (Exercici).

Proposició 2.5.1. *L'anell de fraccions de A és un cos.*

Demostració. Hem de veure que tot element no nul té un invers. Sigui $a/s \in \mathrm{Fr}(A)$. Suposem que $a/s \neq 0_{\mathrm{Fr}(A)} = 0/1 \implies a \neq 0$. Aleshores $s/a \in \mathrm{Fr}(A)$ i $(a/s) \cdot (s/a) = 1/1$. Per tant, s/a és l'invers de a/s. □

Comentari. Degut a la proposició anterior, d'ara endavant ens referirem a $\mathrm{Fr}(A)$ com el *cos de fraccions* de A.

Fins ara no hem relacionat el cos de fraccions amb l'anell A, però observem que amb el morfisme natural

$$A \overset{i}{\hookrightarrow} \mathrm{Fr}(A)$$
$$a \mapsto i(a) = \frac{a}{1}$$

podem incloure l'anell A dins de $\mathrm{Fr}(A)$.

Observem que el morfisme anterior i és injectiu ($i(a) = 0 \iff a = 0$), de manera que habitualment identificarem $a \in A$ amb $a/1 \in \mathrm{Fr}(A)$, i escriurem $a = a/1$ (tot i que tècnicament això seria un abús de notació, ja que els dos costats de la igualtat pertanyen a objectes diferents).

Exemple 2.5.1. Observem que ja hem treballat amb alguns cossos de fraccions sense saber-ho:

- $\mathbb{Q} = \mathrm{Fr}(\mathbb{Z})$
- $\mathbb{Q}(x) := \mathrm{Fr}(\mathbb{Q}[x]) = \mathrm{Fr}(\mathbb{Z}[x])$ (fraccions polinòmiques)
- $\mathbb{Q}(i) = \mathrm{Fr}(\mathbb{Z}[i])$ (enters de Gauss)
- Exercici: trobeu el cos de fraccions de $\mathbb{Q}[[x]]$ (conjunt de sèries de potències amb coeficients racionals).

Per construir fraccions a partir d'anells, a vegades és interessant restringir més els denominadors, i agafar per exemple tots aquells que no són múltiples d'un primer donat. Aquestes construccions no es veuran en aquest curs, però convé saber que existeixen.

A continuació, donem una caracterització del cos de fraccions:

Proposició 2.5.2 (Propietat universal del cos de fraccions)**.** *Sigui A un anell íntegre.*

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

2. *Si $A \overset{i'}{\hookrightarrow} F'$ és una injecció d'A en un cos F' que satisfà 1, aleshores $F' \simeq \mathrm{Fr}(A)$.*

Demostració. 1. Si ϕ fos un morfisme tal que $\phi \circ i = f$, tindríem que $\phi\left(\frac{a}{s}\right) = \phi\left(\frac{a}{1}\right)\phi\left(\frac{1}{s}\right) = \phi(i(a)) \cdot \phi(i(s)^{-1}) = f(a)f(s)^{-1}$. Per tant, definim $\phi\left(\frac{a}{s}\right) := f(a)f(s)^{-1}$ i es pot comprovar que aquesta ϕ està ben definida, que és un morfisme i que satisfà $\phi \circ i = f$ (Exercici). La unicitat la tenim per l'argument que hem fet servir per construir-la.

2. Sigui F' un cos tal que existeix una injecció $A \overset{i'}{\hookrightarrow} F'$ i un morfisme ϕ' que compleix $\phi' \circ i' = f$. Aleshores, utilitzant aquestes hipòtesis i el resultat de l'apartat (a), tenim que el diagrama de la figura 2.1 és commutatiu. Això implica que les composicions $\phi' \circ \phi$ i $\phi \circ \phi'$ són les identitats respecte F' i $\mathrm{Fr}(A)$, de manera que $F' \simeq \mathrm{Fr}(A)$.

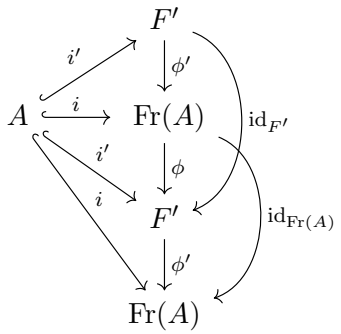


Figura 2.1

□

El que ve a dir aquesta proposició és que el cos de fraccions d'un anell qualsevol és el cos més petit que el conté. Aleshores, per exemple, sabent que $\mathbb{R}$ és un cos que conté $\mathbb{Z}$ i donat que $\mathbb{Q} = \mathrm{Fr}(\mathbb{Z})$, tenim que $\mathbb{R}$ ha de contenir $\mathbb{Q}$.

2.6 Anells factorials

En els enters, sabem que tot nombre es pot descomposar en primers:

Proposició 2.6.1 (Teorema fonamental de l'aritmètica)**.** *Tot nombre enter $m \in \mathbb{Z}$ té una factorització única com a producte de nombres primers*

$$m = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad p_i > 0 \text{ primer}$$

Aquesta proposició ens garanteix que la factorització sempre existeix, però trobar la factorització en sí pot ser molt complicat. Es coneixen algorismes en temps polinòmic per dir si un nombre és primer, però no per trobar la seva factorització. De fet, si es pogués factoritzar un enter en temps polinòmic, es podrien trencar molts sistemes de xifratge (com el RSA).

Definició 2.6.1 (Irreductible)**.** Un element $a \in A$, $a \neq 0$ és *irreductible* si $a \notin A^*$ i

$$a = bc \implies b \in A^* \text{ o } c \in A^*$$

Definició 2.6.2 (Primer)**.** Un element $a \in A$, $a \neq 0$ és *primer* si (a) és un ideal primer.

Proposició 2.6.2. *En un anell íntegre A, $a \in A$ primer $\implies$ a irreductible*

Demostració. Suposem que a és primer. Sigui $a = bc$, aleshores, donat que (a) és un ideal primer,

$$bc \in (a) \implies b \in (a) \text{ o } c \in (a)$$

Suposem spdg que $b \in (a)$. Aleshores, $\exists\, d \in A$ tal que $b = ad$. Per tant,

$$a = bc = adc \implies a(1 - dc) = 0 \implies 1 = dc \implies c \in A^*$$

Per tant, a és irreductible. □

Observem que el recíproc no és cert: no tot element irreductible en un anell íntegre és primer. Un exemple és el següent:

Exemple 2.6.1. Sigui $A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Aleshores, 2 és irreductible, ja que si $2 = (\alpha + \beta\sqrt{-5})(\gamma + \delta\sqrt{-5})$, multipliquem 2 pel seu conjugat complex i obtenim

$$4 = (\alpha^2 + 5\beta^2)(\gamma^2 + 5\delta^2)$$

que és una igualtat a $\mathbb{Z}$. Per tant, $\alpha^2 + 5\beta^2$ només pot ser 1, 2 o 4. Aleshores, $\beta = 0$ i, com que $\alpha \in \mathbb{Z}$, tenim per força que $\alpha = \pm 1$ o $\alpha = \pm 2$. En el primer cas, α és una unitat, mentre que en el segon $\gamma + \delta\sqrt{-5} = \mp 1$, que és una unitat. Per tant, 2 no es pot expressar com a producte de dos elements no invertibles, i 2 és irreductible a $\mathbb{Z}[\sqrt{-5}]$.

En canvi, observem que

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \implies 2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$$

però $2 \nmid 1 \pm \sqrt{-5}$, de manera que 2 no és primer.

Un altre exemple d'elements irreductibles no primers és el següent:

Exemple 2.6.2. Considerem un cos K i l'anell format per $A = K[x^2, x^3]$. L'element x^2 és irreductible a A (A no té polinomis de grau 1), però x^2 no és primer, ja que $x^2 \nmid x^3$ dins de A i en canvi $x^2 \mid x^3x^3 = x^6$.

Exemple 2.6.3. Un últim exemple és l'anell $A = \mathbb{R}[\sin x, \cos x]$, ja que

$$\sin^2 x = (1 + \cos x)(1 - \cos x)$$

i (FALTA)

Definició 2.6.3 (Associats)**.** Direm que dos elements $a, b \in A$ són associats si $\exists\, u \in A^*$ tal que $a = ub$.

Definició 2.6.4 (Anell factorial)**.** Un *anell factorial* (o *domini de factorització única – DFU* o *UFD*) és un anell íntegre en el qual cada element no nul admet una factorització única com el producte d'elements irreductibles (llevat de canvis d'ordre i de producte per unitats).

Observació. Observem que, segons la definició anterior, considerem que un cos és un anell factorial (tot i que un anell factorial avorrit, perquè tots els elements són unitats i no hi ha irreductibles).

Proposició 2.6.3. *Sigui A un anell factorial. Aleshores, p primer $\iff$ p irreductible*

Demostració. La implicació cap a la dreta ja l'hem vista en anells íntegres (i un anell factorial és per definició íntegre), de manera que només hem de demostrar la implicació cap a l'esquerra.

Sigui p irreductible. Suposem que $p \mid ab$. Aleshores existeix un $d \in A$ tal que $pd = ab$. Observem que la factorització de ab és única, de manera que és la que s'obté ajuntant les factoritzacions de a i b. Per tant, p apareix o en la factorització de a o en la de b, de manera que $p \mid a$ o $p \mid b$. Per tant, p és primer. □

Més endavant veurem que podem tenir el mateix resultat amb una hipòtesi més feble.

Proposició 2.6.4. *Sigui A un anell factorial. Siguin $p, q \in A$ elements irreductibles no associats i sigui $a \in A$ un element qualsevol. Aleshores,*

$$\begin{cases} p \mid a \\ q \mid a \end{cases} \implies pq \mid a$$

Demostració. Exercici. □

Observació. Observem que la proposició anterior es pot extendre a un producte finit d'elements irreductibles no associats dos a dos.

2.7 Anells principals

Recordem que un *anell principal*, o *domini d'ideals principals* és un anell on tots els ideals són principals. En aquesta secció estudiarem els anells principals íntegres.

Definició 2.7.1 (Màxim comú divisor)**.** Siguin $a, b \in A$. Direm que $m \in A$ és *màxim comú divisor* (*mcd* o *gcd*) de a i b si

- $m \mid a$ i $m \mid b$
- $\forall\, c \in A$, si tenim que $c \mid a$ i $c \mid b$, aleshores $c \mid m$.

Comentari. Observem que la segona condició és necessària perquè no a tots els anells hi tenim un ordre, de manera que no podem demanar que el màxim comú divisor sigui el "màxim" de tots els divisors comuns.

Observació. No sempre existeix un màxim comú divisor, com es veu a l'exemple següent:

Exemple 2.7.1. Sigui $A = \mathbb{Z}[\sqrt{-5}]$. Tenim que 2 i $1+\sqrt{-5}$ són divisors comuns de 6 i $2+2\sqrt{-5}$, però no tenim que cap dels dos sigui divisible per l'altre.

Definició 2.7.2 (Mínim comú múltiple)**.** Un element $M \in A$ és *mínim comú múltiple* (*mcm* o *lcm*) de a i b si

- $a \mid M$, $b \mid M$
- $\forall\, c \in A$, si tenim que $a \mid c$ i $b \mid c$, aleshores $M \mid c$.

Proposició 2.7.1. *Sigui A un anell principal i siguin $a, b \in A$. Aleshores,*

1. *Sigui $(m) = (a) + (b)$, aleshores m és un gcd de a i b.*
2. *Sigui $(M) = (a) \cap (b)$, aleshores M és un lcm de a i b.*

Demostració.

1. Tenim que $a, b \in (m)$, de manera que $a \mid m$ i $b \mid m$. Sigui $c \in A$ tal que $c \mid a$ i $c \mid b$. Aleshores, $a, b \in (c) \implies (m) = (a) + (b) \subseteq (c)$, de manera que $m \in (c)$ i $c \mid m$.
2. Exercici.

□

Definició 2.7.3 (Coprimers)**.** Dos ideals I, J d'un anell A s'anomenen *coprimers* si $I + J = A$. Igualment, dos elements $a, b \in A$ s'anomenen *coprimers* si $(a) + (b) = A$.

Observació. Si a i b són coprimers, aleshores tenim una identitat de Bézout:

$$\exists\, \lambda, \mu \in A \text{ tals que } \lambda a + \mu b = 1$$

En general, si $(a) + (b) = (m)$,

$$\exists\, \lambda, \mu \in A \text{ tals que } \lambda a + \mu b = m$$

Lema 2.7.1. *Sigui A un anell principal i sigui $a \in A$ un element de l'anell. Aleshores,*

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

Demostració. Observem que només hem de demostrar la implicació cap a la dreta (ja que l'altra es compleix en general). Sigui a irreductible. Suposem que $a \mid bc$ i $a \nmid b$. Sigui $(d) = (a) + (b)$. $a \in (d) \implies d \mid a$, però com a és irreductible, això implica que o bé $d \in A^*$, o bé $d = au$ amb $u \in A^*$. Observem que aquest últim cas ens porta a contradicció, ja que aleshores d i a són associats i com que $a \nmid b$, $d \nmid b$. Per tant, tenim que $d \in A^*$.

Tenim que $(a) + (b) = (d)$, i com que $d \in A^*$, $(d) = A = (1)$. Aleshores, per la identitat de Bézout, $\exists\, \lambda, \mu \in A$ tals que

$$\lambda a + \mu b = 1 \implies \lambda ac + \mu bc = c$$

Degut a que $a \mid ac$ i $a \mid bc$, tenim que $a \mid c$, com volíem demostrar. □

Es pot extendre la proposició anterior amb una altra equivalència:

Proposició 2.7.2. *Sigui A un anell principal, i sigui $a \in A$ un element de l'anell. Aleshores,*

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

Demostració. Exercici. □

Corol·lari 2.7.1. *Sigui $p \in \mathbb{Z}$. Aleshores, p primer $\iff \mathbb{Z}/p\mathbb{Z}$ és un cos.*

Proposició 2.7.3 (Teorema)**.** *Sigui A un anell principal, aleshores A és un anell de factorització única.*

Demostració. Sigui $a \in A$ un element d'un anell principal tal que $a \notin A^*$. Hem de veure que a té una factorització única (llevat ordre i producte per unitats). Si a és irreductible, ja estem. Si a no és irreductible, aleshores $a = a_1 \cdot a_1'$, amb $a_1, a_1' \notin A^*$. Aleshores, $(a) \subset (a_1)$ i $(a) \subset (a_1')$. Si a_1 i a_1' són irreductibles, ja estem. En cas contrari, repetim el mateix procediment amb a_1 i a_1'.

Poden passar dues coses. Si aquest procés acaba en un nombre de repeticions finit, aleshores haurem expressat a com el producte d'elements irreductibles. Si el procés no acaba en un nombre finit de passos, obtenim una llista d'elements no irreductibles $a, a_1, \ldots, a_n, \ldots$ tals que

$$(a) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \ldots$$

Les inclusions són estrictes perquè si $(a_i) = (a_{i+1})$, aleshores $a_{i+1} \in (a_i) \implies a_i \mid a_{i+1}$. Per tant, existiria un $d \in A$ tal que $a_i = a_{i+1}a_{i+1}' = a_i d a_{i+1}' \implies (da_{i+1}' - 1)a_i = 0$. Estem demanant que els anells principals siguin íntegres, de manera que això implicaria que $da_{i+1}' = 1 \implies a_{i+1}' \in A^*$, arribant a una contradicció.

Considerem $I = \bigcup(a_i)$. En general, les unions d'ideals no són un ideal, però en aquest cas sí (Exercici). Recordem que A és un anell principal, de manera que $I = (b) \implies b \in I$, per un cert $b \in A$. Per tant, $\exists\, i_0$ tal que $b \in (a_{i_0})$, de manera que $(b) \subset (a_{i_0}) \subsetneq (a_{i_0+1}) \subseteq I = (b)$.

Donat que hem arribat a una contradicció, concloem que el procés anterior ha d'acabar amb un nombre de repeticions finit.

Per veure la unicitat, suposem que $a = p_1 \dots p_r = q_1 \dots q_s$ amb p_i, q_i irreductibles. Observem que $p_1 \mid p_1 \dots p_r = q_1 \dots q_s$, de manera que $\exists\, j$ tal que $p_1 \mid q_j$ i com q_j és irreductible, $p_1 = uq_j$ amb $u \in A^*$. Aleshores, podem cancel·lar p_1 i q_j de la igualtat anterior. Donat que les factoritzacions tenen un nombre finit d'elements, si repetim aquest procés acabarem arribant a que $r = s$ i cada p_i és associat a un cert q_j. □

Exemple 2.7.2. Observem que el teorema anterior és important, ja que ens permet demostrar que anells com $(\mathbb{Z}/37\mathbb{Z})[x]$ o $K(y)[x]$ són factorials a partir del fet que són principals.

Observació. Tot i que sapiguem que un anell és factorial, a vegades podem no saber com factoritzar els seus elements. Per exemple, només recentment s'ha descobert un algorisme per factoritzar elements de $\mathbb{Q}[x]$, i utilitza tècniques matemàtiques i aproximacions numèriques molt avançades.

2.8 Anells euclidians

Informalment, els anells euclidians són els anells on "es pot dividir", com per exemple els enters o els anells de polinomis.

Definició 2.8.1 (Anell euclidià)**.** Direm que l'anell A és euclidià si existeix una funció $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ tal que

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

Exemple 2.8.1. Per veure que $\mathbb{Z}$ és un anell euclidià, podem agafar $\delta(a) := |a|$, i aleshores observem que la condició de que $|r| < |b|$ és la condició que demanem al dividir enters.

Per veure que $A = K[X]$ és un anell euclidià, agafem $\delta(p) := \text{grau}(p)$. Aleshores ens queda la condició $\text{grau}(r) < \text{grau}(b)$, que és la condició que demanem al dividir polinomis.

Observem també que la primera condició es compleix en els dos casos: $|ab| = |a|\ |b| \geq |a|$ (ja que $b \in \mathbb{Z}$ i $b \neq 0$) i $\text{grau}(pq) = \text{grau}(p) + \text{grau}(q) \geq \text{grau}(p)$ (ja que $K[x]$ és un cos i per tant un anell íntegre).

Un tercer exemple d'anell euclidià seria un cos K qualsevol, agafant $\delta(a) = 0$ per qualsevol $a \in A$, ja que tot element és invertible i no fa falta residu per dividir.

Proposició 2.8.1 (Teorema)**.** *Tot anell euclidià és principal, i per tant factorial.*

Demostració. Sigui $I \subset A$ un ideal no nul. Sigui $m = \min_{a \in I} \delta(a)$. Tenim que m existeix, ja que $\delta(A) \subset \mathbb{N}$ i $\mathbb{N}$ compleix el principi de bona ordenació.

Sigui $c \in I$ tal que $\delta(c) = m$. Veurem que $I = (c)$. Sigui $a \in I$ qualsevol. Donat que A és euclidià, existeixen $q, r \in A$ tals que $a = qc + r$ i $\delta(r) < \delta(c)$ o $r = 0$.

Si $r = 0$, tenim que $a \in (c)$ i ja hem acabat. Altrament, tenim que $\delta(r) < \delta(c)$, de manera que $r \notin I$. Però $r = a - cq$, i donat que $a, c \in I$ i $q \in A$, tenim que $r \in I \implies$ contradicció. □

Corol·lari 2.8.1. *Tot anell que no sigui principal no és euclidià, com per exemple* $\mathbb{Z}[\sqrt{-5}]$.

Definició 2.8.2 (Anell quadràtic)**.** Anell de la forma $\mathbb{Z}[\sqrt{d}]$, on $d \equiv 2,3\ (4)$ o $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, on $d \equiv 1\ (4)$, i on en els dos casos demanem que d estigui lliure de quadrats.

Observació. La majoria d'anells quadràtics no són euclidians, i això implica que l'aritmètica en aquest tipus d'anells és molt més complicada que en els enters o altres cossos euclidians.

Proposició 2.8.2 (Propietats bàsiques dels anells de polinomis)**.** *Sigui K un cos i $K[x]$ el seu anell de polinomis.*

1. *Siguin $f, g \in K[x]$, $f, g \neq 0 \implies \deg(fg) = \deg f + \deg g$*
2. *Sigui $f \in K[x]$, aleshores $n = \deg f \implies f$ té com a molt n arrels diferents.*
3. (Identitat de Bézout). *Donats $f, g \in K[x]$, existeix un únic polinomi mònic $h(x) \in K[x]$ i polinomis $\lambda(x), \mu(x) \in K[x]$ tals que*

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

Demostració. 1. Exercici.

2. Siguin $\alpha_1 \ldots, \alpha_n$ arrels diferents de $f(x)$. Donat que $f(\alpha_i) = 0$, $x - \alpha_i \mid f$ (Exercici). Al ser α_i diferents, tenim que $x - \alpha_i$ són polinomis irreductibles no associats, i per tant

$$\prod_{i=1}^{n}(x - \alpha_i) \mid f(x)$$

   Aplicant (1), ens queda doncs que $\deg f \geq \sum_{i=1}^{n} 1 = n$.

3. Exercici. S'ha d'aplicar l'algorisme extès d'Euclides, que s'explicarà a continuació.

□

Observació. A la identitat de Bézout, podem exigir a més que $\deg \lambda \leq \deg g$ i $\deg \mu \leq \deg f$.

Exemple 2.8.2. Recordem l'algorisme d'Euclides per trobar el màxim comú divisor. Per calcular el mcd de 34 i 21, anem dividint i quedant-nos amb el divisor i el residu:

$$\begin{aligned}\gcd(34,21) &= \gcd(21,13) = \gcd(13,8) = \gcd(8,5) = \gcd(5,3) = \gcd(3,2) = \gcd(2,1) \\ &= \gcd(1,0) = 1\end{aligned}$$

Pensat en termes d'ideals, estem dient que l'ideal generat per (a, b) és el mateix que el generat per $(a - bq, b)$ per qualsevol $q \in \mathbb{Z}$, i aleshores $(34, 21) = (21, 13) = \cdots = (1, 0) = (1)$.

