Apunts d'estructures algrebraiques

Aleix Torres i Camps

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

Índex

Capítol 1

Introducció

1.1 Operacions i propietats

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

Definició 1.1.2. Algunes propietats de les operacions poden ser:

1. (PC) Propietat commutativa (o abeliana) $\forall a, b \in A \ \varphi(a, b) = \varphi(b, a)$.
2. (PA) Propietat associativa $\forall a, b, c \in A \ \varphi(a, \varphi(b, c)) = \varphi(\varphi(a, b), c)$.
3. (EN) Element neutre $\exists e \in A$ tal que $\forall a \in A \ \varphi(e, a) = \varphi(a, e) = a$.
4. (PI) Invers d'un element $a \in A$ és $b \in A$ tal que $\varphi(a, b) = \varphi(b, a) = e$.
5. (PD) Si tenim dues operacions, que la primera (φ) sigui distributiva respecte la segona (μ) vol dir que $\varphi(a, \mu(b, c)) = \varphi(\mu(a, b), \mu(a, c))$ i que $\varphi(\mu(b, c), a) = \varphi(\mu(b, a), \mu(b, c))$.

Proposició 1.1.3. L'element neutre és únic.

Demostració. En efecte, si existisin 2 elements neutres, e i e', aleshores $e = \varphi(e, e') = e'$, amb la qual cosa, han de ser el mateix element. □

Proposició 1.1.4. Si l'invers existeix i l'operació és associativa, aleshores és únic.

Demostració. En efecte, si $\exists b, c$ tals que $\varphi(a, b) = \varphi(b, a) = \varphi(a, c) = \varphi(c, a) = e$. En aquest cas, $b = \varphi(b, \varphi(a, c)) = \varphi(\varphi(b, a), c) = c$, per tant, $b = c$ i són el mateix element. □

1.2 Estructures algebraiques bàsiques

Definició 1.2.1.

1. Un Grup $(G, *)$ cal que compleixi EN, PA, PI.
2. Un Semigrup $(G, *)$ cal que compleixi EN, PA.
3. Un Grup Abelià és un grup amb PC.
4. Una Anell $(A, +, *)$ cal que $(A, +)$ sigui un grup abelià, $(A, *)$ un semigrup i la PD respecte la primera.
5. Un Anell communtatiu (o abelià) és un anell on $(A, *)$ és commutatiu.
6. Un Cos és un Anell $(A, +, *)$ tal que $(A \setminus \{0\}, *)$ és un grup abelià. On 0 és l'element neutre de $(A, +)$.
7. $(M, +)$ és un mòdul sobre l'Anell A si $(M, +)$ és un grup abelià i $A \times M \to M$ (multiplicació per escalars) tal que: $a(m_1 + m_2) = am_1 + am_2$, $(a + b)m = am + bm$, $a(bm) = (ab)m$ i $1_A m = m$ $(\forall a, b \in A, \forall m, m_1, m_2 \in M)$.
8. Un espai vectorial és un mòdul sobre un Cos.

Capítol 2

Anells

En tot el capítol abreujarem $(A, +, \cdot)$ per A que denotarà un anell communatiu sense necessitat de dir-ho explícitament.

2.1 Propietats dels anells

Definició 2.1.1. 0_A és l'element neutre de la suma $(+)$, el zero. Mentre que l'element neutre del producte $(\cdot)$ és 1_A, que l'anomenarem u. Denotarem $-a$ l'element invers d'a respecte $+$ (l'oposat d'a). I denotarem a^{-1} l'element invers d'a respecte del producte (en un anell no sempre existeix). Anomenarem $A^* = \{a \in A \text{ tal que } \exists a^{-1}\}$ el conjunt dels inversos del qual s'obté un grup abelià, també se l'anomena grup multiplicatiu.

Proposició 2.1.2. Propietats bàsiques dels anells:

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

Demostració.

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

□

Exemple 2.1.1. Alguns exemples d'anells.

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. Les matrius amb components a A $(M_n(A))$ és un anell
3. $\mathbb{Z}[J] = \{a_0 + a_1 J + a_2 J^2 + a_3 J^3 + a_4 J^4 : a_i \in \mathbb{Z}\}$ $J = e^{2\pi i/5}$

Proposició 2.1.3. Sigui A un anell tal que el neutre de la suma és el neutre del producte $(0_A = 1_A)$ aleshores l'anell té un sol element $(A = \{0_A\})$.