A partir de l'algorisme d'Euclides podem trobar la identitat de Bézout, amb el que es coneix com *algorisme extès d'Euclides.*

Suposem que volem trobar la identitat de Bézout de 16 i 40. Ens definim $u_1 = (40, 1, 0)$ i $u_2 = (16, 0, 1)$, i anem realitzant l'algorisme d'Euclides amb els vectors, i observem que per cada vector es conserva que $40x_2 + 16x_3 = x_1$ (on definim $u_i = (x_1, x_2, x_3)$).

Per exemple, a partir de $(40, 1, 0)$ i $(16, 0, 1)$ trobem $(8, 1, -2)$. Per tant, $8 = \gcd(40, 16) = 40 \cdot 1 + 16 \cdot (-2)$, que és la identitat de Bézout de 40 i 16.

2.9 Polinomis amb coeficients en un anell factorial

Sigui A un anell factorial i sigui $K = \mathrm{Fr}(A)$ el seu cos de fraccions.

Definició 2.9.1 (Contingut d'un polinomi)**.** Donat un polinomi $f(x) = \sum a_i x^i \in A[x]$, definim el seu *contingut* com el màxim comú divisor dels seus coeficients:

$$c(f) := \gcd(a_0, \ldots, a_n)$$

Observació. Observem que el contingut d'un polinomi està determinat llevat del producte per unitats (ja que el gcd també ho està).

Definició 2.9.2 (Primitiu)**.** Direm que el polinomi $f(x) \in A[x]$ és primitiu si $c(f) = 1$.

Observació. Com que el contingut està determinat llevat d'unitats, és equivalent dir que f és primitiu si $c(f) \in A^*$.

Exemple 2.9.1. Sigui $f(x) = 4x + 2 \in \mathbb{Z}[x]$. El contingut de f és $\gcd(4, 2) = 2$, que no és unitat a $\mathbb{Z}$, de manera que f no és primitiu. Si dividim per 2 obtenim $g(x) = 2x + 1$, que sí que és un polinomi primitiu.

Lema 2.9.1 (Lemma de Gauss)**.** *Si $f, g \in A[x]$ són polinomis primitius, aleshores $f \cdot g$ també és un polinomi primitiu.*

Demostració. Siguin $f(x) = \sum_{j=1}^{m} a_j x^j$ i $g(x) = \sum_{j=1}^{n} b_j x^j$. Aleshores,

$$(f \cdot g)(x) = \sum_{j=0}^{m+n} c_j x^j, \qquad \text{on } c_j = \sum_{k=0}^{j} a_j b_{j-k}$$

Suposem que $f \cdot g$ no és primitiu. Aleshores existeix un $p \in A$ irreductible tal que $p \mid c(fg) \implies p \mid c_0$, $p \mid c_1$, $\ldots$, $p \mid c_{m+n}$. Sigui r el màxim índex tal que $p \nmid a_r$, i sigui s el màxim índex tal que $p \nmid b_s$ (sabem que existeixen perquè f i g són primitius).

El coeficient c_{r+s} es pot escriure en funció dels coeficients dels polinomis f i g com

$$c_{r+s} = a_0 b_{r+s} + \cdots + a_r b_s + \ldots a_{r+s} b_0$$

Per definició de r i s, tenim que $p \mid a_i, b_j$ per tot $i < r$ i per tot $j < s$. Observem que això implica que p divideix tots els termes de la dreta de l'igual excepte $a_r b_s$. A més, per hipòtesi $p \mid c_{r+s}$. Aleshores, prenent mòdul p a ambdues bandes, ens queda que $p \mid a_r b_s$, i això implica que $p \mid a_r$ o $p \mid b_s$, arribant a una contradicció. (Hem utilitzat que p és primer, ja que recordem que en un anell factorial tot irreductible és primer.) □

Corol·lari 2.9.1. *Tot polinomi $f(x) \in K[x]$ es pot escriure de manera única (llevat del producte per unitats de A) com $f(x) = cf_0(x)$, amb $c \in K$ i $f_0(x) \in A[x]$ primitiu.*

Demostració. Existència: Per poder calcular-ne el contingut, necessitem portar f a $A[x]$. Donat que K és el cos de fraccions de A, sabem que existeix un $d \in A$ tal que $g(x) := df(x) \in A[x]$.

Aleshores, sigui $k = c(g)$, tenim que $g_0(x) := \frac{1}{k}g(x)$ és primitiu a $A[x]$. Substituint, ens queda que $f(x) = \frac{k}{d}g_0(x)$, on $k/d \in K$ i $g_0(x)$ és primitiu.

Unicitat: Suposem que $c_1 f_1(x) = c_2 f_2(x)$, amb $c_1, c_2 \in K$ i $f_1, f_2 \in A[x]$ primitius. Podem suposar que $c_1, c_2 \in A$ i que són coprimers (altrament els multipliquem pel producte dels seus denominadors i simplifiquem els factors comuns).

Suposem que existeix un $p \in A$ irreductible tal que $p \mid c_1$. Aleshores tindríem que $p \mid c_1 f_1(x) = c_2 f(x) \implies p \mid c(c_2 f_2(x)) = c_2 c(f_2(x)) = c_2$, contradient el fet que c_1 i c_2 són coprimers. Aleshores, $c_1 \in A^*$ i, per l'argument simètric, $c_2 \in A^*$. Per tant, $f_1(x) = c_1^{-1} c_2 f_2(x) \implies f_1$ i f_2 difereixen pel producte d'unitats d'A. □

Corol·lari 2.9.2. *Siguin $f(x), g(x) \in A[x]$. Aleshores, $c(f(x)g(x)) = c(f(x)) \cdot c(g(x))$.*

Demostració. Pel corol·lari anterior, podem escriure $f(x) = af_0(x)$, $g(x) = bg_0(x)$, on $a, b \in K$ i $f_0(x)$ i $g_0(x)$ són primitius. Per tant, tenim que $c(f(x)) = a$ i $c(g(x)) = b$.

Per altra banda, aplicant el lema de Gauss, tenim que $f_0(x)g_0(x)$ és primitiu, de manera que

$$c(f(x)g(x)) = c(abf_0(x)g_0(x)) = ab$$

□

Corol·lari 2.9.3. *Sigui $f(x) \in A[x]$ un polinomi primitiu. Aleshores,*

$$f(x) \text{ irreductible a } A[x] \iff f(x) \text{ irreductible a } K[x]$$

Demostració. La implicació cap a l'esquerra és trivial, ja que $A[x] \subset K[x]$. Per tant, només demostrarem la implicació cap a la dreta.

Sigui $f(x)$ irreductible a $A[x]$. Suposem que $f(x) = a(x)b(x)$ amb $a(x), b(x) \in K[x]$ i $\deg a(x)$, $\deg b(x) \geq 1$. Pel corol·lari 2.9.1 podem escriure $a(x) = \alpha a_0(x)$, $b(x) = \beta b_0(x)$ amb $\alpha, \beta \in K$ i $a_0(x)$ i $b_0(x) \in A[x]$ primitius.

Com que K és el cos de fraccions de A, tenim que $\alpha\beta = \gamma/\delta$, amb $\gamma, \delta \in A$. Aleshores,

$$\delta f(x) = \gamma a_0(x)b_0(x) \implies c(\delta f(x)) = c(\gamma a_0(x)b_0(x)) \implies \delta = \gamma$$

on hem utilitzat que f, a_0 i b_0 són polinomis primitius. Per tant, ens queda que $f(x) = a_0(x)b_0(x)$ i (com que f és irreductible a $A[x]$) el grau de $a_0(x)$ o el grau de $b_0(x)$ han de ser zero. Tenint en compte que $\deg a(x) = \deg a_0(x)$ i $\deg b(x) = \deg b_0(x)$, això suposa una contradicció. □

Proposició 2.9.1 (Teorema)**.** *Sigui A un anell factorial. Aleshores, $A[x]$ també és un anell factorial.*

Demostració. Sigui $f(x) \in A[x]$ un polinomi qualsevol. Pel corol·lari 2.9.1, existeix un f_0 primitiu tal que $f(x) = c(f(x))f_0(x)$, i aquesta descomposició és única (llevat del producte per unitats de A). Sigui $c(f) = p_1^{e_1} \dots p_r^{e_r}$ la descomposició única en elements irreductibles de $c(f) \in A$.

Donat que $K[x]$ és euclidià, també és factorial. Per tant, veient $f_0(x)$ com un element de $K[x]$, tenim que $f_0(x) = h_1^{n_1}(x) \dots h_s^{n_s}(x)$, amb $h_i(x) \in K[x]$ irreductibles. Donat que $f_0(x)$ és primitiu, cada un dels $h_i(x)$ és primitiu, i per tant també són irreductibles a $A[x]$ (aplicant el corol·lari 2.9.3).

Ajuntant-ho tot, ens queda que

$$f(x) = p_1^{e_1} \dots p_r^{e_r} h_1^{n_1}(x) \dots h_s^{n_s}(x)$$

on cada factor és irreductible a $A[x]$.

Deixem la demostració de la unicitat com a exercici, ja que no suposa cap dificultat. □

Corol·lari 2.9.4. *Sigui A un anell factorial. Aleshores, $A[x_1, \dots, x_n]$ és un anell factorial.*

Demostració. Es prova per inducció sobre n, veient que $A[x_1, \dots, x_n] = A[x_1, \dots, x_{n-1}][x_n]$ i aplicant el teorema. □

2.10 Criteris d'irreductibilitat

Sigui A un anell factorial i sigui $K = \mathrm{Fr}(A)$ el seu cos de fraccions.

Proposició 2.10.1. *Sigui $f(x) = a_0 + a_1 x + \dots + a_n x^n \in A[x]$. Sigui $\alpha = u/v \in K$, una arrel del polinomi, amb u i v coprimers. Aleshores, tenim que $u \mid a_0$ i $v \mid a_n$.*

Demostració. Com que α és arrel de f, $v^n f(\alpha) = 0$ i per tant,

$$a_0 v^n + a_1 v^{n-1} u + \dots + a_n u^n = 0$$

Prenent mòdul u o mòdul v als dos costats de la igualtat, ens queda que $u \mid a_0 v^n \implies u \mid a_0$ i $v \mid a_n u^n \implies v \mid a_n$. □

Exemple 2.10.1. Considerem el polinomi $f(x) = x^5 + 2x + 6$. Aquest polinomi no té arrels a $\mathbb{Q}$, ja que si $u/v \in \mathbb{Q}$ fos arrel, tindríem que $u = \pm 1, \pm 2, \pm 3, \pm 6$ i $v = \pm 1$, i es comprova que cap d'aquestes possibilitats és arrel.

Exemple 2.10.2. El polinomi $x^2 - 2$ no té arrels racionals, ja que $f(\pm 1) = -1$ i $f(\pm 2) = 2$. D'aquí es pot deduir que $\sqrt{2}$ és irracional.

Proposició 2.10.2 (Criteri d'irreductibilitat d'Eisenstein)**.** *Sigui $f(x) = a_0 + a_1 x + \dots + a_n x^n \in A[x]$. Sigui $p \in A$ primer. Aleshores,*

$$\left.\begin{array}{l} p \mid a_0,\ \dots,\ p \mid a_{n-1} \\ p \nmid a_n \\ p^2 \nmid a_0 \end{array}\right\} \implies f(x) \text{ és irreductible a } K[x]$$

Demostració. Per resultats anteriors, podem suposar que f és primitiu i demostrar només que és irreductible a $A[x]$.

Suposem que $f(x) = g(x)h(x)$, amb $g(x) = \sum_{i=0}^{r} b_i x^i$ i $h(x) = \sum_{i=0}^{s} c_i x^i$, $r, s \geq 1$. Tenim que $a_0 = b_0 c_0$, $p \mid a_0$ i $p^2 \nmid a_0$. Per tant, p no pot dividir tant a b_0 com a c_0. Suposem spdg que $p \nmid b_0$ i $p \mid c_0$.

Tenim que $p \nmid a_n = b_r c_s \implies p \nmid c_s$. Sigui t el mínim índex j tal que $p \nmid c_j$. Tenim que $t \leq s < r + s = n$. Aleshores,

$$a_t = b_0 c_t + \cdots + b_t c_0$$

Com que t era el mínim índex tal que $p \nmid c_t$ i $t < n$, tenim que p divideix tots els termes de la igualtat excepte $b_0 c_t \implies p \mid b_0 c_t$. Havíem suposat que $p \nmid b_0$ i $p \nmid c_t$, de manera que arribem a una contradicció. □

Exemple 2.10.3. El polinomi $f(x) = x^5 + 3x^4 + 6x^3 + 12x^2 + 15$ és irreductible a $\mathbb{Q}[x]$, ja que és 3-Eisenstein (compleix el criteri d'Eisenstein amb $p = 3$).

Observació. Si agafem un polinomi a l'atzar, la probabilitat que sigui p-Eisenstein és nul·la. Tot i això, el criteri d'Eisentein és molt important per la teoria de nombres, ja que ens permet demostrar que certs tipus de polinomis ciclotòmics com $x^{p-1} + \cdots + x + 1$ (amb p primer) són irreductibles. Observem que aquest polinomi no és Eisenstein directament, però es pot transformar en un polinomi que sí que ho és.

Lema 2.10.1 (Extensió de morfismes a l'anell de polinomis)**.** *Sigui $f : A \longrightarrow B$ un morfisme entre dos anells qualssevol. Aleshores, l'aplicació*

$$\begin{aligned} \tilde{f} : A[x] &\longrightarrow B[x] \\ \sum_i a_i x^i &\mapsto \sum_i f(a_i) x^i \end{aligned}$$

és un morfisme d'anells.

Demostració. Exercici. □

Proposició 2.10.3 (Criteri de reducció)**.** *Siguin A, B anells qualssevol, amb A factorial. Sigui $\phi : A \longrightarrow B$ un morfisme d'anells, i sigui $\tilde{\phi}$ la seva extensió als anells de polinomis. Sigui $f(x) \in A[x]$ tal que*

$$\begin{cases} \deg \tilde{\phi}(f) = \deg f \\ \tilde{\phi}(f) \text{ és irreductible} \end{cases}$$

Aleshores, $f(x)$ és irreductible.

Demostració. Suposem que $f(x) = a(x)b(x)$ en $A[x]$. Donat que $\tilde{\phi}$ és un morfisme,

$$\tilde{\phi}(f(x)) = \tilde{\phi}(a(x))\tilde{\phi}(b(x)) \implies \begin{cases} \deg \tilde{\phi}(a(x)) = 0 \\ \quad \text{o} \\ \deg \tilde{\phi}(b(x)) = 0 \end{cases}$$

Observem que $\tilde{\phi}$ només pot reduir el grau o mantenir-lo constant, però mai augmentar-lo. Aleshores, donat que $\deg \tilde{\phi}(f(x)) = \deg f(x) = \deg a(x) + \deg b(x)$, tenim que

$$\begin{cases} \deg \tilde{\phi}(a(x)) = \deg a(x) \\ \deg \tilde{\phi}(b(x)) = \deg b(x) \end{cases}$$

Juntant-ho amb el resultat anterior, això implica que $\deg a(x) = 0$ o $\deg b(x) = 0$.

Per tant, f és irreductible. □

Exemple 2.10.4. Vegem un exemple d'aplicació per comprovar la utilitat d'aquest criteri. Considerem el polinomi $f(x) = x^3 + 6x + 2^{20} \in \mathbb{Z}[x]$. Per comprovar si és irreductible amb Ruffini, hauríem d'iterar per tots els divisors de 2^{20}. En lloc d'això, observem que l'extensió als anells de polinomis de la projecció $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$ compleix que

$$\tilde{\pi}(f) = x^3 + x + 1$$

que és de grau 3 i irreductible. Aleshores, f és irreductible.

Exemple 2.10.5. Considerem $f(x) = x^5 + 2x + 6 \in \mathbb{Z}[x]$, FALTA

Exemple 2.10.6. Sigui $f(x) = x^5 + x + 1$. Observem que $f(x) \mod p$ sempre té un factor de grau 2. Això ens fa sospitar que $f(x)$ no és irreductible i, efectivament,

$$f(x) = (x^2 + x + 1)(x^3 - x^2 + 1)$$

Observem, però, que això no sempre es dona, ja que existeixen polinomis irreductibles tals que sempre tenen un factor a $(\mathbb{Z}/p\mathbb{Z})[x]$ d'una mida donada.

3 Cossos

3.1 Motivació

(Falta organitzar una mica aquest apartat)

Començarem amb un exemple que ens demostra la utilitat dels cossos. Siguin

$$A = \sqrt{5 + \sqrt{22 + \sqrt{5}}}$$

$$B = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}$$

Per estrany que sembli, tenim que $A = B$. Com es pot demostrar aquesta igualtat? Observem que A és arrel del polinomi

$$((A^2 - 5)^2 - 22)^2 - 5 = 0$$

Una manera de veure que $A = B$, seria demostrar que B també és arrel del polinomi, i després demostrar numèricament que, per una certa precisió, $A = B$.

En aquest capítol, aprendrem a resoldre problemes d'aquest tipus.

Una altra cosa que ens pot interessar és, donada un $\alpha \in \mathbb{R}$, construir un polinomi a $\mathbb{Z}[x]$ que tingui α com a arrel. Per exemple, podem voler construir un polinomi que tingui com a arrel $\sqrt[3]{5} + \sqrt[2]{7} + \sqrt[3]{9}$. També aprendrem a fer això en aquest capítol.

En el capítol anterior, hem vist que

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{R}\}$$

és un cos, ja que és isomorf al quocient de $\mathbb{Q}[x]$ per $(x^3 - 2)$, que és un polinomi irreductible (en particular, 2-Eisenstein), de manera que $(x^3 - 2)$ és un anell maximal.

Al mateix temps, podríem agafar un altre cos isomorf a $\mathbb{Q}[x]/(x^3-2)$, el cos $\mathbb{Q}[e^{2\pi i/3}\sqrt[3]{2}]$. Tenim que aquest cos no està contingut als reals, a diferència de $\mathbb{Q}[\sqrt[3]{2}]$, però el que no es tan fàcil de veure és que $\mathbb{Q}[\sqrt[3]{2}]$ no està contingut a $\mathbb{Q}[e^{2\pi i/3}\sqrt[3]{2}]$, cosa que també aprendrem a fer en aquest capítol.

Considerem $\zeta = e^{2\pi i/7}$, arrel de $f(x) = x^6+x^5+\cdots+x+1$. Observem que, a diferència de x^3-2, tenim que $Q[\zeta]$ conté tota la resta d'arrels de $f(x)$ $(\zeta^2, \ldots, \zeta^6)$. Com veurem més endavant, això es deu a que aquests dos cossos tenen certes propietats diferents.

Observem que aquests cossos es poden veure com un $\mathbb{Q}$-espai vectorial, on $\mathbb{Q}[\sqrt[3]{2}] = \langle 1, \sqrt[3]{2}, \sqrt[3]{4}\rangle$ i $\mathbb{Q}[\zeta] = \langle 1, \zeta, \ldots, \zeta^5\rangle$. Ens podríem preguntar si $\mathbb{R}$ és també un $\mathbb{Q}$-espai vectorial d'una certa dimensió, o si $\mathbb{Q}[\pi] = \mathbb{Q}(\pi)$, preguntes que respondrem al llarg del capítol.

Sigui $K = \mathbb{Q}(S,T)$ el conjunt de fraccions polinòmiques de $\mathbb{Q}$ amb dues variables. Ens podem preguntar si K és algebraicament tancat, o si hi ha algun cos tancat que contingui K. En aquest capítol introduirem el concepte de clausura algebraica que resoldrà aquesta qüestió.

També estudiarem els cossos finits, que tenen moltes aplicacions pràctiques a la vida real, com per exemple en el camp de la criptografia.

3.2 Nocions bàsiques

Definició 3.2.1 (Extensió de cossos)**.** 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 (és a dir, un subanell que és cos). Ho denotarem per F/K.

En aquesta situació tenim una aplicació natural

$$\begin{aligned} K \times F &\longrightarrow F \\ \lambda, \alpha &\mapsto \lambda\alpha \end{aligned}$$

Aquesta aplicació ens permet veure F com un K-espai vectorial (on aquesta aplicació representa el producte per escalars).

Definició 3.2.2 (Extensió finita, grau de l'extensió)**.** Direm que F/K és una *extensió finita* si $\dim_K F < +\infty$ (entenent F com un K-espai vectorial).

En aquest cas, anomenem *grau de l'extensió* a aquesta dimensió. Denotarem el grau com

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

Si $\dim_k F = +\infty$ direm que F és una *extensió infinita* de K.

Exemple 3.2.1. Els complexos són una extensió dels nombres reals: $\mathbb{C}/\mathbb{R}$. De fet,

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{R}\langle 1, i\rangle$$

Donat que 1 i i són $\mathbb{R}$-linealment independents, tenim que $[\mathbb{C} : \mathbb{R}] = 2$.

Exemple 3.2.2. Ja hem vist anteriorment que $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ és un cos. Es pot comprovar que $1, \sqrt[3]{2}$ i $\sqrt[3]{4}$ són $\mathbb{Q}$-linealment independents, de manera que formen una base i tenim

$$\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}\langle 1, \sqrt[3]{2}, \sqrt[3]{4}\rangle \implies [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$$

Exemple 3.2.3. Un exemple d'extensió infinita d'un cos és $\mathbb{Q}(x_1, x_2, \dots,)$, el conjunt de fraccions polinòmiques en infinites variables. Observem que $\mathbb{Q}(x_1, x_2, \dots,)/\mathbb{Q}$, i que no hi pot haver cap base finita de l'extensió (ja que una base finita involucraria com a molt una quantitat finita de variables, i no podria cobrir tot el cos). Per tant, l'extensió és infinita.

Exemple 3.2.4. Observem que $\mathbb{R}/\mathbb{Q}$ també és una extensió infinita, però en aquest cas és més complicat de demostrar. També seria infinita $\mathbb{Q}(x)/\mathbb{Q}$. Deixem com a exercici comprovar que així és.

Proposició 3.2.1. *Siguin F/K i H/F extensions de cossos. Aleshores H/K també és una extensió de cossos, i tenim que*

$$H/K \text{ finita} \iff H/F,\ F/K \text{ finites}$$

En aquest cas, tenim a més que els graus es multipliquen:

$$[H : K] = [H : F][F : K]$$

Demostració. Suposem que H/K és finita. Aleshores, podem pensar $F \subset H$ com un sub-K-espai vectorial de H. Aleshores, $\dim_K F \leq \dim_K H < \infty \implies F/K$ és finita.

Per veure que H/F és finita, agafem $\omega_1, \dots, \omega_n$ una K-base de H. Aleshores,

$$H = K\langle \omega_1, \dots, \omega_n \rangle \underset{K \subset F}{=} F\langle \omega_1, \dots, \omega_n \rangle$$

Observem que pot passar que els ω_i ja no siguin F-linealment independents, però en tot cas tindrem que $\dim_F H \leq n < \infty$.

Anem ara a demostrar la implicació contrària. Suposem que $r = [F : K] < \infty$ i $s = [H : F] < \infty$. Sigui $\alpha_1, \dots, \alpha_r$ una K-base de F, i sigui $\beta_1, \dots, \beta_s$ una F-base de H. N'hi ha prou amb veure que $\{\alpha_i\beta_j\}_{i,j}$ és una K-base de H (ja que aleshores $[H : K] = rs < \infty$).

Suposem que $\{\alpha_i\beta_j\}_{i,j}$ fossin K-linealment dependents. Aleshores, tindríem una expressió de l'estil

$$\sum_{i,j} \lambda_{i,j}\alpha_i\beta_j = 0$$

Agrupem les β_j:

$$\sum_j \underbrace{\left(\sum_i \lambda_{i,j}\alpha_i \right)}_{\in F} \beta_j = 0$$

Donat que $\{\beta_j\}_j$ són F-linearment independents, tenim que tots els coeficients han de ser zero. Aleshores, per qualsevol j, tenim que

$$\sum_i \lambda_{i,j}\alpha_i = 0$$

i donat que $\{\alpha_i\}_i$ són K-linearment independents, $\lambda_{i,j} = 0$ per qualsevol i i j.

Ens faltaria veure que $\{\alpha_i\beta_j\}_{i,j}$ també són un conjunt K-generador de H (Exercici). □

Observació. Observem que la fórmula $[H : K] = [H : F][F : K]$ també val quan la extensió és infinita.

3.3 Elements algebraics

Sigui L/K una extensió de cossos.

Definició 3.3.1 (Algebraic)**.** Direm que $\alpha \in L$ és *algebraic sobre* K (ho denotarem com α algebraic/K) si α és arrel d'un polinomi amb coeficients a K.

En cas contrari, direm que α és transcendent sobre K.

Denotarem per $\bar{K}$ el conjunt d'elements algebraics/K. Observem però que encara no sabem si tots els cossos tenen extensions, ni quina relació hi ha entre les extensions d'un cos, de manera que, de moment, aquesta definició no té gaire sentit.

Exemple 3.3.1.

1. $\sqrt{2} \in \mathbb{R}$ és algebraic/$\mathbb{Q}$, ja que agafant $f(x) = x^2 - 2$, $f(\sqrt{2}) = 0$.
2. π és algebraic/$\mathbb{R}$ (agafant per exemple $f(x) = x - \pi$), però és transcendent/$\mathbb{Q}$ (tot i que no és gens fàcil de provar).

Definició 3.3.2 (Polinomi irreductible)**.** Si $\alpha \in F$ és un element algebraic/K, anomenem *polinomi irreductible* de α/K (que denotarem com $\mathrm{Irr}(\alpha, K, x)$) al polinomi mònic de $K[x]$ de menor grau que té α com a arrel.

Observació. Per definició, el polinomi irreductible de α/K és irreductible, ja que si fos el producte de dos de menor grau, un d'ells tindria α com a arrel.

Observem també que el polinomi irreductible de α/K és únic, ja que siguin $f, g \in K[x]$ polinomis irreductibles de α/K, f i g tenen el mateix grau i són mònics, de manera que $f - g$ és un polinomi de grau menor que té α com a arrel $\implies f - g = 0 \implies f = g$.

A continuació veurem que podem caracteritzar el polinomi irreductible de α/K d'una altra manera. Considerem l'aplicació

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

que es pot comprovar que és un morfisme d'anells.

Observem que tenim la cadena d'implicacions

$$\alpha \text{ algebraic}/K \iff \varphi_\alpha \text{ no injectiu} \iff \ker \varphi_\alpha \neq (0) \underset{K[x] \text{ principal}}{\iff} \ker \varphi_\alpha = (p(x))$$

Aleshores, pel teorema d'isomorfisme, $K[x]/(p(x)) \simeq \mathrm{Im}\, \phi_\alpha \subset K$. Tot subanell d'un cos és un anell íntegre, i la propietat de ser anell íntegre es conserva per isomorfisme, de manera que $K[x]/(p(x))$ és un anell íntegre i aleshores $p(x)$ és primer. Per tant, $p(x)$ és irreductible, i és el polinomi irreductible de α/K que buscàvem (llevat del producte per una unitat per tal que sigui mònic).

Exemple 3.3.2. El polinomi irreductible depèn de l'extensió que prenem. Per exemple, $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}, x) = x^2 - 2$, però $\mathrm{Irr}(\sqrt{2}, \mathbb{R}, x) = x - \sqrt{2}$.

Definició 3.3.3 (Cos generat)**.** Sigui $\alpha \in L$, on L/K és una extensió de cossos. Aleshores, definim el *cos generat* per α/K com el menor cos que conté α i K. Es pot escriure aquest cos explícitament com

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

Proposició 3.3.1. *Si α és algebraic/K, aleshores*

$$K(\alpha) \simeq K[x]/(\mathrm{Irr}(\alpha, K, x)$$

En cas contrari, si α és transcendent/K, aleshores $K(\alpha) \simeq K(x)$.

Demostració. Exercici. □

A continuació, veurem una caracterització alternativa dels nombres algebraics:

Proposició 3.3.2. *Sigui $\alpha \in L/K$. Aleshores,*

$$\alpha \text{ algebraic}/K \iff K(\alpha) = K[\alpha] \iff K(\alpha)/K \text{ és finita}$$

Demostració.

1 $\implies$ 2: N'hi ha prou amb veure que, donat $q(x) \in K[x]$ tal que $q(\alpha) \neq 0$, aleshores $1/q(\alpha) \in K[\alpha]$.

Sigui $f(x) = \mathrm{Irr}(\alpha, K, x)$ el polinomi irreductible de α/K. Donat que $q(\alpha) \neq 0$, tenim que $f \nmid q \implies \gcd(f, q) = 1$ (ja que f és irreductible).

Aleshores, tenim una identitat de Bézout, de manera que $\exists\, \lambda, \mu \in K[x]$ tals que $\lambda(x)f(x) + \mu(x)q(x) = 1$.

Avaluant a α, ens queda que

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

2 $\implies$ 3: Per hipòtesi, tenim que $1/\alpha \in K[\alpha]$. Aleshores,

$$\frac{1}{\alpha} = \sum_{i=0}^{n-1} a_i \alpha^i$$

per uns certs n i a_i. Multiplicant per α, ens queda que

$$1 = \sum_{i=0}^{n-1} a_i \alpha^{i+1} \implies \alpha^n = \frac{1}{a_n} \left(\sum_{i=0}^{n-1} a_i \alpha^i - 1 \right)$$

Per inducció, tenim que $\alpha^k \in K\langle 1, \ldots, \alpha^{n-1} \rangle$ per qualsevol k, de manera que $[K(\alpha) : K] \leq n < \infty$.

3 $\implies$ 1: Per hipòtesi, $[K(\alpha) : K] = n < \infty$. Aleshores, $1, \alpha, \alpha^2, \ldots, \alpha^n$ han de ser linealment dependents (ja que són un conjunt de $n+1$ elements), de manera que $\exists\, a_0, \ldots, a_n \in K$ tals que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

és a dir, que α és arrel del polinomi $a_0 + a_1 x + \cdots + a_n\alpha^n \in K[x]$. □

Lema 3.3.1. *Siguin $L/M/K$ extensions de cossos. Aleshores,*

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

Proposició 3.3.3. *Sigui L/K una extensió de cossos. Siguin α i β algebraics/K. Aleshores,*

1. *$\alpha \pm \beta$ és algebraic/K.*
2. *$\alpha\beta$ és algebraic/K.*
3. *α/β és algebraic/K si $\beta \neq 0$.*

Demostració. Per hipòtesi, α és algebraic/K, i β és algebraic/$K(\alpha)$ (pel lema anterior), de manera que

$$[K(\alpha, \beta) : K] = [K(\alpha)(\beta) : K(\alpha)]\,[K(\alpha) : K] < \infty$$

Observem que $K \subset K(\alpha + \beta) \subset K(\alpha, \beta)$. Aleshores, donat que $K(\alpha, \beta)/K$ és finita, tenim que $K(\alpha + \beta)/K$ és finita $\implies$ $\alpha + \beta$ és algebraic/K.

La resta de casos es fan de manera anàloga. □

Observació. La demostració anterior no es constructiva, i no ens dona cap pista sobre quin pot ser el polinomi que tingui com a arrel $\alpha + \beta$.

A la pràctica tenim dues opcions per trobar-ho. L'opció "algebraica" seria fer servir la *resultant*, que és una generalització del discriminant d'un polinomi.

L'opció "numèrica" seria calcular una aproximació numèrica del polinomi. En aquest mètode, calcularíem les primeres 20 o 30 potències de l'arrel i buscaríem una $\mathbb{Z}$-combinació lineal d'aquestes potències (amb l'algorisme LLL).

Si les aproximacions són prou bones, podrem adaptar la combinació lineal de les potències aproximades a una combinació lineal de les potències exactes, obtenint un polinomi que té l'arrel que volíem.

El mètode numèric és més eficient en general, però no tenim garantit que sempre arribi a un resultat, ja que podem trobar nombres algebraics diferents arbitràriament propers.

3.4 Representació matricial de nombres algebraics

Sigui L/K una extensió finita. Com hem vist abans, aleshores tot $\alpha \in L$ és algebraic sobre K. Fixem una K-base $\omega_1, \ldots, \omega_n$ de L.

Donat un $\alpha \in L$, considrem l'aplicació

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

Observem que m_α és una aplicació K-lineal del K-espai vectorial L en ell mateix. Per tant, la podem descriure com una matriu (respecte la base fixada).

$$M_\alpha := (a_{ij})_{i,j}, \quad \text{on } m_\alpha(\omega_i) = \sum_j a_{ij}\omega_j$$

Exemple 3.4.1. Prenem $K = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt{2}]$. Agafem la base $\omega_1 = 1$ i $\omega_2 = \sqrt{2}$. Aleshores, la representació matricial de $\alpha = \sqrt{2}$ seria

$$M_\alpha = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Si agafem $\alpha = 3 + 2\sqrt{2}$, aleshores la seva representació matricial seria

$$M_\alpha = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$$

És interessant veure que

$$M_{3+2\sqrt{2}} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} = 3\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = 3M_1 + 2M_{\sqrt{2}}$$

El polinomi característic de M_α és $x^2 - 6x + 1$, que també és el polinomi mínim (ja que és irreductible).

Observem que $3 + 2\sqrt{2}$ és una de les arrels d'aquets polinomi. Això no és casualitat, el càlcul del polinomi mínim de la representació matricial d'un α algebraic/K ens dona el polinomi irreductible de α/K.

A més, pel teorema de Cayley-Hamilton la matriu és una arrel del polinomi mínim, de manera que podrem "identificar" el nombre algebraic amb la seva representació matricial.

A continuació formalitzarem algunes d'aquestes idees.

Proposició 3.4.1. *L'aplicació*

$$\begin{aligned} L &\longrightarrow M_n(K) \\ \alpha &\longmapsto M_\alpha \end{aligned}$$

és un morfisme injectiu d'anells (que pot dependre de la base de L triada).

En particular, si $\alpha \neq 0$, aleshores $M_\alpha \in G\ell_n(K)$ (el grup lineal amb coeficients a K, és a dir, el conjunt de matrius invertibles).

A més, $\alpha, \beta \in L \implies M_\alpha M_\beta = M_\beta M_\alpha$.

Demostració. Exercici. □

Corol·lari 3.4.1. *Si* $\alpha = \sum \lambda_i \omega_i$*, aleshores*

$$M_\alpha = \sum \lambda_i M_{\omega_i}$$

Proposició 3.4.2. *El polinomi* $\operatorname{Irr}(\alpha, K, x)$ *coincideix amb el polinomi mínim de* M_α*.*
En particular, els valors propis de M_α *són les arrels de* $\operatorname{Irr}(\alpha, K, x)$*.*

Demostració. Per la proposició anterior, el morfisme $\alpha \mapsto M_\alpha$ és injectiu, de manera que $p(M_\alpha) = 0 \iff p(\alpha) = 0$ per qualsevol polinomi $p(x) \in K[x]$. □

Observació. Observem que la representació matricial ens permet racionalitzar fraccions amb radicals. Com a exercici, es pot racionalitzar $1/(\sqrt[3]{5} + 2)$.

3.5 Teorema de l'element primitiu

Exemple 3.5.1. Suposem que agafem l'extensió $K/\mathbb{Q}$ on $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Ens agradaria expressar aquest cos com $\mathbb{Q}(\alpha)$, ja que aleshores tenim una base molt fàcil $\mathbb{Q}\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$, on $n = \deg \operatorname{Irr}(\alpha, \mathbb{Q})$. En aquest cas, podem prendre $\alpha = \sqrt{2} + \sqrt{3}$. Anem a provar-ho.

Observem que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ i $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, ja que $x^2 - 2$ i $x^2 - 3$ són irreductibles/Q. Observem a més que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})]$ pot ser 1 o 2 (depenent de si són el mateix cos o no). Si aquest grau fos 1, tindríem que $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$, de manera que podríem escriure $\sqrt{2} = \lambda + \mu\sqrt{3}$, on λ, $\mu \in \mathbb{Q}$. Aleshores,

$$2 = \lambda^2 + 3\mu^2 + 2\lambda\mu\sqrt{3}$$

Fent servir de nou que $\langle 1, \sqrt{3}\rangle$ és una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{3})$, tindríem que

$$\begin{cases} 2 = \lambda^2 + 3\mu^2 \\ 2\mu\lambda = 0 \end{cases}$$

Tant $\mu = 0$ com $\lambda = 0$ porten a contradicció, de manera que $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{3})] = 2$, i per tant $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Recordem que el nostre objectiu era veure que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$ amb $\alpha = \sqrt{2} + \sqrt{3}$. Observem que $\alpha^2 = 5 + 2\sqrt{6}$, de manera que

$$(\alpha^2 - 5)^2 = 26 \implies \alpha^4 - 10\alpha^2 + 1 = 0$$

Es pot veure que aquest polinomi és irreductible sobre $\mathbb{Q}$, de manera que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Per últim, donat que

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

tenim que $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 1$, i que són el mateix cos.

Per tant, una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ serà $\mathbb{Q}\langle 1, \alpha, \alpha^2, \alpha^3\rangle$, amb $\alpha = \sqrt{2} + \sqrt{3}$.

Exercici. Escriviu $\sqrt{2}$ i $\sqrt{3}$ en la base anterior i doneu les seves representacions matricials amb els corresponents polinomis característics i mínims.

Aquest exemple ens ha servit per veure la utilitat de representar una extensió com l'extensió generada per un únic element (monògena). El següent teorema ens dona unes certes condicions sota les quals podrem garantir que l'extensió és monògena.

Proposició 3.5.1 (Tma de l'element primitiu)**.** *Sigui K un cos amb* $\mathrm{char}K = 0$*, i sigui L/K una extensió finita. Aleshores, existeix un element $\gamma \in L$ tal que $L = K(\gamma)$.*

Demostració. En primer lloc, veurem que si l'extensió és finita, podem generar-la amb un nombre d'elements finit (és a dir, $L = K(\alpha_1, \ldots, \alpha_n)$ per uns certs $\alpha_1, \ldots, \alpha_n \in L$).

Per veure-ho, comencem triant un $\alpha_1 \in L/K$ qualsevol. Aleshores,

$$K \subsetneq K(\alpha_1) \subseteq L \implies [L : K(\alpha_1)] = \frac{[L : K]}{[K(\alpha_1) : K]} < [L : K]$$

Per tant, el grau de l'extensió decreixerà estrictament, i podrem iterar el procés i acabar en un nombre de passos finit.

A continuació veurem que $\exists\, \gamma \in K(\alpha_1, \ldots, \alpha_n)$ tal que $K(\gamma) = K(\alpha_1, \ldots, \alpha_n)$. Per inducció, només ens fa falta demostrar-ho per $n = 2$.

Suposem doncs que $L = K(\alpha, \beta)$ i busquem γ tal que $K(\gamma) = K(\alpha, \beta)$. Suposem que tenim un γ de la forma $\gamma = \alpha + c\beta$, amb $c \in K$. Aleshores,

$$K \subset K(\gamma) \subset K(\alpha, \beta)$$

Per tant, en tenim prou amb veure que $\beta \in K(\gamma)$ perquè llavors $\alpha = \gamma - c\beta \in K(\gamma)$. Això no passarà per tots els c, però en tenim prou amb trobar-ne un de sol.

Siguin $f(x) = \mathrm{Irr}(\alpha, K, x) \in K[x]$ i $g(x) = \mathrm{Irr}(\beta, K(\gamma), x) \in K(\gamma)[x]$. Sigui $h(x) = f(\gamma - cx) \in K(\gamma)[x]$.

Suposem que $\beta \notin K[x]$. Aleshores, $\deg g(x) > 1$. Per tant, $g(x)$ té una altra arrel $\beta' \neq \beta$. Per altra banda,

$$h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0 \implies g(x) \mid h(x)$$

ja que el polinomi irreductible de β divideix tot altre polinomi que tingui β com a arrel.

Aleshores, $h(\beta') = 0$, de manera que $\alpha' := \gamma - c\beta' = \alpha + c\beta - c\beta' \neq \alpha$ és una altra arrel de $f(x)$. Per tant, si $\beta \notin K(\gamma)$, c haurà de tenir la forma

$$c = \frac{\alpha' - \alpha}{\beta - \beta'}$$

Hi ha un nombre finit de c's d'aquesta forma (ja que hi ha un nombre finit d'arrels de f i de g). Donat que $\mathrm{char}K = 0$, tenim que $\mathbb{Q} \subset K$ i per tant K té infinits elements. Aleshores, segur que existeix un c que no satisfà la condició anterior, de manera que $\beta \in K(\gamma)$. □

Observació. A la demostració anterior, hem donat per suposat que si $g(x) = \mathrm{Irr}(\beta, K(\gamma), x)$ tenia grau > 1, aleshores tenia una arrel $\beta' \neq \beta$.

Aquí hi poden haver dos problemes: no sabem a quin espai es troba β' ni si $\exists\, \beta' \neq \beta$.

A la propera clase veurem que tot cos té un cos més gran que conté totes les arrels dels seus polinomis. Per veure que $\beta' \neq \beta$, podem utilitzar que si $\mathrm{char} K = 0$, tot polinomi irreductible$/K$ és separable (té totes les arrels diferents).

La demostració es faria veient que si α és una arrel doble de $f(x) \in K[x]$ irreductible, aleshores

$$h(x) := \gcd(f(x), f'(x)) \text{ té grau } \geq 1$$

Donat que f és irreductible, i $h(x) \mid f(x)$, la única opció és que $h(x) = f(x) \implies f(x) \mid f'(x) \implies f'(x) = 0$ (ja que $\deg f'(x) < \deg f(x)$ i $\mathrm{char}\, K = 0$). Aleshores $f(x)$ hauria de ser un polinomi constant, arribant a una contradicció.

Observació. El teorema de l'element primitiu és vàlid a qualsevol extensió finita i separable (tot polinomi irreductible té únicament arrels simples). La demostració seria més complicada i no la veurem en aquest curs.

Això inclou en particular les extensions dels cossos finits.

Exemple 3.5.2. Sigui F un cos de $\mathrm{char}\, F = p > 0$. Sigui $f(x) = x^{p^n} - T^{p^n} \in K[x]$, on $K = F(T)$. Aleshores,

$$f'(x) = p^n x^{p^n - 1} = 0$$

Però només té una única arrel de multiplicitat p^n:

$$\alpha^{p^n} - T^{p^n} = 0 \iff (\alpha - T)^{p^n} = 0 \iff \alpha = T$$

((S'ha de revisar))

3.6 Cos de descomposició

Suposem que agafem el polinomi $f(x) = x^5 + 3x^4 + 2x + 7$. Si considerem $f(x) \in \mathbb{Q}[x]$, aleshores les seves arrels són a $\mathbb{C}$, però si $f(x) \in \mathbb{Z}/17\mathbb{Z}[x]$, on viuen les seves arrels (si és que existeixen)?

Proposició 3.6.1. *Sigui K un cos qualsevol, i $p(x) \in K[x]$ irreductible. Aleshores existeix una extensió L/K finita en la que $p(x)$ té una arrel.*

Demostració. Si $\deg p(x) = 1$, aleshores podem prendre $L = K$, ja que $p(x)$ té una arrel a K.

En general, considerem $L := K[x]/(p(x))$. Això és un cos, ja que $K[x]$ euclidià $\implies K[x]$ principal, i tot polinomi irreductible en un anell principal és maximal, de manera que $K[x]/(p(x))$ és un cos.

Aleshores, tenim un morfisme d'anells

$$\begin{aligned} \pi : K[x] &\longrightarrow L \\ f(x) &\longmapsto \overline{f(x)} \end{aligned}$$

que podem concatenar amb la inclusió:

$$\begin{aligned} K \hookrightarrow & K[x] \xrightarrow{\pi} L \\ a \mapsto & a \mapsto \overline{a} \end{aligned}$$

Aquesta aplicació $\iota : K \longrightarrow L$ és injectiva (ja que $p(x)$ no pot dividir una constant), de manera que podem identificar K amb un subcos de L i, per tant, podem veure L com a extensió de K. Donat que $p(x) \in K[x]$, aleshores podem pensar que $p(x) \in L[x]$.