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

Definició 2.1.4. Sigui A un anell, $n \in \mathbb{Z}$ i $a \in A$. Llavors, si $n > 0$, $n \cdot a := a + \cdots + a$, si $n < 0$, $n \cdot a := (-a) + \cdots + (-a)$, si $n = 0_{\mathbb{Z}}$, $0_{\mathbb{Z}} \cdot a = 0_A$. De la mateixa manera, si $n > 0$, $a^n := a \cdot \ldots \cdot a$, si $n < 0$, $a^n := a^{-1} \cdot \ldots \cdot a^{-1}$ i si $n = 0_{\mathbb{Z}}$, $a^n = 1_A$.

Definició 2.1.5. Direm que l'anell A té característica n, si n és el menor enter positiu tal que $n \cdot 1_A = 0_A$. En cas que no existeixi ($n \cdot 1_A \neq 0_A \ \forall n \in \mathbb{Z}^+$), direm que té característica 0.

Observació 2.1.6. Està clar que $\operatorname{char} A \cdot a \overset{\text{def}}{=} a + \ldots + a = a(1 + \ldots + 1) = a \cdot 0_A = 0_A \quad \forall a \in A$.

2.2 Subanells i anells productes

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

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

Proposició 2.2.2. Sigui $S \subset A$ un anell, aleshores S és un subanell $\iff$ S és un anell i $1_A \in S$.

Demostració.
$\implies$) Cal veure que $(S, +)$ és un grup (Abelià), $(S, \cdot)$ és un semigrup i que és compleix la PD. De les operacions de A s'hereden automàticament les propietats PA, PC, PD. Ara de la primera característica dels subanells tenim $1_A \in S$. I de la 2a, fent $b = a$, tenim $0_A \in S$ i ara, fent $a = 0_A$, $b = a$, tenim l'invers per la suma. Per tant, S és un anell.
$\impliedby$) Si S és un anell, té invers de la suma, per tant, està tancat per la suma i està tancat per la multiplicació. Això demostra les característiques 2 i 3, respectivament. La propietat 1 ens la donen d'hipòtesi. □

Exemple 2.2.1. $\mathbb{Z} \subset \mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ són anells amb el mateix neutre, per tant, els petits són subanells dels grans. Per altra banda, $2\mathbb{Z} = \{a \in \mathbb{Z} : a \equiv 0 \mod 2\} = \{2k : k \in \mathbb{Z}\}$ no és un subanell, perquè no té EN.

Exercici 2.2.3. Sigui $J = e^{2\pi i/n}$. $\mathbb{Z}[J] = \{a_0 + a_1 J + \ldots + a_{n-1} J^{n-1} : a_i \in \mathbb{Z}\}$. Demostreu que és un anell comprovant que és un subanell de $\mathbb{C}$ i tenen el mateix neutre.

Solució. Per començar $\mathbb{Z}[J] \subset \mathbb{C}$. El neutre d'ambdos és $1 \in \mathbb{Z} \subset \mathbb{C}$. Si restem o multipliquem dos elements de $\mathbb{Z}[J]$ ens hi quedem. Aleshores és un subanell de $\mathbb{C}$ i, per tant, és un anell. □

Definició 2.2.4. Donats A, B anells. el seu anell producte és el conjunt $A \times B$ amb les operacions:

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

Exemple 2.2.2. Com que $\mathbb{Z}$ és un anell, $\mathbb{Z} \times \mathbb{Z}$ és també un anell amb les operacions definides pel producte. Ara, el subconjunt $A = \{(a, 0) : a \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$ és un anell, però no és un subanell perquè el neutre d'$\mathbb{A}$ és $(1, 0)$ i el de $\mathbb{Z} \times \mathbb{Z}$ és $(1, 1)$.

Definició 2.2.5. Sigui A un anell, definim $A[x]$ com el conjunt de polinomis amb coeficients a A. De la mateixa manera, $A[x_1, \ldots, x_n]$ indicarà el conjunt de polinomis amb n variables amb coeficients a A.