Volem veure que $p(x)$ té una arrel a L. Sigui $\alpha = \pi(x) = x \mod p(x)$. Aleshores,

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{on } a_i \in K$$

$$p(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i \pi(x)^i = \pi\left(\sum_{i=0}^{n} a_i x^i\right) = \pi(p(x)) = 0$$

Aleshores, α és una arrel de $p(x)$ a L. Per acabar, veiem que L/K és finita, ja que qualsevol classe de $L = K[x]/(p(x))$ admet un representant de grau menor que $\deg p(x)$, de manera que podem agafar la base $L = K\langle 1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}\rangle$. □

((FALTA: explicacio de la identificacio de K amb un subcos de L – veure video 23/10))

Proposició 3.6.2 (Teorema de Krönecker)**.** *Sigui K un cos, i $p(x) \in K[x]$ (no necessàriament irreductible). Aleshores existeix una extensió finita L/K en la qual $p(x)$ descompon en factors lineals (és a dir, té totes les arrels a L).*

Demostració. Utilitzem la proposició anterior fent inducció sobre el grau de $p(x)$. □

Definició 3.6.1 (Cos de descomposició)**.** Un cos de descomposició de $f(x) \in K[x]$ és un cos L/K en el qual f descompon en producte de factors lineals i que sigui minimal amb aquesta propietat (és a dir, que si M/K és una extensió tal que $f(x)$ descompon linearment$/M$, aleshores existeix una immersió $L \hookrightarrow M$).

Observació. La pròpia definició ens garanteix que el cos de descomposició és únic llevat d'isomorfismes, ja que

$$L \hookrightarrow L' \hookrightarrow L \implies L \simeq L'$$

Comentari. Utilitzarem K_f per denotar un cos de descomposició de f/K, que serà únic llevat d'isomorfismes.

Observació. El cos de descomposició K_f depèn tant de f com de K. Per exemple, sigui $f(x) = x^2 - 3$, aleshores $\mathbb{Q}_f = \mathbb{Q}(\sqrt{3})$ però $\mathbb{R}_f = \mathbb{R}$.

Definició 3.6.2 (Composició de dos cossos)**.** Siguin $K \subset M$ i $L \subset M$ cossos. Aleshores definirem la *composició* de K amb L (KL) com el menor subcos de M que conté K i L.

Proposició 3.6.3. *Per qualssevol $f(x), g(x) \in K[x]$, si existeixen K_f, K_g i K_{fg}, llavors*

1. $K_f \subset K_{fg}$
2. $K_{fg} = K_f K_g$

Demostració. 1. f descompon en factors lineals a K_{fg}, de manera que existeix una immersió $K_f \hookrightarrow K_{fg}$, i per definició de cos de descomposició, $K_f \subset K_{fg}$.

2. Tenim que $K_f \subset K_{fg}$ i $K_g \subset K_{fg}$, de manera que $K_f K_g \subset K_{fg}$. A més, fg descompon en factors lineals a $K_f K_g$, de manera que $K_{fg} \subset K_f K_g$.

□

Proposició 3.6.4. *Sigui $f(x) \in K[x]$ irreductible. Sigui L/K una extensió qualsevol on $f(x)$ descompon linealment:*

$$f(x) = a(x-\alpha_1)\dots(x-\alpha_r), \quad \text{amb } \alpha_i \in L$$

Aleshores $K(\alpha_1,\dots,\alpha_r)$ és un cos de descomposició de f.

Demostració. Ho farem per inducció sobre el grau de $f(x)$. Si $n = 1$, tenim una sola arrel que està a K, de manera que $K(\alpha_1) = K$.

Si $n > 1$, f descompon linealment a $K(\alpha_1,\dots,\alpha_n)$. Sigui M/K una altra extensió on f descompon linealment.

$$f(x) = a(x-\beta_1)\dots(x-\beta_n), \quad \text{amb } \beta_i \in M$$

Definim l'aplicació

$$\begin{aligned} \tilde{K} = K(\alpha_1) &\hookrightarrow M \\ \alpha_i &\mapsto \beta_i \\ \sum a_1 \alpha_1^i &\mapsto \sum a_1 \beta_1^i \end{aligned}$$

Si $\alpha_2,\dots,\alpha_n \in \tilde{K}$, aleshores ja estem. Si una certa $\alpha_i \notin \tilde{K}$ (sense pèrdua de generalitat podem suposar que $\alpha_2 \notin \tilde{K}$), sigui $\tilde{f} = \mathrm{Irr}(\alpha_2, \tilde{K})$. Aquest polinomi compleix que $\deg \tilde{f} < \deg f$. Per tant, per hipòtesi d'inducció, $\tilde{K}(\alpha_2,\dots,\alpha_n)$ és cos de descomposició de $\tilde{f}$, de manera que existeix una immersió

$$\underbrace{\tilde{K}(\alpha_2,\dots,\alpha_n)}_{K(\alpha_1,\dots,\alpha_n)} \hookrightarrow M$$

que era el que ens faltava per demostrar. □

Corol·lari 3.6.1. *Tot polinomi $f \in K[x]$ té un cos de descomposició.*

Exemple 3.6.1. Sigui $K = \mathbb{Q}$, $f(x) = x^3 - 2$. Sigui $\sqrt[3]{2}$ la única arrel real de f. Sigui $\omega = e^{2\pi i/3}$. Aleshores, $\mathbb{Q}_f = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

3.7 Normalitat. Clausura algebraica

Definició 3.7.1 (Extensió normal)**.** Direm que una extensió L/K és *normal* si L és el cos de descomposició d'un cert $f(x) \in K[x]$.

Exemple 3.7.1.

- L'extensió trivial K/K és normal, ja que $K_{x-1} = K$.
- Siguin $K = \mathbb{Q}$ i $f(x) = (x^2-2)(x^2-3)$. Aleshores $\mathbb{Q}_f = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ és normal.
- Siguin $K = \mathbb{Q}$, $f(x) = x^3 - 2$ i $\omega = e^{2\pi i/3}$. Aleshores, $L = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ és normal/$\mathbb{Q}$, perquè $L = \mathbb{Q}_f$.

Ens podríem preguntar si una extensió donada com $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ és normal. Sabem que $\mathbb{Q}(\sqrt[3]{2})$ no és el cos de descomposició de $x^3 - 2$ (ja que hi ha arrels del polinomi que no hi pertanyen), però com podem saber si existeix un altre polinomi tal que $\mathbb{Q}(\sqrt[3]{2})$ és el seu cos de descomposició?

Podem veure que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no és una extensió normal utilitzant la següent proposició.

Proposició 3.7.1. *Sigui L/K una extensió normal, i sigui $f(x) \in K[x]$ irreductible. Aleshores, si $f(x)$ té una arrel en L, les hi té totes.*

Demostració. L/K és normal, de manera que $L = K_\varphi$ per un cert $\varphi(x) \in K[x]$. Sigui α una arrel de f en L, i $\beta \in L_f$ una altra arrel de f, amb $\alpha \neq \beta$. Volem veure que $\beta \in L$.

Observem que $L(\beta) = K(\beta)_\varphi$ (ja que és l'extensió minimal de $K(\beta)$ en la qual φ descompon linealment. De la mateixa manera, $L(\alpha) = K(\alpha)_\varphi$.

Per altra banda, tenim que $K(\alpha) \simeq K[x]/(f(x)) \simeq K(\beta)$. Per la unicitat (llevat d'isomorfisme) del cos de descomposició, tenim que $L(\alpha) = K(\alpha)_\varphi \simeq K(\beta)_\varphi = L(\beta)$.

Donat que $\alpha \in L$, $L(\alpha) = L$. Per tant, $[L(\beta) : K] = [L(\alpha) : K] = [L : K]$, de manera que $[L(\beta) : L] = 1 \implies L(\beta) = L \implies \beta \in L$. □

Observació. De fet, la propietat anterior caracteritza les extensions normals:

Proposició 3.7.2. *L/K és una extensió normal $\iff$ $\forall f \in K[x]$ irreductible, f té una arrel en L sii les hi té totes.*

Demostració. No demostrarem la implicació cap a l'esquerra en general però, per L/K separable, podem aplicar el teorema de l'element primitiu i tenim que $L = K(\alpha)$ per un cert α, i aleshores $L = K_f$ amb $f = \mathrm{Irr}(\alpha, K)$. □

Definició 3.7.2 (Clausura algebraica)**.** Sigui K un cos qualsevol. Una *clasura algebraica* de K és una extensió $\bar{K}/K$ en la qual tot polinomi descompon linearment, i que és minimal entre totes les extensions que compleixen aquesta propietat.

Observació. Si α és algebraic/K, aleshores $\alpha \in \bar{K}$ (de fet, en realitat $K(\alpha) \hookrightarrow \bar{K}$). És per això que s'anomena clausura algebraica, perquè "conté" tots els elements algebraics sobre K.

Proposició 3.7.3 (Teorema)**.** *Tot cos té una clausura algebraica, que a més és única llevat d'isomorfisme.*

Definició 3.7.3 (Algebraicament tancat)**.** Diem que un cos és algebraicament tancat si $\bar{K} = K$.

Exemple 3.7.2. $K = \mathbb{C}$ és algebraicament tancat (teorema fonamental de l'àlgebra).

Proposició 3.7.4. *$\bar{\mathbb{Q}}$ és numerable (i per tant, en particular, $\bar{\mathbb{Q}} \neq \mathbb{C}$).*

Demostració. Per un $n \in \mathbb{N}$ fixat, el conjunt de polinomis de $\mathbb{Q}[x]$ de grau n ($\mathbb{Q}_n[x]$) és numerable. Observem que $\mathbb{Q}[x] = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n[x]$, que és unió numerable de conjunts numerables, i per tant és numerable.

Donat un $f \in \mathbb{Q}[x]$, f té un nombre d'arrels finit. Per tant, $\bar{\mathbb{Q}}$ és una unió numerable de conjunts finits, i és numerable. □

Corol·lari 3.7.1. *Hi ha una infinitat no numerable de nombres transcendents sobre* $\mathbb{Q}$.

3.8 Cossos finits

Definició 3.8.1 (Cos finit de p elements)**.** Sigui $p \in \mathbb{N}$ primer. Definirem el *cos finit de p elements* com

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

Observació. Parlarem de "el" cos finit de p elements i no "un" cos finit de p elements perquè després veurem que tot altre cos finit de p elements serà isomorf a $\mathbb{F}_p$.

Exemple 3.8.1. Sigui $f(x) = x^2+1 \in \mathbb{F}_3[x]$. Observem que $f(x)$ és irreductible a $\mathbb{F}_3[x]$, perquè és de grau 2 i no té arrels (com que el cos és finit, per veure si té arrels podem provar per força bruta cada un dels elements del cos).

Tenim que $\mathbb{F}_3[x]$ és un anell principal (ja que és euclidià). Aleshores $f(x)$ irreductible $\implies$ $(f(x))$ primer $\implies$ $(f(x))$ maximal. Per tant, $F = \mathbb{F}_3[x]/(f(x))$ és un cos. Sigui $\alpha = \overline{x}$. Aleshores F també serà un cos finit, i el podem escriure com

$$F = \mathbb{F}_3(\alpha) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\} = \{a + b\alpha : a, b \in \mathbb{F}_3[x]\}$$

El cardinal d'aquest cos serà $\#F = 3^2 = 9$, ja que cada un dels dos coeficients del polinomi pot ser qualsevol dels tres elements de $\mathbb{F}_3[x]$.

Sigui F un cos finit qualsevol, amb $m = \operatorname{char} F$ (tenim que $m \neq 0$ perquè F és finit). Recordem que podem definir un morfisme

$$\begin{aligned} \mathbb{Z} &\xrightarrow{\iota} F \\ a &\mapsto a \cdot 1_F \end{aligned}$$

amb nucli $\ker \iota = (m)$. Aleshores, tenim una inclusió $\mathbb{Z}/(m) \overset{\iota}{\hookrightarrow} F$, de manera que $\mathbb{Z}/(m)$ és integre i, per tant, m és primer.

Per tant, tot cos finit F té característic primer. A més, la inclusió anterior ens diu que si $\operatorname{char} F = p$, F és extensió de $\mathbb{F}_p$. En aquest cas, diem que $\mathbb{F}_p$ és el *cos primer* de F.

Donat que F és finit, $[F : \mathbb{F}_p] < \infty$. Sigui $\omega_1, \ldots, \omega_n$ una $\mathbb{F}_p$-base de F. Aleshores, per definició de base,

$$F = \{a_1\omega_1 + \cdots + a_n\omega_n : a_i \in \mathbb{F}_p\}$$

Com que $\{\omega_i\}$ és una base, aquesta representació és unívoca, de manera que $\#F = p^n = p^{[F:\mathbb{F}_p]}$. És a dir, tot cos finit té com a cardinal una potència d'un nombre primer.

El mateix raonament ens permet dir que si H/F és una extensió finita de F, aleshores H és finit i

$$\#H = (\#F)^{[H:F]} = p^{r[H:F]}$$

on $p^r = \#F$. En particular, tenim que $\#F \mid \#H$.

Recíprocament, es pot demostrar fàcilment que si F és finit i té cardinal p^r, tenim que $\operatorname{char} F = p$ i $\mathbb{F}_p \subset F$.

Proposició 3.8.1. *Sigui F un cos finit qualsevol, amb cardinal $\#F = q = p^r$. Sigui $f(x) \in F[x]$ irreductible de grau n. Aleshores,*

$$H = F[x]/(f(x)) \text{ és finit i } \#H = q^n = p^{rn}$$

Demostració. Aquesta proposició es correspon a l'exemple que hem comentat abans. Sigui $\alpha = \overline{x} \in H$. Tenim que $H = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F\}$. Aleshores $\#H = q^n$ i $[H : F] = n$ (podem agafar la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$). □

Exemple 3.8.2. Sigui $g(x) = x^2+x-1 \in F_3[x]$ que és irreductible (ho podem veure comprovant que els 3 elements de F_3 no són arrels). Sigui $G = \mathbb{F}_3[x]/(g(x)) = \mathbb{F}_3(\beta)$, amb $\beta = \overline{x}$. Observem que $\#G = 9$, igual que $F = \mathbb{F}_3[x]/(x^2 + 1)$, que és l'exemple que havíem vist abans.

Abans hem afirmat que els cossos finits de n elements són únics llevat d'isomorfisme. En aquest cas, un possible isomorfisme és

$$\begin{aligned} F = \mathbb{F}_3(\alpha) &\longrightarrow G = \mathbb{F}_3(\beta) \\ a + b\alpha &\longmapsto a + b(\beta - 1) \end{aligned}$$

Es pot comprovar que aquesta aplicació està ben definida i és un isomorfisme. Com a exercici, es pot buscar un altre cos de 9 elements i trobar l'isomorfisme amb aquests dos.

Comentari. S'ha de vigilar de no confondre els cossos finits amb $\mathbb{Z}/n\mathbb{Z}$. Hem vist que per p primer $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$, però aquesta relació no es compleix per n compost, ja que $\mathbb{Z}/n\mathbb{Z}$ no és ni tan sols un cos. Per tant, el cos $G \simeq \mathbb{F}_9$ que ha aparegut a l'exemple no té res a veure amb l'anell $\mathbb{Z}/9\mathbb{Z}$.

Encara no hem definit un cos finit "canònic" de n elements, amb n no primer. Recordem primer un resultat que ja s'ha vist a l'assignatura de Fonaments:

Proposició 3.8.2 (Petit teorema de Fermat)**.** *Per qualssevol $a, p \in \mathbb{Z}$ amb p primer, $a^p = a \mod p$. En el llenguatge de cossos finits, això s'expressa com $a^p = a$ per qualsevol $a \in \mathbb{F}_p$.*

Demostració. Si $a = 0$, $0^p = 0$. Altrament, $a \in \mathbb{F}_p^*$, que és un grup multiplicatiu (s'ha vist a l'assignatura de Fonaments). Aleshores, donat que $\#F_p^* = p - 1$, tenim que $a^{p-1} = 1 \implies a^p = a$. (En el capítol de grups repassarem això i ho demostrarem des de zero.) □

Corol·lari 3.8.1. *A* $\mathbb{F}_p[x]$,

$$x^p - x = x(x-1)(x-2)\dots(x-(p-1))$$

és a dir, $\mathbb{F}_p$ *és el cos de descomposició (sobre ell mateix) de* $\varphi(x) = x^p - x$.

Demostració. Els dos polinomis són polinomis mònics del mateix grau i amb les mateixes arrels (pel petit teorema de Fermat), de manera que són iguals. □

Sigui F finit amb $\#F = q = p^r$ i p primer. Aleshores, tenim també que F^* és un grup multiplicatiu de cardinal $\#F = q - 1$, de manera que $\alpha^q = \alpha$ per qualsevol $\alpha \in F^*$.

Aleshores,

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) \mid \varphi_q(x) := x^q - x$$

Com que tenen el mateix grau i són mònics, tenim novament que

$$\varphi_q(x) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$$

Per tant, al final el que estem dient és que $F = \{\text{arrels de } \phi_q\}$. Per tant, F és el cos de descomposició de ϕ_q sobre $\mathbb{F}_p$.

Proposició 3.8.3 (Teorema)**.** *Per cada primer* $p \in \mathbb{N}$ *i cada potència* $q = p^n$*, existeix un cos finit de* q *elements, que és únic llevat d'isomorfisme. El denotarem gènericament com* $\mathbb{F}_q$.

Demostració. Definim $\mathbb{F}_q := (\mathbb{F}_p)_{x^q - x}$ (cos de descomposició de $x^q - x$ sobre $\mathbb{F}_p$). El polinomi $\varphi_q(x) = x^q - x$ és separable, perquè la seva derivada és $\varphi_q'(x) = qx^{q-1} - 1 = -1 \neq 0$, de manera que φ_q no té arrels múltiples. Aleshores, efectivament $\#\mathbb{F}_q = q$, tal i com volíem. La unicitat la tenim perquè hem vist abans que tot cos finit de q elements és un cos de descomposició de $\varphi_q(x)$ sobre $\mathbb{F}_p$, i el cos de descomposició és únic llevat d'isomorfisme. □

Proposició 3.8.4. $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$

Demostració. Suposem que $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. Vam veure que $\#\mathbb{F}_{p^n} = (\#F_{p^m})^r$. Per tant,

$$p^n = (p^m)^r = p^{mr} \implies n = mr \implies m \mid n$$

Observem que, per veure que $n = mr$, estem utilitzant implícitament el teorema fonamental de l'aritmètica, ja que utilitzem que dues descomposicions en primers d'un cert $x \in \mathbb{Z}$ han de tenir els mateixos factors primers (llevat d'unitats) elevats als mateixos exponents.

Anem a veure la implicació contrària. Suposem que $m \mid n$. Aleshores, sigui $r = n/m$,

$$p^n - 1 = (p^m)^r - 1 = (p^m - 1)\left(\sum_{k=0}^{r-1} p^{mk}\right)$$

Sigui $\alpha \in \mathbb{F}_{p^m}$. Volem veure que $\alpha \in \mathbb{F}_{p^n}$. N'hi ha prou amb veure que $\alpha^{p^n} = \alpha$, ja que hem caracteritzat F_{p^n} com el cos de descomposició de $x^{p^n} - x$. Si $\alpha = 0$ és trivial. Altrament, tenim que

$$\alpha^{p^n-1} = (\alpha^{p^m-1})^{\sum_{k=0}^{r-1} p^{mk}}$$

Teníem que $\alpha \in \mathbb{F}_{p^m} \implies \alpha^{p^m-1} = 1$. Aleshores, $\alpha^{p^n-1} = 1 \implies \alpha^{p^n} = \alpha \implies \alpha \in \mathbb{F}_p^n$. □

Podem reinterpretar aquesta proposició en termes dels polinomis $x^q - x \in \mathbb{F}_p[x]$. La proposició anterior és equivalent a dir que, a $\mathbb{F}_p[x]$,

$$x^{p^m} - x \mid x^{p^n} - x \iff m \mid n$$

Observem però que, a $\mathbb{Q}[x]$, només seria certa la implicació cap a l'esquerra.

Una tercera versió alternativa del teorema és

Proposició 3.8.5 (Teorema)**.** *A $\mathbb{F}_p[x]$,*

$$x^{p^n} - x = \prod_{d \mid n} \prod_{\substack{f(x) \in \mathbb{F}_p[x] \\ \text{mònic irred} \\ \deg f = d}} f(x)$$

Demostració. Sigui $q = p^n$ i $\varphi_q(x) = x^q - x$. Sigui $f(x) \in \mathbb{F}_p[x]$ un polinomi mònic irreductible de grau $d \mid n$. Aleshores, tenim que $(\mathbb{F}_p)_f = \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Sigui $\alpha \in \mathbb{F}_{p^d}$ una arrel de f. Donat que $\alpha \in \mathbb{F}_{p^n}$, $\varphi_q(\alpha) = 0$.

Aleshores, $x - \alpha \mid f(x)$ i $x - \alpha \mid \varphi_q(x)$, de manera que $x - \alpha \mid \gcd(f(x), \varphi_q(x))$. Tant $f(x)$ com $\varphi_q(x)$ pertanyen a $\mathbb{F}_p[x]$, de manera que el seu gcd també. A més, donat que $x - \alpha$ el divideix a $\mathbb{F}_q[x]$, tenim que el gcd no pot ser de grau zero. Per tant, com que havíem demanat que $f(x)$ fos irreductible a $\mathbb{F}_p[x]$ i $f(x)$ i $\varphi_q(x)$ no són coprimers, la única opció possible és que $f(x) = \gcd(f(x), \varphi_q(x))$.

En particular, això implica que $f(x) \mid \varphi_q(x)$. Per tant,

$$H(x) = \prod_{d \mid n} \prod_{\substack{f(x) \in \mathbb{F}_p[x] \\ \text{mònic irred} \\ \deg f = d}} f(x) \mid x^q - x$$

i aleshores existeix un $G(x)$ tal que $x^q - x = H(x)G(x)$. Si tinguéssim que $\deg G(x) \geq 1$, hauria de tenir algun factor irreductible $g(x)$ amb $\deg g(x) = s \geq 1$, ja que $\mathbb{F}_p[x]$ és factorial.

Com $x^q - x$ és separable, no té arrels múltiples, de manera que $g(x)$ no està entre els factors de $H(x)$. Per altra banda, $g(x) \mid x^q - x \implies (\mathbb{F}_p)_g \subset \mathbb{F}_q \implies s \mid n$. Però aleshores $g(x)$ és un dels factors de $H(X)$, arribant a una contradicció.