Proposició 2.2.6. Si A és un anell, $A[x]$ també.

Demostració. Les operacions de polinomis es fan component a component i, per tant, hereden les propietats de A. La suma té element neutre (el mateix que A), invers (el polinomi el qual cada un dels coeficients és l'invers del corresponent amb mateix grau), és associatiu i comutatiu. El producte té el mateix element neutre que A i hereda l'associativitat i la commutativitat. □

Exemple 2.2.3. $\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$ és una cadena d'anells i subanells.

2.3 Ideals

Definició 2.3.1. Sigui A un anell. Un subconjunt $I \subset A$ és un ideal si:

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

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

Exemple 2.3.1. Alguns ideals:

1. $\{0_A\}$ L'ideal zero. A l'ideal total.
2. $m\mathbb{Z} \subset \mathbb{Z}$ és un ideal.
3. Per $\alpha \in \mathbb{Q}$, aleshores $I = \{f(x) \in \mathbb{Q}[x] : f(x) = 0\} \subset \mathbb{Q}[x]$ és un ideal de $\mathbb{Q}[x]$ i coincideix amb el generat per $(x - \alpha)$.
4. De forma similar $I = \{f(x, y) \in \mathbb{Q}[x, y] : f(0, 0) = 0\} \subset \mathbb{Q}[x, y]$ ideal de $\mathbb{Q}[x, y]$. Coincideix amb $(x, y) = I$.

Definició 2.3.2. L'anell principal o l'anell generat per $a \in A$ és $(a) := \{am : m \in A\}$. Similarment l'ideal finitament generat per $a_1, \ldots, a_n \in A$ és $(a_1, a_2, \ldots, a_n) := \{a_1 m_1 + \ldots + a_n m_n : m_i \in A\}$. Direm que un anell és principal si tots els seus ideals són principals, és a dir, generats per un sol element.

Proposició 2.3.3. $I, J \subset A$ ideals

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

Demostració.

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

   A més, és el menor que conté a I i a J, perquè si un ideal K els conté, com que $\forall a \in I \subset K$, $\forall b \in J \subset K$ aleshores, com que K ha de ser tancat per la suma, segur que $a + b \in K$.

2. Siguin $a_j, a_i \in I$, $b_j, b_i \in J$ i $u = \sum_j a_j \cdot b_j, v = \sum_i a_i \cdot b_i \in I \cdot J$, $\alpha_1, \alpha_2 \in A$, llavors, $\alpha_1 u + \alpha_2 v = \alpha_1 \sum_j a_j \cdot b_j + \alpha_2 \sum_i a_i \cdot b_i =$ [PD i PA] $= \sum_j (\alpha_1 a_j) \cdot b_j + \sum_i (\alpha_2 a_i) \cdot b_i = \sum_{k=i,j} (\alpha a_k) b_k \in I \cdot J$, perquè $\alpha_1 a_j, \alpha_2 a_i \in I$.

□

Proposició 2.3.4. Sigui A un anell i siguin $a \in A$, $u \in A^*$, aleshores $(a) = (ua)$, és a dir, l'ideal generat per a i per ua són el mateix.

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

Proposició 2.3.5. A és un cos $\iff$ els seus únics ideals són 0 i A.

Demostració.
$\implies$) Sigui $I \subset A$ un ideal no nul. Sigui $x \in I$, $x \neq 0$, A cos $\implies \exists x^{-1}$, i com $x \in I \implies 1 = xx^{-1} \in I \implies \forall a \in A \ a = a \cdot 1 \in I \implies I = A$.
$\impliedby$) Sigui $x \neq 0 \in A$, com que $(x) \neq 0 \implies (x) = A \implies 1 \in (x) \implies \exists y \in A$ tal que $1 = xy$ per tant, $y = x^{-1}$. □

Teorema 2.3.6. Tots els ideals de l'anell de $\mathbb{Z}$ són principals.

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

Aleshores, suposem que hi ha un element y que no és de la forma mk. Li fem la divisio euclidiana i escrivim $y = mk + r$ per algun r (el qual pertany a I perquè I és tancat per la suma) entre $m-1$ i 0, suposem que no és 0. Aleshores, hem arribat a contradicció, perquè abans haviem dit que m era el mínim i ara hem vist que n'existeix un element positiu més petit. Per tant, $r = 0$, que implica que $y = mk \in I$, aleshores $I = (m)$ és principal. □

Proposició 2.3.7. Sigui k un cos. Tots els ideals de $k[x]$ són principals.