Per tant, $G(x)$ ha de ser una unitat. Teníem que $H(x)G(x) = x^q - x$ i que tant $H(x)$ com $x^q - x$ són mònics, de manera que $H(x) = x^q - x$. □

Exemple 3.8.3. A $\mathbb{F}_3[x]$,

$$x^9 - x = \underbrace{x(x-1)(x-2)}_{\text{irreductibles grau 1}}\underbrace{(x^2+1)(x^2+x-1)(x^2-x-1)}_{\text{irreductibles grau 2}}$$

Observem que només considerem els polinomis mònics.

En particular, com el grau del polinomi és 9 i sabent que hi ha 3 polinomi mònics irreductibles de grau 1, obtenim directament que hi ha $\frac{9-3}{2} = 3$ polinomis mònics irreductibles de grau 2 (sense haver de calcular-los explícitament!). Això es pot generalitzar per a un $\mathbb{F}_p$ qualsevol.

Corol·lari 3.8.2. *A $\mathbb{F}_p[x]$ hi ha $(p^2-p)/2$ polinomis mònics irreductibles de grau 2 i $(p^3-p)/3$ polinomis mònics irreductibles de grau 3.*

En general, es pot saber quants irreductibles hi ha de qualsevol grau. Com a exercici, trobeu una fórmula vàlida per a grau qualsevol. (*Pista:* involucra la funció φ d'Euler).

Passem ara a estudiar l'estructura interna dels cossos finits.

Proposició 3.8.6 (Teorema)**.** *El grup multiplicatiu d'un cos finit és cíclic. És a dir, existeix una $\zeta \in \mathbb{F}_q^*$ d'ordre $q-1$ tal que $\mathbb{F}_q^* = \langle\zeta\rangle = \{1, \zeta, \ldots, \zeta^{q-2}\}$.*

Demostració. Sigui $q - 1 = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ on p_i són primers i $\alpha_i > 0$. Per a cada p_i, triem $y_i \in \mathbb{F}_q^*$ tal que $y_i^{(q-1)/p_i} \neq 1$. Observem que sempre existeix un y_i que ho compleixi, perquè el polinomi $x^{(q-1)/p_i} - 1$ té grau menor que $x^{q-1} - 1$, de manera que alguna de les arrels de $x^{q-1} - 1$ no és arrel de $x^{(q-1)/p_i} - 1$.

Prenem $\zeta_i = y_i^{(q-1)/p_i^{\alpha_i}}$. L'ordre de ζ_i és $p_i^{\alpha_i}$. (Es pot comprovar com a exercici.) Aleshores, prenem $\zeta := \zeta_1 \ldots \zeta_r$. Donat que els ordres de ζ_i són coprimers, es pot veure que $\operatorname{ord}(\zeta) = \prod \operatorname{ord}(\zeta_i) = q - 1$. (Es pot veure per inducció sobre r, però no ho farem, ja que veurem aquest tipus de qüestions amb més detall al capítol de grups.)

Per tant, $1, \zeta, \zeta^2, \ldots, \zeta^{q-2}$ són tots diferents i $\mathbb{F}_q^* = \langle\zeta\rangle$. □

Corol·lari 3.8.3. *Tot cos finit és una extensió simple del seu cos primer. Més concretament, sigui $q = p^n$ i sigui ζ tal que $\mathbb{F}_q^* = \langle\zeta\rangle$, aleshores $\mathbb{F}_q = \mathbb{F}_p(\zeta)$.*

Demostració. Sigui $q = p^n$ i sigui ζ tal que $\mathbb{F}_q^* = \langle\zeta\rangle$. Si $n = 1$, el resultat és trivial. Altrament, tenim que $\operatorname{ord}(\zeta) = q - 1 \neq p - 1 \implies \zeta \notin \mathbb{F}_p$.

Tota extensió d'un cos finit té com a grau una potència de la característica, de manera que $[\mathbb{F}_p(\zeta) : \mathbb{F}_p] = r$. A més, $r \mid n \implies r \leq n$, ja que $\mathbb{F}_p(\zeta) \subset \mathbb{F}_q$. Aleshores, $\#\mathbb{F}_p(\zeta) = p^r \implies \zeta^{p^r-1} = 1$. Per altra banda, $\operatorname{ord}(\zeta) = q-1$, de manera que $q-1 \mid p^r-1 \implies q \leq p^r \implies n \leq r$.

Hem vist les dues desigualtats, de manera que $n = r$. Per tant, $[\mathbb{F}_p(\zeta) : \mathbb{F}_p] = r = n = [\mathbb{F}_q : \mathbb{F}_p]$, i donat que $\mathbb{F}_p(\zeta) \subset \mathbb{F}_q$, tenim que $\mathbb{F}_p(\zeta) = \mathbb{F}_q$. □

Corol·lari 3.8.4 (Teorema de l'element primitiu per a cossos finits)**.** *Tota extensió finita d'un cos finit és simple.*

Demostració. Sigui $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ una extensió de cossos finits. Prenem ζ tal que $\mathbb{F}_{q^n}^* = \langle\zeta\rangle$. Pel corol·lari anterior, $\mathbb{F}_{q^n} = \mathbb{F}_p(\zeta)$ i, com que $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}/\mathbb{F}_p$, tenim que $\mathbb{F}_p(\zeta) = \mathbb{F}_{q^m}(\zeta)$, de manera que $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ és simple. □

3.9 Aplicacions dels cossos finits

A l'hora de transmetre informació per mitjans digitals, s'incorporen tota una sèrie de mesures de seguretat que tenen dos objectius: assegurar la integritat de les dades (és a dir, detectar i corregir les interferències que pugui rebre el missatge durant la seva transmissió) i protegir la seva confidencialitat (mitjançant algoritmes de xifratge).

Antigament, els sistemes de xifratge es basaven en l'existència d'una clau secreta que només coneixien l'emissor i el receptor. Actualment, però, aquest tipus de sistemes han estat substituits per la criptografia de clau pública.

En la criptografia de clau pública, cada usuari té dues claus: una privada, que només coneixen ells, i una pública, que comparteixen amb la resta. Les claus s'escullen de manera que un missatge encriptat amb la clau pública d'un usuari només es pot desxifrar amb la clau privada del mateix usuari. Per tant, si A vol enviar un missatge a B, A xifrarà el missatge amb la clau pública de B, de manera que només el pot desxifrar B, que és l'únic que té la clau privada corresponent.

Els sistemes de clau pública acostumen a ser més costosos. Per tant, per estalviar diners, sovint es combinen els dos sistemes: els missatges s'encripten amb un sistema de clau secreta i aquesta clau secreta es transmet entre emissor i receptor mitjançant un sistema de clau pública.

3.9.1 Intercanvi de claus de Diffie-Hellman

L'algorisme de Diffie-Hellman permet acordar una clau secreta entre dos usuaris sense que algú que intercepti els seus missatges pugui averiguar quina és. L'algorisme és el següent:

Algorisme de Diffie-Hellman:

1. Triem $q = p^r$ gran (actualment s'utilitza $q \simeq 2^{1000}$) i triem un generador g de $\mathbb{F}_q^*$ (és a dir, un $g \in \mathbb{F}_q$ tal que $\langle g \rangle = \mathbb{F}_q^*$.

2. L'usuari A tria una $a \in \{1, \ldots, q-1\}$ a l'atzar, i calcula $u_A = g^a$.

3. L'usuari B tria una $b \in \{1, \ldots, q-1\}$ a l'atzar, i calcula $u_B = g^b$.

4. Els usuaris A i B s'intercanvien u_A i u_B.

5. La clau comuna serà $k = g^{ab}$, que A calcula com $k = (u_B)^a$ i B calcula com $k = (u_A)^b$.

Un espia que intercepti les comunicacions només té accés a g, $u_A = g^a$ i $u_B = g^b$, i no es coneix cap manera de calcular $k = g^{ab}$ eficientment a partir d'aquests (suposant que el cos és prou gran i no es poden provar totes les possibilitats a força bruta). Aquest és el que es coneix com a problema de Diffie-Hellman:

Problema de Diffie-Hellman: Donats g, g^a i g^b, calcula g^{ab} (sense conèixer a i b).

No està demostrat, però es conjectura que no hi ha cap algorisme en temps polinòmic per resoldre aquest problema.

3.9.2 Criptosistema d'Elgamal

Triem un cos finit $\mathbb{F}_q$ amb cardinal q gran, i $g \in \mathbb{F}_q^*$ tal que $\mathbb{F}_q^* = \langle g \rangle$. Identificarem cada missatge natural amb un element de $\mathbb{F}_q$ (lletra per lletra, o de maneres més sofisticades, pels propòsits de l'algorisme ens és igual).

En aquest context, el xifratge consistirà en transformar el missatge original $m \in \mathbb{F}_q^*$ en el missatge xifrat $\tilde{m} \in \mathbb{F}_q^*$ de manera que només es pugui recuperar m a partir de $\tilde{m}$ si es coneix una certa clau secreta.

Volem que el procés de xifratge i desxifratge sigui eficient. Per tant, volem que els càlculs per passar de m a $\tilde{m}$ o viceversa siguin ràpids i que la mida del missatge xifrat no sigui gaire més gran que la del missatge original.

Cada usuari A_i tria una clau secreta $ks_i \in \{1, \dots, q-1\}$ a l'atzar, i fa públic $kp_i = g^{ks_i}$. Si algú li vol enviar un missatge m a l'usuari A_i, tria un $k \in \{1, \dots, q-1\}$ a l'atzar i li envia el parell $\tilde{m} = (g^k, g^{ks_i \cdot k} m)$ de manera pública. Observem que, com que la clau $kp_i = g^{ks_i}$ és pública, qualsevol usuari pot calcular $g^{ks_i k} = (kp_i)^k$.

Per desxifrar el missatge, l'usuari A_i calcula

$$m = \frac{g^{ks_i \cdot k} m}{(g^k)^{ks_i}}$$

que observem que pot calcular tot i no conèixer k.

En canvi, un espai no pot desxifrar el missatge, ja que no pot calcular el denominador sense conèixer ks_i o k. Per trobar-los, s'hauria de resoldre un logaritme discret:

$$k = \log_g(g^k) = \log_{g^{ks_i}}(g^{k \cdot ks_i})$$

Per tant, la seguretat del criptosistema d'Elgamal es basa en la dificultat de calcular logaritmes discrets computacionalment. És per això que elegim q gran, per tal de que trobar logaritmes a $\mathbb{F}_q$ sigui intractable. De fet, es pot demostrar que es pot reduir el problema del logaritme discret al problema de Diffie-Hellman.

3.9.3 Codis correctors d'errors

Quan transmitim dades, es poden produir interferències que modifiquin el contingut del missatge. Els codis correctors d'errors es basen en afegir informació extra al missatge per tal de poder detectar quan es produeix un error (i en alguns casos recuperar el missatge original).

Un exemple quotidià d'un protocol per detectar errors és la lletra del DNI, que es calcula prenent mòdul 26, i que permet detectar si s'ha escrit algun dígit malament (la majoria de les vegades). A continuació donarem un protocol per no només detectar errors sinó per corregir-los.

Suposem que tenim un conjunt finit de missatges. Com a exemple, agafarem el conjunt de paraules de 8 lletres, identificant cada lletra amb el seu codi ASCII. Hi ha $256 = 2^8$ càracters ASCII, de manera que tindrem un total de $(2^8)^8 = 2^{64}$ missatges possibles. Per tant, podem identificar cada paraula amb un element de $\mathbb{F}_{2^{64}}$.

Aquesta identificació no la farem de qualsevol manera. Prenem un $n > 0$ i a l'espai vectorial $(\mathbb{F}_2)^n$ triem un subespai V de dimensió 64. Aleshores, $\#V = 2^{64}$. Triant una base de V, tenim un isomorfisme $\mathbb{F}_{2^{64}} \simeq V$.

Aleshores, trobant les equacions que descriuen V com a subespai de $(\mathbb{F}_2)^n$, tindrem que els missatges correctes seran aquells elements de $(\mathbb{F}_2)^n$ que satisfacin aquestes equacions. Això ens permet detectar errors (ja que la probabilitat de que una interferència aleatòria modifiqui el missatge sense fer que surti de V és molt petita).

Exemple 3.9.1. A $(\mathbb{F}_{2^{64}})^3$ podríem prendre $V = \{(x, y, z) \in (\mathbb{F}_{2^{64}})^3 : x = y = x\}$. És a dir, codifiquem un missatge repetint-lo 3 cops. Aquesta codificació és "bastant" segura, però és molt cara, ja que requereix enviar un missatge 3 vegades més llarg que l'original.

Habitualment, diem que la n és la *longitud del codi*, mentre que la $k = \dim V$ diem que és la *dimensió del codi*. Al quocient k/n l'anomenem *ratio del codi*. En aquest exemple, el codi és molt poc eficient, ja que $k/n = 1/3 << 1$ (no es el que va dir a classe(?)).

Per tal de poder corregir errors, necessitem definir d'alguna manera la distància entre missatges.

Definició 3.9.1 (Pes de Hamming)**.** Definim el pes de Hamming d'un element $v \in \mathbb{F}_{q^n}$ com el nombre de coordenades no nul·les de v:

$$w : \mathbb{F}_{q^n} \longrightarrow \mathbb{N}$$
$$v = (a_1, \ldots, a_n) \mapsto w(v) = \#\{i : a_i \neq 0\}$$

A partir del pes de Hamming, definim la distància minimal en el codi V com el mínim pes de Hamming d'un element de V:

Definició 3.9.2 (Distància minimal en V)**.**

$$d(V) := \min\{w(v) : v \in V \setminus \{0\}\}$$

Per tant, si rebem un missatge $r \notin V$, el substituim pel $c \in V$ tal que $w(r - c)$ sigui mínima (és a dir, el que tingui més bits en comú).

Es pot demostrar que si $w(r - m) \leq d(V)/2$, aleshores el c que obtenim amb aquest procediment coincideix amb m. Per tant, sempre que no hi hagi més de $d(V)/2$ bits erronis, podem recuperar sense error el missatge original.

3.9.4 Esquemes per compartir secrets

Volem compartir un secret $s \in \mathbb{F}_p$ entre n persones de manera que calguin al menys t persones per reconstruir-lo.

Triem $p >> n$. Construim a l'atzar un polinomi $H(x) \in \mathbb{F}_p[x]$ tal que $\deg H(x) \leq t - 1$ i $H(0) = s$. Triem $x_1, \ldots, x_n \in \mathbb{F}_p$ a l'atzar i calculem $s_i = H(x_i)$. A cada usuari li enviem un parell (x_i, s_i). Aleshores, per recuperar s s'ha de trobar $H(x)$, interpolant-lo a partir dels $H(x_i)$ coneguts.

Per tant, es necessita la col·laboració de t persones per reconstruir el secret. Un avantatge d'aquest esquema respecte a altres com el criptosistema de Diffie-Hellman és que la seguretat

d'aquest esquema no depèn de la potència de càlcul. Per molt que un usuari tingui potència de càlcul infinita, si només reuneix $r < t$ persones, hi haurà múltiples polinomis que passin pels r punts, i no tindrà cap manera d'esbrinar el secret.

3.10 Cossos ordenats

3.10.1 Definició i propietats bàsiques

En aquesta secció, construirem el cos dels nombres reals de manera axiomàtica. El cos dels nombres reals també es poden construir d'altres maneres, com amb els talls de Dedekind, però nosaltres ho farem d'aquesta manera perquè és més general i es pot aplicar a altres cossos.

En primer lloc, necessitem definir un valor absolut. Una de les maneres de fer-ho és a partir d'un ordre.

Definició 3.10.1 (Anell ordenat)**.** Un *anell ordenat* és un anell A amb una relació d'ordre total '$>$' compatible amb les operacions. És a dir, tal que $\forall\, x, y, x', y' \in A$,

1. $x > x'$, $y > y' \implies x + y > x' + y'$
2. $x > 0$, $y > 0 \implies xy > 0$

Definició 3.10.2 (Con positiu)**.** El *con positiu* d'un anell ordenat A és el conjunt d'elements de l'anell més grans que zero:

$$A^+_> = \{a \in A : a > 0\}$$

Observació. Donar un ordre '$>$' equival a donar el con positiu de l'anell, ja que $x > y \iff x - y \in A^+_>$.

Per tant, és molt fàcil donar l'ordre d'un anell, ja que només hem de donar el conjunt d'elements positius. Observem però que no tot anell és ordenable:

Lema 3.10.1. *Sigui A un anell ordenat. Aleshores,*

1. *A és un anell íntegre i* $\operatorname{char}(A) = 0$.
2. *Per tot $x \in A \setminus \{0\}$, $x^2 > 0$. En particular,* $1 = 1^2 > 0$.

Demostració. En primer lloc veurem que A ha de ser íntegre. Siguin x i $y \in A \setminus \{0\}$. Si $x > 0$ i $y > 0$, aleshores $xy > 0 \implies xy \neq 0$. Similarment, si $x > 0$ i $y < 0$, aleshores $x(-y) > 0 \implies xy = -(x(-y)) < 0 \implies xy \neq 0$. Els altres dos casos es fan de manera anàloga.

De la definició d'anell ordenat, si $x = y > 0$, aleshores $x^2 = xy > 0$. Per tant, $1 = 1^2 > 0$. Això ens permet demostrar per inducció que la característica és zero. Suposem que $k > 0$, aleshores, com $1 > 0$, tenim que $k + 1 > 0 + 0 = 0$. Per tant, per tot $n \in \mathbb{Z}^+$, $n > 0$, de manera que $\operatorname{char}(A) = 0$. □

Observació. La primera condició ens diu, en particular, que no podem ordenar cap cos finit, ja que tots tenen característica diferent de zero.

Observació. En tot cos ordenat, $-1 < 0$, ja que $0 - (-1) = 1 > 0$. Això implica que no es pot definir un ordre en $\mathbb{C}$, ja que aleshores $-1 = i^2 > 0$. Igualment, tampoc es poden ordenar els enters de Gauss, $\mathbb{Z}[i]$.

Proposició 3.10.1. *Sigui A un cos ordenat, aleshores existeix una única manera d'extendre l'ordre de A al seu cos de fraccions $k = \mathrm{Fr}(A)$.*

Demostració. Sigui $a/b \in k = \mathrm{Fr}(A)$. Observem que,

$$\frac{a}{b} > 0 \iff \frac{a}{b}b^2 > 0 \iff ab > 0$$

Com que $ab \in A$ i volem que l'ordre de k sigui compatible amb l'ordre d'A, per força tenim que

$$k^+ = \left\{ \frac{a}{b} \in k : ab >_A 0 \right\}$$

i ja hem vist que donar el con positiu determina totalment l'ordre. □

Proposició 3.10.2. *El cos dels nombres enters $\mathbb{Z}$ admet un únic ordre.*

Demostració. Sigui '$>$' un ordre de $\mathbb{Z}$. Hem vist que $1 > 0$ i que, per inducció, $n > 0$ per tot $n \in \mathbb{N} \setminus \{0\}$. També hem vist que $-1 < 0$. Utilitzant el mateix raonament que abans, això implica per inducció que $-n < 0$ per tot $n \in \mathbb{N} \setminus \{0\}$. Per tant, el con positiu de $\mathbb{Z}$ és

$$\mathbb{Z}^+_> = \mathbb{N} \setminus \{0\}$$

que és el con positiu de $\mathbb{Z}$ amb l'ordre canònic. Donat que el con positiu determina unívocament l'ordre, tenim que '$>$' ha de ser l'ordre canònic. □

Corol·lari 3.10.1. *El cos dels nombres racionals $\mathbb{Q}$ admet un únic ordre.*

Demostració. Tenim que $\mathbb{Z}$ té un únic ordre i $\mathbb{Q} = \mathrm{Fr}(\mathbb{Z})$, de manera que $\mathbb{Q}$ té un únic ordre. □

3.10.2 Completació d'un cos ordenat

Definició 3.10.3. Sigui k un cos ordenat. Definim el *valor absolut* d'un element $a \in k$ com $|a|_k := \max\{-a, a\}$.

Proposició 3.10.3. *El valor absolut satisfà*

1. $|a|_k > 0$ *si* $a \neq 0$
2. $|ab|_k = |a|_k \cdot |b|_k$
3. $|a + b|_k \leq |a|_k + |b|_k$

A partir de la noció de valor absolut ja podem definir les successions de Cauchy.

Definició 3.10.4 (Successió de Cauchy)**.** Una successió $(a_n)_{n\in\mathbb{N}}$ d'elements de k és de Cauchy si, per tot $\varepsilon \in K^+$, existeix un $n_0 \in \mathbb{N}$ tal que $|a_m - a_n|_k < \varepsilon$ per tot $m, n \geq n_0$.

Definició 3.10.5 (Convergència)**.** Una successió $(a_n)_n$ d'elements de k convergeix a $\ell \in k$ si, per tot $\varepsilon \in K^+$, existeix un $n_0 \in \mathbb{N}$ tal que $|a_n - \ell|_k < \varepsilon$ per tot $n \geq n_0$.

Notació: Utilitzarem $SC(k)$ per referir-nos al conjunt de successions de Cauchy del cos k, $SCV(k)$ per al conjunt de successions convergents a un element de k i $S_0(k)$ per al conjunt de successions convergents a 0. (*Atenció: Aquesta notació no és estàndar.*)

Igual que es va fer al Càlcul de 1r, es demostra que $SCV(k) \subset SC(k)$, és a dir, que tota successió convergent és de Cauchy. En general, però, no tota successió de Cauchy és convergent.

Exemple 3.10.1. A $k = \mathbb{Q}$, considerem la successió $a_0 = 1$, $a_{n+1} = 1 + 1/(1 + a_n)$. En els reals, aquesta successió convergeix a $\sqrt{2}$. A $\mathbb{Q}$, en canvi, no existeix $\sqrt{2}$ (comparant amb els reals, és com si hi tinguéssim un "forat"), de manera que $(a_n)_n \subset \mathbb{Q}$ és una successió de Cauchy que no convergeix.

Definició 3.10.6 (Cos complet)**.** Direm que un cos ordenat és *complet* si tota successió de Cauchy és convergent (és a dir, $SC(k) = SCV(k)$).