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

2.4 Morfisme d'anells

Definició 2.4.1. Siguin A, B dos anells. Es diu que una aplicació $f : A \to B$ és un morfisme d'anells si preserva les operacions en A i B. És a dir, si

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

Anomenarem monomorfisme al morfisme injectiu, epimorfisme al morfisme exhaustiu i isomorfisme al morfisme bijectiu.

Proposició 2.4.2. Sigui A un anell qualsevol, l'aplicació $\varphi : \mathbb{Z} \to A$ amb $\varphi(m) = m \cdot 1_A$ és un morfisme. A més, φ és un morfisme injectiu si, i només si, $\operatorname{char} A = 0$. En tot cas, es compleix que $\varphi^{-1}(0) = (\operatorname{char} A)$.

Demostració. Per veure que φ és un morfisme cal comprovar les 3 propietats dels morfismes. La primera és que $\varphi(1) = 1 \cdot 1_A = 1_A$. La segona que $\varphi(n+m) = (n+m)1_A = (1_A + \ldots + 1_A) + (1_A + \ldots + 1_A) = n1_A + m1_A = \varphi(n) + \varphi(m)$. Per últim, $\varphi(nm) = nm1_A = (1_A + \ldots + 1_A) + \ldots + (1_A + \ldots + 1_A) = (1_A + \ldots + 1_A)(1_A + \ldots + 1_A) = \varphi(n)\varphi(m)$. Aleshores, φ és un morfisme d'anells.

$\Longrightarrow$) Suposem que és φ injectiu i que $\operatorname{char} A = n \neq 0$. Aleshores, $\varphi(0) = \varphi(n) = \varphi(2n) = \ldots = \varphi(mn) = 0$, cosa que no pot passar si φ és injectiu, llavors $\operatorname{char} A = 0$.

$\Longleftarrow$) Suposem que $\operatorname{char} A = 0$ i que tenim $\varphi(n) = \varphi(m)$. Aleshores, per ser φ un morfisme tenim que $\varphi(n) - \varphi(m) = \varphi(n-m) = 0$, que significa que sumant 1_A un total de $n-m$ vegades, arribem a 0, per tant, que $\operatorname{char} A = n - m$. Per altra banda, sabem que la característica de A és 0 llavors $n = m$. En conseqüència, φ és un morfimes injectiu.

$\subseteq$) L'antiimatge del 0 per φ són els enters tals que si sumem 1_A tantes vegades com l'enter arribem a 0. Per tant, han de ser divisors del $\operatorname{char} A$ o 0, és a dir, pertanyen a $(\operatorname{char} A)$. Tenim que $\varphi^{-1}(0) \subseteq (\operatorname{char} A)$.

$\supseteq$) Sigui $a \in (\operatorname{char} A)$, és a dir, a és un múltiple de la característica d'A, llavors podem escriure $a = k \operatorname{char} A$ i, per tant, $\varphi(a) = \varphi(k)\varphi(\operatorname{char} A) = \varphi(k) \cdot 0_A = 0_A$. És a dir, $a \in \varphi^{-1}(0)$, com que ho hem fet per un a arbitrari, tenim que $\varphi^{-1} \supseteq (\operatorname{char} A)$. Ajuntant aquest resultat i l'anterior, tenim que $\varphi^{-1}(0) = \operatorname{char} A$ que és el que volíem veure. □

Proposició 2.4.3. Siguin A i B dos anells i $f : A \to B$ un morfisme d'anells. Aleshores:

1. $f(a^n) = f(a)^n$
2. $a \in A^* \implies f(a) \in B^*$, $f(a)^{-1} = f(a^{-1})$
3. Sigui $J \subset B$ un ideal, llavors $f^{-1}(J) \subset A$ és un ideal
4. En general, la imatge d'un ideal d'A no és un ideal de B.

5. Si f és exhaustiva, llavors $I \subset A$ ideal $\implies f(I) \subset B$ també és un ideal.
6. $\ker f := \{a \in A : f(a) = 0\}$ és un ideal d'A.
7. $\mathrm{Im} f := \{f(a) : a \in A\} \subset B$ subanell de B.
8. f injectiva $\iff \ker f = 0$.
9. A cos $\implies f = 0$ o f injectiu.

Demostració.

1. Per inducció, es poden treure potències una per una.
2. Per la propietat del producte dels morfismes i envia l'element neutre a l'element neutre $1_B = f(1_A) = f(aa^{-1}) = f(a)f(a^{-1})$. Per tant, $f(a)$ té invers i és $f(a^{-1})$.
3. Siguin $a_1, a_2 \in f^{-1}(J)$ i $\lambda, \mu \in A$, llavors $\lambda a_1 + \mu a_2 \in f^{-1}(J)$? Sí, perquè $f(\lambda a_1 + \mu a_2) = f(\lambda)f(a_1) + f(\mu)f(a_2) \in J$ perquè és combinació d'elements de J. Per tant, és un ideal.
4. Contraexemple: si $A = \mathbb{Z}$ i $B = \mathbb{Q}$ i f és la inclusió. Un ideal de A és per exemple (2) però $f((2))$ no és un ideal perquè $2\frac{1}{3} \notin f((2))$.
5. Siguin $f(a), f(b) \in f(I)$ i $\lambda, \mu \in B$, llavors $\lambda f(a) + \mu f(b) \in f(I)$, sí, perquè al ser exhaustiva, $\exists x_\lambda, x_\mu$ tal que $f(x_\lambda) = \lambda$ i $f(x_\mu) = \mu$. Per tant, $\lambda f(a) + \mu f(b) = f(x_\lambda)f(a) + f(x_\mu)f(b) = f(x_\lambda a + x_\mu b) \in f(I)$.
6. Per la definició $\ker f = f^{-1}((0))$, utilitzant la propietat 3, el $\ker f$ és un ideal.
7. L'element neutre hi és perquè $f(1_A) = 1_B$, la resta i el producte de dos elements hi són perquè f està tancat per la suma (i resta) i pel producte.
8. Que f sigui injectiva fa que només el 0 pugui anar al 0. Ja que, en qualsevol cas $f(0+0) = f(0)+f(0) \implies f(0) = 0$. I que $\ker f = 0$ implica que si dos elements tiguéssin la mateixa imatge $f(a) = f(b) \implies f(a) - f(b) = 0 \implies f(a-b) = 0$ i com que només el 0 va al 0, $a = b$.
9. Suposem que A és un cos i que dos elements diferents tenen la mateixa imatge $f(a) = f(b) \implies f(a-b) = 0$. Aleshores, $f(x) = f(x)f(1) = f(x(a-b)^{-1}(a-b)) = f(x(a-b)^{-1})f(a-b) = 0$. Llavors, f és la funció que va tot a 0. (I sembla que $0_B = 1_B$). Altrament f és injectiva.

□

2.5 Anell quocient

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

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

Observació 2.5.2. Aquestes operacions estan ben definides:

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

Proposició 2.5.3. Aquestes dues operacions tenen totes les propietats necessàries per a què A/I sigui un anell. El qual en direm l'anell quocient d'A per I.

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

Exemple 2.5.1. Alguns exemples d'espais quocients.

1. Si $A=\mathbb{Z}$ i $I=(m)$, aleshores $A/I=\mathbb{Z}/m\mathbb{Z}$.
2. Sigui $A=K[x]$, $\alpha\in K$ i $I=(x-\alpha)$. Aleshores, fixem-nos que la següent aplicació

$$\begin{array}{rccc} A/I= & K[x]/(x-\alpha) & \longrightarrow & K \\ & \overline{p(x)} & \longmapsto & p(\alpha) \end{array}$$

   està ben definida. Si $q(x)\in\overline{p(x)}$, llavors $q(x)-p(x)\in(x-\alpha)\implies q(x)-p(x)=(x-\alpha)h(x)\implies q(\alpha)-p(\alpha)=0$. Per tant $p(\alpha)=q(\alpha)$. A més, és un morfisme d'anells.
3. $A=\mathbb{R}[x]$ i $I=(x^2+1)$ llavors el seu quocient és isomorf a $\mathbb{C}$. Enviant $\overline{p(x)}$ a $p(i)$.