Segons l'exemple que hem donat abans, tenim que $\mathbb{Q}$ no és complet. Per tant, el nostre objectiu serà "completar-lo", és a dir, trobar una extensió $k/\mathbb{Q}$ que sigui completa i "minimal" (després precisarem que volem dir amb això).

Per construir la completació, ens inventarem nombres que siguin límits de les successions de Cauchy de $\mathbb{Q}$ que no tenen límit. S'ha d'anar amb compte, però, ja que hi ha successions de Cauchy que poden convergir al mateix límit. Per exemple, la successió

$$x_{n+1} = \frac{x_n^2 + 2}{2x_n}$$

també convergeix a $\sqrt{2}$ als reals, de manera que haurà de tenir el mateix límit que la successió que hem donat a l'exemple.

Per tant, no en tenim suficient amb inventar-nos un nou nombre per cada successió de Cauchy no convergent, sinó que hem d'agrupar les successions de Cauchy que s'apropen infinitament. Això ens porta a definir la relació d'equivalència següent:

$$(a_n)_n \sim (b_n)_n \iff (a_n - b_n)_n \to 0$$

Lema 3.10.2. *Aquesta expressió defineix efectivament una relació d'equivalència a $SC(k)$.*

A continuació, donem uns quants resultats tècnics que utilitzarem posteriorment.

Lema 3.10.3. *Sigui k un cos ordenat.*

1. *Sigui $(a_n)_n$ una successió de Cauchy d'elements de k, aleshores $(a_n)_n$ està fitada a k.*
2. *Siguin $(a_n)_n$ i $(b_n)_n$ dues successions de Cauchy. Aleshores, la seva suma $(a_n)_n + (b_n)_n := (a_n + b_n)_n$ i el seu producte $(a_n)_n \cdot (b_n)_n = (a_n \cdot b_n)_n$ són també successions de Cauchy.*

3. *Siguin $(a_n)_n$ i $(b_n)_n$ successions tals que $(a_n)_n \to 0$ i $(b_n)_n \to 0$. Aleshores, $(a_n)_n+(b_n)_n \to 0$ i $(a_n)_n \cdot (b_n)_n \to 0$.*

4. *Sigui $(a_n)_n \to 0$, i $(\lambda_n)_n$ una successió de Cauchy qualsevol. Aleshores, $(a_n)_n \cdot (\lambda_n)_n \to 0$.*

5. *Si $(a_n)_n$ és una successió de Cauchy i té una subsuccessió $(a_{n_k})_k \to 0$, aleshores $(a_n)_n \to 0$.*

Demostració. S'han d'adaptar les demostracions que es van veure a càlcul de 1r per al valor absolut derivat de l'ordre de k. □

Corol·lari 3.10.2. *El conjunt de successions de Cauchy de k ($SC(k)$) és un anell (commutatiu i unitari) respecte la suma i producte definits anteriorment, amb $0 = (0_k)_n$ i $1 = (1_k)_n$. El subconjunt $S_0(k)$ de les successions de Cauchy convergents a zero és un ideal de $SC(k)$, i tenim que*

$$(a_n)_n \sim (b_n)_n \iff (a_n)_n - (b_n)_n \in S_0(k)$$

Definició 3.10.7 (Completació com a cos ordenat)**.** Definim la *completació com a cos ordenat* de k com

$$\hat{k} := SC(k)/S_0(k)$$

Proposició 3.10.4.

1. *$\hat{k}$ és un cos (és a dir, $S_0(k)$ és maximal).*

2. *Existeix una immersió de k a $\hat{k}$ que envia $\alpha \in k$ a la classe de la successió constant $(\alpha)_n$*

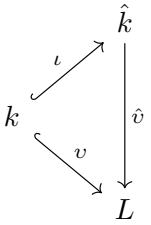
$$\begin{aligned} k &\overset{\iota}{\hookrightarrow} \hat{k} \\ \alpha &\longmapsto \iota(\alpha) = [(\alpha)_n] \end{aligned}$$

3. *$\hat{k}$ és ordenat, i el seu ordre és compatible amb l'ordre de k (segons la immersió anterior). És a dir, si $\alpha, \beta \in k$ i $\alpha <_k \beta$, aleshores $\iota(\alpha) <_{\hat{k}} \iota(\beta)$.*

4. *k és un subcos dens de $\hat{k}$ (de fet, tècnicament seria $\iota(k)$, però ho denotarem com k).*

5. *$\hat{k}$ és complet.*

6. *$\hat{k}$ és "minimal" entre tots els cosssos ordenats que satisfan (3), (4) i (5). És a dir, si $k \overset{\upsilon}{\hookrightarrow} L$ és una immersió de k en un cos ordenat i complet L que respecta l'ordre i tal que $\upsilon(k)$ és dens a L, aleshores existeix un únic morfisme de cossos $\hat{\upsilon} : \hat{k} \hookrightarrow L$ que respecta l'ordre i tal que el següent diagrama és commutatiu.*



Demostració. Només donarem les idees bàsiques de la prova. La demostració detallada es pot trobar al document penjat a Atenea.

1. Una de les coses que s'ha de veure és que tot element no nul té invers. Sigui $x = [(a_n)_n] \neq 0$. Aleshores, $(a_n)_n \not\to 0$. Per tant, $(a_n)_n$ té un nombre finit de termes nuls (ja que és de Cauchy). Canviant-los per 1, obtenim una successió equivalent que no té cap terme nul, de manera que podem invertir terme a terme.

2. Donat un $x \in k$, definim $\iota(x) = [(x)_n]$.

3. Tenim el següent resultat d'anàlisi:

   Lema 3.10.4. *Sigui $(a_n)_n \in SC(k)$. Aleshores, es satisfà exactament una de les tres condicions següents:*

   (a) $(a_n)_n \to 0$.

   (b) Existeixen un $\varepsilon \in k$, $\varepsilon > 0$ i un $n_0 \in \mathbb{N}$ tals que $a_n \geq \varepsilon$ per tot $n \geq n_0$.

   (c) Existeixen un $\varepsilon \in k$, $\varepsilon < 0$ i un $n_0 \in \mathbb{N}$ tals que $a_n \leq \varepsilon$ per tot $n \geq n_0$.

   A partir d'aquest lema, definim l'ordre en $\hat{k}$ de manera que $x = [(a_n)_n] > 0 \iff (a_n)_n$ satisfà la condició (b). Es pot comprovar que aquest ordre és compatible amb les operacions i està ben definit.

4. $\iota(k)$ és dens a $\hat{k}$ perquè tota successió de Cauchy $(\iota(a_n))_n$ tendeix a la classe d'equivalència $[(a_n)_n]$.

5. Veure document Atenea.

6. Veure document Atenea.

□

Un cop definit el concepte de completació d'un cos, podem definir els nombres reals com la completació dels racionals.

Definició 3.10.8. $\mathbb{R} := \hat{\mathbb{Q}}$.

Exemple 3.10.2.

1. $\mathbb{Q}(\sqrt{2})$ és un altre cos ordenat que té com a completació $\widehat{\mathbb{Q}(\sqrt{2})} = \mathbb{R}$.

2. El cos $\mathbb{Q}(i)$ no és ordenat, de manera que no podem definir-ne la completació com hem vist abans. Observem, però, que sí que tenim una noció de "cos complet minimal que el conté", ja que sabem que $\mathbb{Q}(i) \subset \mathbb{C}$ que és cos complet i tot cos complet que contingui $\mathbb{Q}(i)$ ha de contenir tant $\mathbb{R}$ com i (i per tant $\mathbb{C}$).

En la secció següent, veurem una manera alternativa de completar cossos que no siguin ordenats.

3.11 Cossos valorats

Definició 3.11.1 (Valoració discreta)**.** Una *valoració discreta* d'un anell íntegre A és una aplicació $v : A \setminus \{0\} \longrightarrow \mathbb{Z}$ que satisfà

1. $v(a \cdot b) = v(a) + v(b)$
2. $v(a + b) \geq \min\{v(a), v(b)\}$

per tot $a, b \in A$. Per convenció, s'acostuma a definir $v(0) := +\infty$.
Sigui $k = \mathrm{Fr}(A)$. Podem extendre v a k com

$$v\left(\frac{a}{b}\right) := v(a) - v(b)$$

Observació. Per definició, $v(1) = v(1) + v(1) \implies v(1) = 0$ i $v(-1) + v(-1) = v(1) = 0 \implies v(-1) = 0$.

Exemple 3.11.1.

1. Sigui $A = k[x]$. Podem definir la valoració $v : A \longrightarrow \mathbb{Z}$ tal que $v(p(x)) = -\deg p(x)$. Això ens defineix una valoració a $k(x)$ tal que $v(p(x)/q(x)) = \deg q(x) - \deg p(x)$.
2. Sigui $A = \mathbb{Z}$ i p un primer qualsevol. Definim la *valoració p-àdica* com l'aplicació $v_p : \mathbb{Z} \longrightarrow \mathbb{Z}$ on $v_p(n)$ és el màxim k tal que $p^k \mid n$.

   Per exemple, $v_2(40) = 3$, ja que $2^3 \mid 40$ però $2^4 \nmid 40$.
3. En analogia amb la valoració p-àdica, podem definir una altra valoració a l'anell de polinomis $A = k[x]$. Sigui $p(x)$ un polinomi irreductible. Definim la valoració

$$\begin{aligned} v_{p(x)} : k[x] &\longrightarrow \mathbb{Z} \\ m(x) &\longmapsto \max\{k : p(x)^k \mid m(x)\} \end{aligned}$$

Proposició 3.11.1. *Donada una valoració $v : A \setminus \{0\} \longrightarrow \mathbb{Z}$, tenim que*

1. $R_v = \{a \in k = \mathrm{Fr}(A) : v(a) \geq 0\}$ *és un anell.*
2. $R_v^* = \{a \in k; v(a) = 0\}$ *són les unitats de R_v.*
3. $M_v = \{a \in k : v(a) > 0\}$ *és l'únic ideal maximal de R_v.*

Demostració. Exercici. □

Observació. En aquest curs no hi entrarem, però l'anell R_v s'anomena *anell de valoració discreta*, i es pot veure que és equivalent donar una valoració en A que un anell amb les propietats anteriors.

Definició 3.11.2 (Cos residual)**.** Sigui v una valoració sobre un anell íntegre A. El cos $R(v) = R_v/M_v$ s'anomena *cos residual* de v.

Exercici. Considerem la valoració p-àdica $v_p : \mathbb{Z} \longrightarrow \mathbb{Z}$. Descriviu $\mathbb{Z}_{(p)} := \mathbb{Z}_{v_p}$ i comproveu que $R(v_p) = \mathbb{Z}/p\mathbb{Z}$.

A partir d'una valoració es pot definir un valor absolut a un cos no ordenat.

Definició 3.11.3 (Valor absolut)**.** Un valor absolut en un cos k és una aplicació

$$\begin{aligned} |\cdot| : k &\longrightarrow \mathbb{R} \\ x &\longmapsto |x| \end{aligned}$$

que satisfà

1. $|x| = 0 \iff x = 0$
2. $|x \cdot y| = |x| \cdot |y|$ per tot $x, y \in k$

A més, demanem que satisfaci una de les dues propietats següents:

3a. $|x + y| \leq |x| + |y|$ per tot $x, y \in k$

3b. $|x + y| \leq \max\{|x|, |y|\}$ per tot $x, y \in k$

Si satisfà (3a), diem que $|\cdot|$ és un *valor absolut arquimedià*, mentre que si satisfà (3b) diem que és un *valor absolut ultramètric*.

A la tupla $(k, |\cdot|)$ d'un cos i un valor absolut l'anomenem *cos valorat*.

Exemple 3.11.2.

1. $\mathbb{R}$ amb el $|\cdot|$ habitual.
2. $\mathbb{C}$ amb el $|\cdot|$ habitual.
3. $\mathbb{Q}(i)$ amb $|a + bi| := \sqrt{a^2 + b^2}$
4. Si $v : A \longrightarrow \mathbb{Z}$ és una valoració i $k = \mathrm{Fr}(A)$, triem un $\rho \in (0, 1) \subset \mathbb{R}$ qualsevol i tenim que l'aplicació

$$\begin{aligned} |\cdot|_v : k &\longrightarrow \mathbb{R} \\ |x|_v &\longmapsto \rho^{v(x)} \end{aligned}$$

és un valor absolut.

Exercici. Proveu que els exemples anteriors són efectivament valors absoluts.

Observació. Podem expressar el valor absolut habitual de $\mathbb{R}$ com $|x| = (1/e)^{-|x|}$. Veiem aleshores que l'aplicació $-\log|\cdot| : \mathbb{R}^* \longrightarrow \mathbb{R}$ és una mena de pseudo-valoració.

Un valor absolut en un cos k ens permet definir una mètrica. A partir d'aquesta mètrica, podem definir una topologia donada per la base d'oberts

$$\{B(a, r) : a \in k,\, r \in \mathbb{R},\, r > 0\}$$

on $B(a, r) := \{b \in k : |b - a| < r\}$ és una bola oberta de centre a i radi r.

Observació. Si $|\cdot|$ prové d'una valoració v (és a dir, $|x| = \rho^{v(x)}$ per un cert $\rho \in (0,1)$), aleshores la topologia definida per $|\cdot|$ és la mateixa per a tot ρ. És per això que sovint es diu que aquests valors absoluts són *valors absoluts equivalents.*

A partir d'aquesta topologia, podem definir els conceptes de successions de Cauchy, convergència i completesa, utilitzant ara el valor absolut de la mètrica en lloc del valor absolut derivat de l'ordre.

Observem que aquest valor absolut ens porta a $\mathbb{R}$, de manera que podem prendre els ε's a $\mathbb{R}$ en lloc de a k.

Definició 3.11.4 (Cos complet)**.** Un cos valorat $(k, |\cdot|)$ és *complet* si totes les successions de Cauchy en k són convergents.

Proposició 3.11.2 (Teorema)**.** *Per a tot cos valorat $(k, |\cdot|_k)$, existeix un cos valorat complet $(\hat{k}, |\cdot|_{\hat{k}})$ i una immersió $\iota : k \hookrightarrow \hat{k}$ tal que $|\iota(x)|_{\hat{k}} = |x|_k$ per a tot $x \in k$ i tal que, a més, $\hat{k}$ és minimal respecte aquesta propietat.*

Demostració. Es pot fer copiant la construcció que vam fer per a cossos ordenats. Aleshores,

$$\hat{k} = \{\text{successions de Cauchy}\}/\{\text{successions} \to 0\}$$

□

Exemple 3.11.3.

1. Recordem que la valoració p-àdica era una aplicació $v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ tal que $v_p(a/b) = v_p(a) - v_p(b)$ i $v_p(a) = \max k$ tal que $p^k \mid a$. A partir d'aquesta valoració, definim el valor absolut p-àdic:

$$|x|_p := \left(\frac{1}{p}\right)^{v(x)}$$

   Es pot veure que, si $p \neq q$, aleshores $|\cdot|_p$ i $|\cdot|_q$ donen topologies diferents.

   Definició 3.11.5 (Cos dels nombres p-àdic)**.** El cos dels nombres p-àdics $(\mathbb{Q}_p)$ és el completat de $\mathbb{Q}$ respecte el valor absolut p-àdic:

$$\mathbb{Q}_p = (\widehat{\mathbb{Q}, |\cdot|_p})$$

   Per tant, per a cada primer p tenim una manera diferent de completar $\mathbb{Q}$, que ens dona cadascuna una topologia diferent. A $\mathbb{Q}_p$ moltes de les intuicions que teníem als reals ja no són vàlides. Per exemple, $|p^r|_p \to 0$ mentre que $|p^{-r}|_p \to \infty$ quan $r \to \infty$.

   Aleshores, de la mateixa manera que podem escriure un nombre real com una suma de potències de 10 (la seva expressió decimal), amb un nombre finit de dígits amb exponent positiu i un nombre (potencialment) infinit de dígits amb exponent negatiu, es poden escriure els nombres p-àdics com una suma de potències de p amb un nombre finit de dígits amb exponent negatiu i un nombre (potencialment) infinit de dígits amb exponent positiu.

Observem que això no comporta cap problema de convergència, ja que a $\mathbb{Q}_p$ tenim que $|p^r| \to 0$.

Els nombres p-àdics també tenen altres peculiaritats. Per exemple, a $\mathbb{Q}_7$ podem escriure $\sqrt{2}$ com $3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \ldots$, seguint la recurrència $x_1 = 3$ i $x_n = x_{n-1}^2 + x_{n-1} - 2 \mod 7^k$. Aquesta successió surt d'aplicar el mètode de Newton (adaptat a $\mathbb{Q}_7$) al polinomi $x^2 - 2$.

Els nombres p-àdics no només són una curiositat matemàtica, sinó que tenen múltiples aplicacions en la teoria de nombres i en la geometria algebraica, on són essencials per a estudiar corbes amb equacions enteres.

Proposició 3.11.3 (Teorema de Ostrowski)**.** *Tot valor absolut en $\mathbb{Q}$ és equivalent (és a dir, dóna lloc a la mateixa topologia) al valor absolut habitual o a un valor absolut p-àdic per un cert p.*

Equivalentment, les úniques completacions de $\mathbb{Q}$ són $\mathbb{R}$ i els $\mathbb{Q}_p$.

2. Sigui k un cos qualsevol. Hem vist que $-\deg$ defineix una valoració a $k[x]$ (i per tant a $k(x)$). La completació de $k(x)$ respecte a aquest valor absolut dona el cos de sèries de Laurent $k[\{x\}]$ (sèries de potències amb un nombre finit de termes d'exponent negatiu). Per altra banda, completant l'anell $k[x]$, obtenim l'anell de sèries de potències $k[[x]]$.

3.12 Equació general de grau n

Definició 3.12.1 (Polinomi general de grau n)**.** Sigui k un cos qualsevol, i siguin $a_n, x_1, \ldots, x_n, T$ variables indeterminades. Definim el *polinomi general de grau n sobre k* com

$$f(T) = a_n(T - x_1) \cdots (T - x_n) \in k(a_n, x_1, \ldots, x_n)[T]$$

Desenvolupant, tenim que

$$f(T) = a_n T^n + a_{n-1}(x_1, \ldots, x_n)T^{n-1} + \cdots + a_0(x_1, \ldots, x_n)$$

on $a_k(x_1, \ldots, x_n)$ són coeficients que depenen de les arrels $x_1, \ldots, x_n$.
Substituint $T = 0$, tenim que $a_0 = (-1)^n a_n x_1 \cdots x_n$. Similarment, calculant $f'(0)$, tenim que

$$a_1 = (-1)^{n-1} a_n \sum_{i=1}^{n} \prod_{j \neq i} x_j$$

En general, tenim que

$$a_k = (-1)^{n-k} a_n \sum_{\#I = n-k} \prod_{i \in I} x_i$$

Definició 3.12.2 (k-èssim polinomi simètric elemental)**.** A partir de la fórmula anterior, definim el *k-èssim polinomi simètric elemental* com

$$S_k(x_1, \ldots, x_n) = \sum_{\#I = n-k} \prod_{i \in I} x_i$$

Diem que aquest polinomi és simètric perquè observem que no depèn de l'ordre de les x_i.

Tenim dos teoremes importants referents als polinomis simètrics elementals:

Proposició 3.12.1 (Teorema)**.** *Tot polinomi simètric en $x_1, \ldots, x_n$ es pot escriure com un polinomi que pren com a variables els polinomis simètrics elementals.*

Equivalentment, tot polinomi simètric en les arrels d'un polinomi es pot escriure com a polinomi en els coeficients dels polinomi.

Exemple 3.12.1. Per exemple, el discriminant d'un polinomi de segon grau no s'acostuma a definir amb la fórmula típica de $b^2 - 4ac$, sinó que es defineix com el quadrat de la diferència de les dues arrels del polinomi. Observem que, segons aquesta definició, el discriminant és un polinomi simètric en les arrels del polinomi, de manera que el teorema anterior ens garanteix que existeix una manera d'expressar el discriminant a partir dels coeficients del polinomi (que és la que ens dona la fórmula típica).

Proposició 3.12.2 (Teorema)**.** *Sigui $M = k(a_n, x_1, \ldots, x_n)$, i considerem-ne el subcos $L = k(a_0, a_1, \ldots, a_n) = k(a_n, s_0(x_1, \ldots, x_n), \ldots, s_{n-1}(x_1, \ldots, x_n))$. Aleshores, M/L és una extensió algebraica de grau $n!$.*

Observació. Aquest teorema pot no semblar gaire rellevant, però és clau per estudiar les propietats dels polinomis. De fet, la no existència de fórmules generals per l'equació de grau 5 prové de l'estudi d'aquesta extensió per $n = 5$.

3.13 Construccions geomètriques

3.13.1 Construccions amb regle i compàs

En aquesta seccció veurem quines longituds es poden construir amb regle i compàs. Abans, però, definirem que entenem per aquests instruments.

Definició 3.13.1 (Regle)**.** Instrument sense marques que ens permet dibuixar rectes arbitràriament llargues a partir de dos punts.

Definició 3.13.2 (Compàs)**.** Instrument que permet dibuixar una circumferència a partir del seu centre i un punt. Assumim que no el podem fer servir per transportar distàncies.

El punt de partida seran dos punts a distància 1, que denotarem com 0 i 1 i que assumirem que estan situats a l'eix d'abscisses.

Volem veure si partint d'aquests dos punts podem construir dos punts P i Q que es trobin a una certa distància $d \in \mathbb{R}$. Igualment, també podem construir nombres complexos, identificant-los com un punt de $\mathbb{R}^2$.

En primer lloc, intersecant una circumferència amb centre 1 i que passa per 0 amb l'eix d'abscisses, obtenim el punt 2. Per inducció, podem repetir aquest procediment per les dues bandes fins a obtenir tot $n \in \mathbb{Z}$. Fent la mediatriu de -1 i 1, obtenim l'eix d'ordenades, i procedint de la mateixa manera que abans obtenim ni per tot $n \in \mathbb{Z}$.

Es pot veure que, donades dues distàncies qualsevols, podem construir-ne la seva suma. També podem construir l'arrel quadrada de qualsevol distància que ja tinguem, amb l'algorisme següent:

Construcció de $\sqrt{d}$ a partir de d:

1. Traslladem la distància a l'eix horitzontal a partir del punt 1, obtenint el punt $d+1$.

2. Dibuixem la mediatriu d'aquest segment.

3. Dibuixem la circumferència que passa per 0 i té centre a $(d+1)/2$.

4. Dibuixem la recta vertical que passa per 1 (recordem que abans ja hem trobat 0 i 2, així que podem fer-ne la mediatriu). La intersecció d'aquesta recta amb la circumferència anterior estarà a distància $\sqrt{d}$ del punt 1.

Per provar que aquesta distància és $\sqrt{d}$, utilitzem el teorema de l'altura. Sigui P la intersecció entre la recta vertical que passa per 1 i la circumferència. Sigui $h = d(1, P)$. Aleshores, els triangles $01P$ i $P1d$ són semblants, de manera que

$$\frac{h}{1} = \frac{d+1-1}{h} \implies h^2 = d \implies h = \sqrt{d}$$

Hem vist que podem sumar distàncies i fer arrels quadrades. A partir del teorema de Tales, es pot veure que podem multiplicar i dividir distàncies. Per tant, el conjunt de distàncies construïbles acaba sent un cos, on tenim les arrels quadrades de qualsevol element del cos.

Proposició 3.13.1 (Teorema)**.** *Un cert $\alpha \in \mathbb{C}$ és constructible amb regle i compàs si, i només si, existeix una torre d'extensions quadràtiques*

$$\mathbb{Q} \overset{2}{\subset} \mathbb{Q}(\alpha_1) \overset{2}{\subset} \ldots \overset{2}{\subset} \mathbb{Q}(\alpha_r) \overset{2}{\subset} \mathbb{Q}(\alpha)$$

Exemple 3.13.1. Aquest teorema ens garantitza que no es pot construir $\sqrt[3]{2}$ amb regle i compàs, ja que $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$. Això implica que no es pot construir amb regla i compàs un cub de volum 2.

Igualment es pot demostrar que per a un α general, no podem trisecar α, ja que en general $[\mathbb{Q}(\cos\alpha) : \mathbb{Q}(\cos 3\alpha)] = 3$.

Una altra conseqüència important d'aquest teorema és que ens caracteritza els polígons regulars que podem construir amb regla i compàs:

Corol·lari 3.13.1. *Un polígon regular de n costats es pot construir amb regle i compàs si, i només si, $n = 2^k p_1 \cdots p^r$, on $k \geq 0$ i p_i són primers de Fermat ($p_i = 2^{2^{k_i}} + 1$)*

Observació. Construir un polígon de n costats equival a construir el seus dos primers vèrtexs, de manera que equival a construir $\zeta = e^{2\pi i/n}$.

3.13.2 Construccions amb origami

Suposem que tenim un full de paper arbitràriament gran. Suposem que tenim un punt marcat a distància 1 d'una cantonada. Anomenarem a aquest punt 1, i a la cantonada del seu costat 0.

El nostre objectiu és construir una certa distància d mitjançant plecs de paper. Per exemple, amb un plec de paper podem dibuixar la mediatriu d'un segment o la bisectriu d'un angle. Obtindrem nous punts intersecant les rectes de dos plecs diferents.

Per exemple, per construir $\sqrt{2}$, pleguem el full paralelament al costat vertical, de manera que el 1 quedi a la cantonada, i tot seguit el despleguem i fem la bisectriu de l'angle amb extrem al 0. La intersecció d'aquests dos plecs es correspondrà al punt $(1, 1)$, que es troba a distància $\sqrt{2}$ del 0.

Es pot provar que el conjunt de distàncies construïbles amb origami també és un cos, però un cos molt més extens que el de les distàncies construïbles amb regle i compàs.

Construcció d'una paràbola:

1. Triem un punt qualsevol del paper, que serà el vèrtex de la paràbola.
2. Escollim un dels costats del paper, que serà l'eix de la paràbola.
3. Dobleguem una de les cantonades d'aquest costat del paper de manera que la vora del paper quedi sobre el punt que havíem triat.
4. Repetim el pas anterior unes quantes vegades, fent coincidir el vèrtex de la paràbola amb punts diferents de la vora del paper.
5. Dibuixem l'envolvent de les rectes anteriors, que serà una paràbola. (L'envolvent és la corba tangent a totes les rectes.)

A diferència de amb regle i compàs, amb origami sí que es pot trisecar un angle qualsevol.

Trisecció d'un angle:

1. Tenim una semirecta que surt de la cantonada inferior esquerra del paper, i que forma l'angle que volem trisecar amb el costat inferior del paper.
2. Fem un plec horitzontal a una altura qualsevol.
3. Dobleguem el paper de manera que l'extrem inferior quedi sobre el plec del pas anterior (és a dir, dibuixant la mediatriu entre aquest i el límit inferior del paper).
4. Dobleguem la cantonada inferior esquerra de manera que l'extrem del plec del pas 2 quedi a sobre de la semirecta que defineix l'angle, i que la cantonada inferior esquerra del paper quedi a sobre del plec del pas 3.
5. Sigui P el punt d'intersecció entre el plec del pas anterior i el plec del pas 3. Dobleguem el costat inferior del paper de manera que la cantonada inferior esquerra quedi fixa i el costat inferior del paper quedi a sobre del punt P. El plec que haurem creat forma un angle que és un terç de l'original.

Proposició 3.13.2 (Teorema)**.** *Un cert $\alpha \in \mathbb{C}$ és constructible amb origami si, i només si, existeix una torre d'extensions quadràtiques o cúbiques*

$$\mathbb{Q} \overset{2,3}{\subset} \mathbb{Q}(\alpha_1) \overset{2,3}{\subset} \ldots \overset{2,3}{\subset} \mathbb{Q}(\alpha_r) \overset{2,3}{\subset} \mathbb{Q}(\alpha)$$

Corol·lari 3.13.2. *Un polígon regular de n costats es pot construir amb origami si, i només si, $n = 2^r 3^s p_1 \cdots p_l$, on $r, s \geq 0$ i p_i són primers de la forma $p = 2^a 3^b + 1$.*

4
Grups

4.1 Definició i propietats bàsiques

Definició 4.1.1 (Grup)**.** Un *grup* és un conjunt G amb una operació

$$\begin{aligned} G \times G &\longrightarrow G \\ a, b &\longmapsto a \cdot b \end{aligned}$$

que satisfà les condicions següents:

1. Té element neutre, és a dir, existeix un $e \in G$ tal que $x \cdot e = e \cdot x = x$ per tot $x \in G$.
2. És associativa, és a dir, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per tot $a, b, c \in G$.
3. Tot element té invers, és a dir, per tot $a \in G$ existeix un cert $\tilde{a} \in G$ tal que $a \cdot \tilde{a} = \tilde{a} \cdot a = e$.

Direm que el grup és *abelià* si, a més, l'operació satisfà la propietat commutativa.

Direm que el grup és *finit* si té un nombre finit d'elements. En aquest cas, anomenarem *ordre del grup* ($|G|$) al seu cardinal. Altrament, direm que el grup és *infinit*.

Proposició 4.1.1.

1. *L'element neutre és únic.*
2. *Cada element té un únic invers.*
3. *Per veure que un element és neutre o que és invers d'un altre, només fa falta veure que ho és per l'esquerra o per la dreta.*

Demostració.

1. Suposem que tant e com e' són elements neutres d'un grup G, aleshores $e' = e \cdot e' = e$.
2. Suposem que per un cert $a \in G$, tenim que $\tilde{a} \cdot a = e$ i $a \cdot \hat{a} = e$. Aleshores,

$$\tilde{a} = \tilde{a} \cdot e = \tilde{a} \cdot (a \cdot \hat{a}) = (\tilde{a} \cdot a) \cdot \hat{a} = e \cdot \hat{a} = \hat{a}$$

   de manera que $\tilde{a} = \hat{a}$.
3. Exercici.

□

Definició 4.1.2 (Potència d'un element)**.** Sigui $a \in G$ un element d'un grup. Per tot $n \geq 1$ enter, definim la seva potència n-èssima com

$$a^n := \underbrace{a \cdots a}_{n \text{ vegades}}$$

Igualment, definim $a^0 = e$ i, per $n \geq 1$ definim $a^{-n} := (\tilde{a})^n$, on $\tilde{a}$ és l'invers de a.

Proposició 4.1.2. *A partir de les definicions anteriors tenim que, de manera natural,* $a^{m+n} = a^m a^n$ *per tot* $m, n \in \mathbb{Z}$.

En general, per treballar amb grups utilitzarem la notació multiplicativa (denotant la operació com un producte), però en els grups abelians s'acostuma a utilitzar la notació additiva (denotant la operació com una suma).
En aquest cas, a^n s'escriu com na i l'invers a^{-1} s'escriu com $-a$.

Exemple 4.1.1.

1. El grup més fàcil no trivial (és a dir, amb més d'un element) és el grup de dos elements $G = \{0, 1\}$ amb l'operació donada per la següent taula:

$\cdot$	0	1
0	0	1
1	1	0

2. $G = \mathbb{Z}/n\mathbb{Z}$ amb l'operació suma mòdul n és un grup abelià.
3. $G = \mathbb{Z}$ també és un grup abelià amb la suma.
4. El conjunt d'arrels n-èssimes de la unitat $G = \{\zeta \in \mathbb{C} : \zeta^n = 1\}$ és un grup finit i abelià amb l'operació producte.
5. Un altre exemple de grup és el grup simètric d'ordre n ($\mathfrak{S}_n$), que es correspon al conjunt de permutacions de n elements. Els grups simètrics són molt importants, perquè veurem més tard que tot grup finit es pot expressar com un subgrup d'un cert grup simètric.
6. $G = \{$moviments del pla que deixen fix un quadrat$\}$ és un grup amb l'operació composició. Els elements del grup són les simetries respecte les diagonals, les simetries respecte les mediatrius de cada costat i les rotacions d'angle $k\pi/2$ respecte el centre del quadrat.

7. Fixat V un k-espai vectorial, el conjunt d'automorfismes a V ($\mathrm{Aut}(V)$) és un grup amb la composició.

   En general, una bona manera de caracteritzar un grup és representant els seus elements com a matrius, és a dir, construir un morfisme de G a $\mathrm{Aut}(V)$ per a un cert espai vectorial V.

   Trobar aquest morfisme no és immediat, i a més s'ha de tenir en compte que les característiques del grup imposen certes condicions sobre l'espai vectorial V. Tot això s'estudia amb més detall a la *teoria de representació de grups*.

8. Donat un cos k, el conjunt de matrius invertibles $G = G\ell_n(k)$ forma un grup amb el producte. Observem que aquest grup està relacionat amb el grup d'automorfismes que hem donat abans, tot i que no són isomorfs.

9. Si G i H són dos grups, el seu producte cartesià $G \times H$ també ho serà, fent les operacions coordenada a coordenada:

$$\begin{aligned}(G \times H) \times (G \times H) &\longrightarrow (G \times H)\\ (a, b), (a', b') &\longmapsto (a \cdot_G a', b \cdot_H b')\end{aligned}$$

   Així, per exemple, es pot construir el grup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, que es pot veure que "coincideix" amb $\mathbb{Z}/6\mathbb{Z}$ (després ho formalitzarem). En canvi, veurem també que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ no té res a veure amb $\mathbb{Z}/4\mathbb{Z}$.

Definició 4.1.3 (Subgrup)**.** Un *subgrup* d'un grup G és un subconjunt $H \subset G$ tal que

1. $e \in H$
2. Per tot $x, y \in H$, tenim que $xy^{-1} \in H$.

En particular, es pot veure que això equival a dir que $x \in H \implies x^{-1} \in H$ i $x, y \in H \implies xy \in H$. Per tant, la operació de G restringida a H li dona estructura de grup.

Exemple 4.1.2.

1. Sigui $G = \mathbb{Z}/12\mathbb{Z}$. Aleshores $H = \{0, 2, 4, 6, 8, 10\}$, $H = \{0, 3, 6, 9\}$, $H = \{0, 4, 8\}$ i $\{0, 6\}$ són subgrups de G. A més, es pot veure que aquests són tots els subgrups propis no trivials de G.
2. Sigui $G = \mathfrak{S}_3$. Aleshores tenim els subgrups $H = \{\mathrm{Id}, (1, 2)\}$ i $H = \{\mathrm{Id}, (1, 2, 3), (1, 3, 2)\}$.

Definició 4.1.4 (Subgrup generat)**.** Sigui $S \subset G$ un subconjunt d'un grup. Anomenem *subgrup generat per* S al menor subgrup de G que conté S. Ho denotarem per $\langle S \rangle$ o per $(s_1, \ldots, s_n)$ (suposant que S és finit i $S = \{s_1, \ldots, s_n\}$).

Exemple 4.1.3. A l'exemple anterior de $G = \mathbb{Z}/12\mathbb{Z}$, tenim que $\langle 2, 3 \rangle = G$. En canvi, $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$.

Definició 4.1.5 (Grup cíclic)**.** Direm que un grup G és cíclic si existeix un $a \in G$ tal que $G = \langle a \rangle$. (És a dir, existeix un element que genera tot el grup.)

Proposició 4.1.3. *Siguin H i K subgrups de G. Aleshores, $H \cap K$ també és un subgrup de G.*

4.2 Classes laterals

Volem construir una noció de "quocient" amb grups. El problema que tenim respecte a quan treballàvem amb altres estructures és que en els grups no assumim la commutativitat, de manera que haurem de definir les classes d'equivalència tant per la dreta com per l'esquerra.

Sigui G un grup, i sigui H un subgrup de G. Definim les següents relacions a G:

$$a \sim_E b \iff \exists\, h \in H \text{ tal que } b = ah$$
$$a \sim_D b \iff \exists\, h \in H \text{ tal que } b = ha$$

És fàcil veure que són relacions d'equivalència:

- Reflexiva: H subgrup $\implies e \in H \implies a \sim a$.
- Simètrica: $b = ah \iff a = bh^{-1}$ i tenim que els inversos estan a H perquè H és un subgrup.
- Transitiva: (exercici).

Definició 4.2.1 (Classes laterals)**.** Denotarem la classe d'equivalència de a per $\sim_E$ com aH i la classe de a per $\sim_D$ com Ha.

Observem que aquesta notació té sentit, ja que

$$aH := \{b \in G : b \sim_E a\} = \{ah : h \in H\}$$
$$Ha := \{b \in G : b \sim_D a\} = \{ha : h \in H\}$$

Definim $G \setminus H$ com el conjunt de classes laterals per l'esquerra d'elements de G i H/G com el conjunt de classes laterals per la dreta d'elements de G.

Exemple 4.2.1. Sigui $G = \mathfrak{S}_3$. Considerem $H = \langle (1,2,3) \rangle = \{\mathrm{Id}, (1,2,3), (1,3,2)\}$. Aleshores, la classe lateral per l'esquerra de $(1,2) \in G$ és

$$(1,2)H = \{(1,2), (2,3), (1,3)\}$$

Observem que les classes laterals no tenen perquè ser un subgrup. En aquest cas, en particular, és fàcil veure que no ho és perquè no conté la identitat.

Observem també que, per definició de classe d'equivalència, tenim que $aH = bH \iff a \sim_E b$ i que són disjuntes en cas contrari. Per tant, $(1,2)H = (2,3)H = (1,3)H$, però aquestes classes són disjuntes amb σH per tot $\sigma \in \mathfrak{S}_3$, $\sigma \notin H$.

En el cas de $\mathfrak{S}_3$, tenim dues classes laterals per l'esquerra, i cada una té 3 elements. Si fem les classes per la dreta, aquestes coincideixen amb les classes per l'esquerra, però això no passa en general.

Per exemple, si considerem $H = \langle (1,2) \rangle = \{\mathrm{Id}, (1,2)\}$, tenim que $(1,3)H = \{(1,3), (1,2,3)\} \neq H(1,3) = \{(1,3), (1,3,2)\}$.

En aquest cas tenim que hi ha 3 classes laterals per l'esquerra, cada una amb 2 elements. Les classes per la dreta són diferents, però també n'hi ha 3 amb 2 elements cadascuna.

En general, per tot $a \in G$ tenim les bijeccions

$$\begin{array}{ccc} H \longrightarrow aH & & H \longrightarrow Ha \\ h \longmapsto ah & & h \longmapsto ha \end{array}$$

Tenim que són bijeccions perquè si $ah = ah'$, aleshores $a^{-1}ah = a^{-1}ah' \implies h = h'$ i similarment per la dreta.

Definició 4.2.2 (Índex d'un subgrup)**.** Denotem per $[G : H]$ el nombre de classes laterals de G/H, que s'anomena *índex de H en G.*

Observació. A la definició anterior no fem distinció entre classes per la dreta i per l'esquerra degut al teorema següent.

Proposició 4.2.1 (Teorema de Lagrange)**.** *Si G és un grup finit i $H \subset G$ un subgrup, aleshores*

$$[G : H] = \frac{|G|}{|H|}$$

En particular, tenim que $[G : H]$ no depèn de si prenem classes per la dreta o per l'esquerra.

Demostració. Per les bijeccions que hem donat abans, tenim que $\#aH = \#Ha = \#H$ per tot $a \in G$. Sabem que les classes laterals particionen G en subconjunts disjunts. Per tant, tenim que G es divideix en $[G : H]$ subconjunts disjunts de $\#H$ elements cadascun. Per tant,

$$\#G = [G : H] \cdot \#H$$

□

Volem definir el concepte de "grup quocient". Per a això, necessitem donar una operació entre classes d'equivalència. L'operació més senzilla seria

$$aH \cdot bH := (ab)H$$

però hem de veure que està ben definida (és a dir, que el resultat no depengui de la tria de representants).

Suposem que $aH = a'H$ i $bH = b'H$. Aleshores, existeixen uns $h_1, h_2 \in H$ tals que $a' = ah_1$ i $b' = bh_2$. Volem veure que $a'b' \in abH$, de manera que hem de trobar un $h_3 \in H$ tal que $ah_1bh_2 = abh_3$.

Tenim que $ah_1bh_2 = abh_3 \iff h_1b = bh_3h_2^{-1} \iff b^{-1}h_1b = h_3h_2^{-1}$. Per tant, tenim que l'operació anterior entre classes d'equivalència estarà ben definida si per a tot $b \in G$ i per a tot $h_1 \in H$, tenim que $b^{-1}h_1b \in H$. (ja que llavors podriem trobar un h_3 segons la fórmula anterior). Això en general, no es donarà, ja que el grup no té perquè ser commutatiu.

Per tant, la operació anterior no és una definició vàlida en general. Als subgrups en els quals funcioni, els anomenarem *subgrups normals.*

Definició 4.2.3. Un subgrup $H \subset G$ s'anomena *normal* si per tot $b \in G$, $bH = Hb$. Equivalentment, tindrem que H és normal si $bHb^{-1} = H$ per tot $b \in G$.

En cas que H sigui un subgrup normal de G, escriurem $H \lhd G$.

Exemple 4.2.2. Sigui $G = \mathfrak{S}_3$. Aleshores, tal com hem vist abans, $H = \langle (1,2,3) \rangle \lhd G$, però $H = \langle (1,2) \rangle \not\lhd G$.

Observació. Observem que tot subgrup és normal en un grup abelià, ja que $bHb^{-1} = bb^{-1}H = H$.

Proposició 4.2.2. *Si $H \lhd G$, el conjunt G/H de classes laterals mòdul H té estructura de grup amb l'operació*

$$(aH) \cdot (bH) := (ab)H$$

Demostració. En primer lloc veiem que l'operació està ben definida. Hem de refer l'argument anterior. Sigui $a' = ah_1$ i $b' = bh_2$. Hem de veure que $a'b' = ah_1bh_2 = abh$ per un cert $h \in H$. Donat que H és normal, tenim que $h_1b \in Hb = bH \implies$ existeix un $h_3 \in H$ tal que $h_1b = bh_3$. Aleshores, prenem $h = h_3h_2$ i tindrem

$$abh = abh_3h_2 = ah_1bh_2 = a'b' \implies abH = a'b'H$$

Com a element neutre prenem $eH = H$, i tota classe aH tindrà com a invers $a^{-1}H$. L'associativitat es pot veure que segueix de l'associativitat en G. □

Exemple 4.2.3. Sigui $G = \mathfrak{S}_3$ i $H = \langle (1,2,3) \rangle$. Aleshores, hi ha $[G : H] = 6/3 = 2$ classes laterals:

$$G/H = \{(1,2)H, H\}$$

Definició 4.2.4 (Grup quocient)**.** Si $H \lhd G$, anomenem *grup quocient de G mòdul H* al conjunt de classes laterals G/H amb l'operació anterior.

4.3 Ordre d'un element

Definició 4.3.1 (Ordre d'un element)**.** Sigui G un grup. Diem que un $a \in G$ té *ordre infinit* si $a^n \neq e$ per tot $n \in \mathbb{Z}$, $n \geq 1$. Altrament, diem que a és un *element de torsió*, i definim *l'ordre de a* com el menor $n \in \mathbb{Z}$, $n \geq 1$, tal que $a^n = e$.

Equivalentment, tenim que $\text{ord}(a) = \#\langle a \rangle = \#\{a^k : k \in \mathbb{Z}\}$.

Proposició 4.3.1. *Sigui $a \in G$ un element de torsió. Aleshores,*

1. $a^m = e \iff \text{ord}(a) \mid m$.
2. $a^m = a^n \iff m \equiv n \mod \text{ord}(a)$.
3. $t \mid \text{ord}(a) \implies \text{ord}(a^t) = \text{ord}(a)/t$.
4. $\text{ord}(a^{-1}) = \text{ord}(a)$.
5. *Per tot $x \in G$,* $\text{ord}(xax^{-1}) = \text{ord}(a)$.

Demostració. Exercici. □

Corol·lari 4.3.1. *Si G és finit, per a tot $a \in G$ tenim que $a^{|G|} = e$, i aleshores tenim també que* $\text{ord}(a) \mid |G|$.

Demostració. Aquest corol·lari és el "culpable" de que haguem hagut d'estudiar abans el concepte de classes laterals, ja que utilitzarem el teorema de Lagrange per demostrar-lo.

Si G és finit, pel teorema de Lagrange $|G| = |\langle a \rangle|\,[G : \langle a \rangle]$. Per tant, $\text{ord}(a) = |\langle a \rangle| \mid G$. Aleshores, per la propietat (a), $a^{|G|} = e$. □

Corol·lari 4.3.2. *Si $|G| = p$ és primer, aleshores G és cíclic (és a dir, existeix un $a \in G$ tal que $\langle a \rangle = G$).*

Demostració. Sigui $a \in G$, amb $a \neq e$. Aleshores, $\{e, a\} \subseteq \langle a \rangle \implies |\langle a \rangle| = \text{ord}(a) \geq 2$. Pel corol·lari anterior, $\text{ord}(a) \mid |G| = p$, de manera que $\text{ord}(a) = p$ i $\langle a \rangle = G$. □

4.4 Morfismes

Definició 4.4.1 (Morfisme de grups)**.** Diem que una aplicació $f : G \longrightarrow H$ entre dos grups G i H és un *morfisme de grups* si $f(x \cdot y) = f(x) \cdot f(y)$ per tot $x, y \in G$.

És a dir, una aplicació entre grups és un morfisme de grups si respecta l'operació del grup.

A partir de la definició, tenim que els morfismes de grups tenen les següents propietats:

Proposició 4.4.1.

1. $f(e_G) = e_H$.
2. $f(x^{-1}) = f(x)^{-1}$.
3. $f(x^n) = f(x)^n$ *per tot* $n \in \mathbb{Z}$.

Demostració.

1. Sigui $u = f(e_G)$. Aleshores $u^2 = f(e_G)^2 = f(e_G^2) = f(e_G) = u$. Multiplicant per l'invers de u, tenim que $u^2 = u \implies u = e_H$.
2. $f(x)f(x^{-1}) = f(x \cdot x^{-1}) = f(e_G) = e_H$. Aleshores, donat que l'element invers és únic, tenim que $f(x^{-1}) = f(x)^{-1}$.
3. Si $n \geq 0$, apliquem inducció. Altrament, apliquem el cas de $n \geq 0$ a x^{-1}.

□

Exemple 4.4.1.

1. Sigui $G = \langle g \rangle = \{g^k\}_{k \in \mathbb{Z}}$ un grup cíclic infinit. Podem construir el morfisme de G a $\mathbb{Z}$ (entès com a grup additiu) donat per

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z} \\ g^k &\longmapsto \varphi(g^k) := k \end{aligned}$$

Està clar que φ és un morfisme, ja que $\varphi(g^k g^j) = \varphi(g^{k+j}) = k + j = \varphi(g^k) + \varphi(g^j)$

2. Un altre exemple de morfisme de grups és l'aplicació

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ k &\longmapsto \pi(k) := k \mod m \end{aligned}$$

Ja havíem vist que π és un morfisme d'anells, de manera que en particular és un morfisme de grups (restringint-nos al grup additiu de $\mathbb{Z}$).

3. Un exemple més elaborat és

$$\begin{aligned} (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^*, \cdot) \\ x &\longmapsto e^x \end{aligned}$$

4. Semblant a l'anterior, tenim també

$$\begin{aligned} (\mathbb{R}^*_{>0}, \cdot) &\longrightarrow (\mathbb{R}, +) \\ x &\longmapsto \log x \end{aligned}$$

5. Si H és un subgrup de G, aleshores la inclusió $H \hookrightarrow G$ és un morfisme.

6. Donat un cos k qualsevol, tenim el morfisme

$$\begin{aligned} G\ell_n(k) &\longrightarrow k^* \\ A &\longmapsto \det A \end{aligned}$$

Observem que el que ens està dient aquest morfisme és que el determinant del producte de matrius invertibles és el producte de determinants.

Els morfismes de grups preserven els subgrups:

Proposició 4.4.2. *Sigui $f : G \longrightarrow H$ un morfisme de grups. Aleshores,*

1. *Si $K \subset G$ és un subgrup, $f(K) \subset H$ és un subgrup.*
2. *Si $M \subset H$ és un subgrup, $f^{-1}(M) \subset G$ és un subgrup.*

Demostració.

1. Siguin $x, y \in f(K)$. Aleshores, existeixen $a, b \in K$ tals que $f(a) = x$ i $f(b) = y$. Per tant, $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(K)$. A més, $e_G \in K \implies e_H = f(e_G) \in f(K)$. Per tant, $f(K)$ és un subgrup de H.
2. Exercici.

□

Això ens porta a la següent definició:

Definició 4.4.2 (Nucli i imatge d'un morfisme)**.** Sigui $f : G \longrightarrow H$ un morfisme de grups. Definim el *nucli de* f com $\ker f := f^{-1}(e_H)$, que per la proposició anterior és un subgrup de G.

Igualment, definim la *imatge de* f com $\operatorname{Im} f := f(G)$, que per la proposició anterior és un subgrup de H.

Definició 4.4.3 (Monomorfisme, epimorfisme, isomorfisme)**.** Un morfisme de grups $f : G \longrightarrow H$ és un *monomorfisme* si f és injectiva, un *epimorfisme* si f és exhaustiva, i un *isomorfisme* si f és bijectiva.

Proposició 4.4.3. *Sigui f un morfisme de grups.*

1. *f és un monomorfisme $\iff \ker f = \{e_G\}$.*
2. *f és un epimorfisme $\iff \operatorname{Im} f = H$.*
3. *f és un isomorfisme $\iff$ f és un monomorfisme i un epimorfisme.*

Exemple 4.4.2. Considerem l'aplicació

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} &\longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ m &\longmapsto (m \bmod 2, m \bmod 3) \end{aligned}$$

Escrivint les imatges dels 6 elements, veiem que $\ker f = \{0\}$ i $\operatorname{Im} f = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, de manera que f és un isomorfisme.

Treballar amb grups abstractes pot arribar a ser molt difícil, de manera que sovint s'intenta expressar els grups abstractes com a grups de matrius o com a permutacions.

Proposició 4.4.4 (Teorema de Cayley)**.** *Tot grup finit és isomorf a un subgrup d'un grup simètric.*

Demostració. Una permutació es pot entendre com una bijecció de $\{1, \dots, n\}$ a $\{1, \dots, n\}$. Com el grup és finit, associarem a cada element del grup una bijecció del grup en ell mateix.

Sigui $x \in G$. Definim l'aplicació

$$\begin{aligned} \varphi_x : G &\longrightarrow G \\ \varphi_x(y) &\longmapsto xy \end{aligned}$$

Observem que φ_x és injectiva, ja que $xy = xz \implies x^{-1}xy = x^{-1}xz \implies y = z$. Per tant, com G és finit, φ_x és una bijecció.

Sigui $n = |G|$. Enumerem els elements del grup d'una manera arbitrària (és a dir, establim una bijecció $\psi : \{1, 2, \dots, n\} \longrightarrow G$). Aleshores, definim $\tilde{\varphi}_x = \psi^{-1} \circ \varphi_x \circ \varphi$, que és composició de bijeccions i per tant bijecció.

Aleshores, $\tilde{\varphi}_x \in \mathfrak{S}_n$, i l'aplicació

$$\begin{aligned} \Phi : G &\longrightarrow G \\ x &\longmapsto \tilde{\varphi}_x \end{aligned}$$

és un morfisme de grups (ja que $\varphi_x \circ \varphi_y = \varphi_{xy}$) i és injectiu (exercici). Aleshores, $G \simeq \operatorname{Im} \Phi \subset \mathfrak{S}_n$, com volíem veure. □

Observació. Observem que aquest isomorfisme que hem definit no és canònic, sinó que és fins a un cert punt arbitrari. Per exemple, $\mathbb{Z}/3\mathbb{Z}$ es pot inserir dins $\mathfrak{S}_3$ prenent $\Phi(1) = (1,2,3)$ o $\Phi(1) = (1,3,2)$.

4.5 Grups quocients

Proposició 4.5.1. *Sigui $H \lhd G$ un subgrup normal. Aleshores, l'aplicació canònica*

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ a &\longmapsto \pi(a) := aH \end{aligned}$$

és un morfisme de grups, i $\ker \pi = H$.

Demostració. Recordem que vam definir el producte de classes de manera que $\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b)$. Per veure que $\ker \pi = H$, utilitzem que $aH = H \iff a \in H$. □

Proposició 4.5.2.

1. *Sigui $f : G \longrightarrow H$ un morfisme de grups. Aleshores $\ker f \lhd G$.*
2. *Recíprocament, si $K \lhd G$, existeix un morfisme de grups $f : G \longrightarrow H$ tal que $\ker f = K$.*

Demostració.

1. Sigui $f : G \longrightarrow H$ un morfisme de grups. Ja sabem que $\ker f$ és un subgrup, només ens falta veure que és normal. Hem de veure que $a \ker f = (\ker f)a$ per a tot $a \in G$. Això equival a veure que $a(\ker f)a^{-1} = \ker f$.

   Sigui $x \in \ker f$. Aleshores, $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e_H f(a^{-1}) = f(a)f(a^{-1}) = e_H$. Per tant, $axa^{-1} \in \ker f$. Amb això hem demostrat que $a(\ker f)a^{-1} \subseteq \ker f$. Com que $axa^{-1} = aya^{-1} \iff x = y$, tenim que els dos conjunts tenen el mateix cardinal, de manera que $a(\ker f)a^{-1} = \ker f$.

2. Sigui $K \lhd G$. Observem que $K = \ker \pi$ pel morfisme $\pi : G \longrightarrow G/K$.

□

Proposició 4.5.3. *Donat $H \lhd G$, sigui $\pi : G \longrightarrow G/H$ el morfisme canònic de pas al quocient. Aleshores, l'aplicació natural*

$$\begin{aligned} \left\{ \begin{smallmatrix} \text{subgrups de } G \\ \text{que contenen } H \end{smallmatrix} \right\} &\longrightarrow \{\text{subgrups de } G/H\} \\ M &\longmapsto \pi(M) := M/H \end{aligned}$$

és una bijecció que

1. *Respecta inclusions: $M_1 \subset M_2 \iff M_1/H \subset M_2/H$*
2. *Envia subgrups normals a subgrups normals*

Demostració. Exercici. És semblant a la demostració que vam fer pel teorema anàleg amb ideals. □

4.6 Teoremes d'isomorfisme

Veurem tres teoremes d'isomorfisme de grups.

Proposició 4.6.1 (1r teorema d'isomorfisme)**.** *Sigui $f : G \longrightarrow H$ un morfisme de grups. Aleshores, existeix un isomorfisme canònic $G/\ker f \simeq \operatorname{Im} f$.*

Demostració. Definim l'aplicació

$$\begin{aligned} \bar{f} : G/\ker f &\longrightarrow \operatorname{Im} f \\ a\ker f &\longmapsto \bar{f}(a\ker f) := f(a) \end{aligned}$$

Tenim que $\bar{f}$ està ben definit, ja que si $a\ker f = b\ker f$, aleshores $a = bh$ per un cert $h \in \ker f$, de manera que $f(a) = f(b)f(h) = f(b)$. Per tant, $\bar{f}(a\ker f) = \bar{f}(b\ker f)$.

Veiem també que $\bar{f}$ és un morfisme. Siguin $a\ker f$ i $b\ker f \in G/\ker f$. Aleshores,

$$\bar{f}((a\ker f)(b\ker f)) = \bar{f}(ab\ker f) = f(ab) = f(a)f(b) = \bar{f}(a\ker f)\bar{f}(b\ker f)$$

Tenim que $\bar{f}$ és injectiu, ja que si $\bar{f}(a\ker f) = e_G$, aleshores $f(a) = e_G \implies a \in \ker f \implies a\ker f = \ker f$.

Per últim, veiem que $\bar{f}$ és exhaustiu. Sigui $x \in \operatorname{Im} f$. Per definició, existeix un $a \in G$ tal que $f(a) = x$. Aleshores, prenent $a\ker f \in G/\ker f$, tenim que $\bar{f}(a\ker f) = f(a) = x$. □

Proposició 4.6.2 (3r teorema d'isomorfisme)**.** *Siguin $H \subseteq K \subseteq G$ dos subgrups normals de G (és a dir, $H \lhd G$ i $K \lhd G$, que juntament amb $H \subseteq K$ implica que $H \lhd K$). Aleshores,*

1. *$K/H \lhd G/H$.*
2. *$(G/H)/(K/H) \simeq G/K$.*

Demostració.

1. S'utilitza la proposició que ens diu que hi ha una bijecció entre els subgrups de G que contenen H i els subgrups de G/H.
2. Exercici.

□

Proposició 4.6.3. *Siguin $H \lhd G$ i $K \lhd G$. Aleshores, el conjunt $HK := \{hk : h \in H, k \in K\}$ és un subgrup de G que conté H i K. A més, $H \lhd HK$ i $K \lhd HK$.*

Demostració. En primer lloc veurem que HK és un subgrup. Tenim que $e_G = e_G e_G \in HK$. Siguin $x, y \in HK$. Aleshores, $x = h_1k_1$ i $y = h_2k_2$ per uns certs $h_1, h_2 \in H$ i $k_1, k_2 \in K$. Això implica que

$$xy^{-1} = h_1 \underbrace{k_1 k_2^{-1}}_{k} h_2^{-1}$$

on $k \in K$. Donat que $H \lhd G$, tenim que $kH = Hk$. Per tant, $kh_2^{-1} = hk$, per un cert $h \in H$. Aleshores, $xy^{-1} = h_1 k h_2^{-1} = h_1 hk \in HK$.

Les inclusions $H \subset HK$ i $K \subset HK$ són trivials, ja que $e_G \in H, K$ pel fet de ser subgrups. Ens queda veure que $H \lhd HK$ i $K \lhd HK$. Veure que $H \lhd HK$ equival a veure que $(hk)u(hk)^{-1} \in H$ per a tot $u \in H$ i per a tot $hk \in HK$. Observem que $H \lhd G$ i $hk \in HK \subset G$, de manera que $(hk)u(hk)^{-1} \in H$. Anàlogament, $K \lhd HK$. □

Observació. Es podria provar a més que tot altre subgrup que contingui H i K està contingut en HK (suposant que com a mínim un de H o K és subgrup normal de G).

Proposició 4.6.4 (2n teorema d'isomorfisme)**.** *Siguin $H \lhd G$ i $K \lhd G$. Aleshores, $H/(H \cap K) \simeq HK/H$.*

Demostració. Definim l'aplicació $\varphi : K \longrightarrow HK/H$ com $\varphi := \pi \circ \iota$, on

$$\begin{array}{ccccc} K & \overset{\iota}{\hookrightarrow} & HK & \overset{\pi}{\longrightarrow} & HK/H \\ k & \longmapsto & k & \longmapsto & kH \end{array}$$

És fàcil veure que φ és un morfisme, ja que tant ι com π ho són.

Veiem que és exhaustiu. Sigui $(hk)H \in HK/H$, on $h \in H$ i $k \in K$. Tenim que $H \lhd G$, de manera que

$$(hk)H = H(hk) = (Hh)(Hk) = H(Hk) = Hk = kH$$

Per tant, $\varphi(k) = kH = (hk)H$, de manera que $(hk)H \in \operatorname{Im}\varphi$.

Pel primer teorema d'isomorfisme, en tenim prou amb veure que $\ker\varphi = H \cap K$. Sigui $k \in K$ tal que $\varphi(k) = eH = H$. Aleshores, $kH = H \implies k \in H$. Per tant, $\ker\varphi = K \cap H$. Aplicant el 1r teorema d'isomorfisme, tenim que

$$K/\ker\varphi \simeq \operatorname{Im}\varphi \implies K/(H \cap K) \simeq HK/H$$

□

4.7 Producte directe

El producte cartesià d'una família finita de grups $G_1, \ldots, G_r$ té una estructura natural de grup, operant component a component:

$$\begin{aligned} (G_1 \times \cdots \times G_r) \times (G_1 \times \cdots \times G_r) &\longrightarrow G_1 \times \cdots \times G_r \\ (a_1, \ldots, a_r) \cdot (b_1, \ldots, b_r) &:= (a_1 \cdot b_1, \ldots, a_r \cdot b_r) \end{aligned}$$

Exercici. Comproveu que és efectivament un grup.

Es pot veure també que les inclusions naturals

$$\begin{array}{ccc} G_k & \overset{\iota_k}{\hookrightarrow} & G_1 \times \cdots \times G_k \times \cdots \times G_r \\ x & \longmapsto & (e, \ldots, x, \ldots, e) \end{array}$$

són morfismes de grups que permeten identificar cada G_k amb el subgrup $\iota_k(G_k) \lhd G_1 \times \cdots \times G_r$.

Exercici. Comprovar que el subgrup anterior és normal.

A més, si $x \in G_k$ i $y \in G_j$ amb $k \neq j$, tenim que les seves imatges commuten:

$$\iota_k(x) \cdot \iota_j(y) = \iota_j(y) \cdot \iota_k(x)$$

Un cop vistes les propietats anteriors, ens plantegem sota quines circumstàncies podem escriure un grup G com a producte cartesià de subgrups seus. Començarem amb un cas senzill:

Proposició 4.7.1. *Siguin $H \lhd G$ i $K \lhd G$. Si $HK = G$ i $H \cap K = \{e\}$, aleshores $G \simeq H \times K$. En aquest cas, diem que G és producte directe de H i K.*

Demostració. Com que suposem que $HK = G$, podem escriure tot $g \in G$ com $g = hk$, on $h \in H$ i $k \in K$. Donat que $H \cap K = \{e\}$, tenim que aquesta descomposició és única.

Vegem-ho. Suposem que $hk = \tilde{h}\tilde{k}$, amb $h, \tilde{h} \in H$ i $k, \tilde{k} \in K$. Aleshores, $\tilde{h}^{-1}h = \tilde{k}k^{-1} \in K \cap H$, de manera que $\tilde{h}^{-1}h = \tilde{k}k^{-1} = e$. Per tant, donat que els inversos són únics, tenim que $h = \tilde{h}$ i $k = \tilde{k}$.

Per tant, tot $g \in G$ es pot escriure de manera única com a $g = hk$, i tenim que $hk \in G$ per a tot $h \in H$ i per a tot $k \in K$. Això ja ens diu que l'aplicació

$$\begin{aligned} \varphi : G &\longrightarrow H \times K \\ hk &\longmapsto (h, k) \end{aligned}$$

és una bijecció. Ens falta veure que aquesta bijecció és un morfisme. Sigui $h \in H$ i $k \in K$. Observem que

$$hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})}_{\in K} k^{-1} \in K$$

ja que K és normal. De la mateixa manera,

$$hkh^{-1}k^{-1} = h \underbrace{(kh^{-1}k^{-1})}_{\in H} \in H$$

ja que H és normal. Per tant, $hkh^{-1}k^{-1} \in H \cap K = \{e\} \implies hk = kh$. Per tant, el producte d'un element de K i un de H commuta. Això ens permet veure que φ és un morfisme. Siguin $h, \tilde{h} \in H$ i $k, \tilde{k} \in K$. Aleshores,

$$\varphi(hk)\varphi(\tilde{h}\tilde{k}) = (h, k) \cdot (\tilde{h}, \tilde{k}) = (h\tilde{h}, k\tilde{k}) = \varphi(h\tilde{h}k\tilde{k}) = \varphi((hk) \cdot (\tilde{h}\tilde{k}))$$

Per tant, φ és un morfisme bijectiu, és a dir, un isomorfisme. □

Exemple 4.7.1. Sigui $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ el grup multiplicatiu dels racionals. Es pot veure que $\mathbb{Q}^* = \mathbb{Q}^*_{>0} \times \{\pm 1\}$. En aquest cas, observem que, com $\mathbb{Q}$ és abelià, tots els seus subgrups són normals.

Existeix una versió general de la proposició anterior, per a més de dos grups:

Proposició 4.7.2. *Siguin $N_1, \ldots, N_r$ subgrups normals de G, tals que cada $g \in G$ s'escriu de manera única com a producte d'elements de N_i:*

$$g = a_1 \cdots a_r \text{ amb } a_i \in N_i$$

Aleshores, $G \simeq N_1 \times \cdots \times N_r$, i diem que G és el producte directe de $N_1, \ldots, N_r$.

Demostració. Exercici. S'ha de repetir la demostració anterior. □

Observem que aquí estem suposant que la descomposició de tot element és única. La següent proposició ens dona un conjunt d'hipòtesis alternatiu on no fa falta que ho suposem.

Proposició 4.7.3. *Siguin $N_1, \ldots, N_r \lhd G$ tals que $N_1 \cdots N_r = G$. Suposem que, per a tot $i \in \{1, \ldots, r\}$, $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_r) = \{e\}$. Aleshores, $G \simeq N_1 \times \cdots \times N_r$.*

Observació. A l'enunciat de la proposició hi surt el producte de r subgrups. Només havíem definit el producte de 2 subgrups, però es pot extendre a un nombre finit de subgrups per inducció, i es pot comprovar que el resultat és un subgrup.

Si tenim una família infinita de grups $\{G_i\}_{i \in I}$, a part del seu producte cartesià també en podem definir la suma directa:

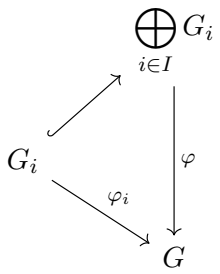
Definició 4.7.1 (Suma directa)**.** Sigui $\{G_i\}_{i \in I}$ una família de grups. Definim la seva *suma directa* com

$$\bigoplus_{i \in I} G_i := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} G_i \quad : \quad x_i = e \text{ llevat d'un nombre finit de } i\text{'s} \right\}$$

La operació entre dos elements de $\bigoplus G_i$ es defineix terme a terme.

La "gràcia" de la suma directa és la següent propietat universal:

Proposició 4.7.4. *Sigui $\varphi_i : G_i \longrightarrow G$ una família de morfismes. Aleshores, existeix un únic morfisme $\varphi : \bigoplus G_i \longrightarrow G$ tal que el diagrama de la dreta és commutatiu.*
A més, el morfisme φ ve donat per $\varphi((x_i)_{i \in I}) = \prod \varphi_i(x_i)$, que observem que és un producte finit per la definició de suma directa.



Observació. Si tenim un nombre finit de grups, aleshores la suma directe és el mateix que el producte directe, ja que la condició que $x_i = e$ llevat d'un nombre finit de i's no aporta res.