Proposició 2.5.4. L'aplicació natural

$$\begin{array}{rcl} \pi : A & \twoheadrightarrow & A/I \\ a & \longmapsto & \bar{a} \end{array}$$

és un morfisme exhaustiu d'anells.

Demostració. La definició de les operacions A/I garanteix que π sigui un morfisme (l'1 va a l'$\overline{1}$, la suma a la suma i el producte al producte). És exhaustiva perquè per a tota classe de A/I, diguem-li $\overline{a}$, té un representant que suposem que és a, llavors $\pi(a)=\overline{a}$. □

Proposició 2.5.5. Sigui A un anell i I un ideal.

(a) Sigui $J\subseteq A$ un ideal tal que $J\supseteq I$, llavors $J/I:=\pi(J)\subseteq A/I$ és un ideal.

(b) Sigui $U\subseteq A/I$ un ideal, existeix un únic ideal $J\subseteq A$ tal que $J/I=U$ i, a més, $J\supseteq I$.

Demostració. (a) Per una propietat anterior, com que π és exhaustiva, la imatge d'un ideal és un ideal, aplicat a a l'ideal J, $\pi(J)$ és un ideal de A/I.

(b) Sigui $J=\pi^{-1}(U)\subseteq A$, que és un ideal, perquè l'antiimatge d'un ideal és un ideal. Notem que $\pi(J)=\pi(\pi^{-1}(U))\overset{\text{exh}}{=}U$. Aleshores, com que U és ideal, $\overline{0}\in U\implies I=\pi^{-1}(0)\subseteq\pi^{-1}(U)=J$, on hem usat que $\ker\pi=I$, que es comprova fàcilment.

Suposem que tenim J,J' que satisfan $\pi(J)=\pi(J')=U$ i $J'\supseteq I\subseteq J$. Sigui $a\in J$, per tant, $\pi(a)=\overline{a}\in U$, llavors existeix $a'\in J'$ tal que $\pi(a')=\overline{a}$. Per tant, tenim que $\pi(a-a')=\overline{0}$, és a dir, $a-a'\in I\subseteq J'$. Com que J' és un ideal, és tancat per la suma i $a=(a-a')+a'\in J'$. Com que ho hem fet per un $a\in J$ arbitrari, tenim que $J\subseteq J'$. El mateix argument serveix per a veure que $J'\subseteq J$. Per tant, $J=J'$ i tenim unicitat. □

Proposició 2.5.6. Propietat universal del quocient. Sigui $f:A\to B$ un morfisme d'anells $I\subset A$ ideal tal que $I\subset\ker f$. Existeix un únic morfisme $\varphi:A/I\to B$ tal que $\varphi\circ\pi=f$.

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

Suposem que existeix una $\varphi'\neq\varphi$ que satisfaci la mateixa propietat. Però per tot $\overline{x}\in A/I$, per ser π exhaustiva podem pendre $x\in A$ i escriure $\varphi(\overline{x})=\varphi(\pi(x))=f(x)=\varphi'(\pi(x))=\varphi'(\overline{x})$. D'aquesta manera veiem que φ i φ' són la mateixa funció. Per tant, hem acabat, només n'hi ha una. □

Teorema 2.5.7. (Teorema d'isomorfisme d'anells) Sigui $f:A\to B$ un morfisme d'anells. Hi ha un morfisme canònic $\overline{f}:A/\ker f\to\operatorname{Im}f$.

Demostració. Aplicarem la proposició anterior al morfisme $\tilde{f} : A \to \mathrm{Im}(f) \subseteq B$ (que fa el mateix que f). $\tilde{f}$ és un morfisme d'anells perquè vam veure que la imatge d'un morfisme era un subanell, per tant, un anell i hereda les propietats de f. També vam veure que $I = \ker f$ és un ideal. Aleshores, la proposició anterior ens proporciona un morfisme φ que li direm $\overline{f} : A/\ker f \to \mathrm{Im}\, f$, que a $\overline{a}$ l'envia a $\overline{f}(a) = \tilde{f}(a) = f(a)$.

$\overline{f}$ és exhaustiu perquè $\tilde{f}$ ho és i és injectiu perquè $\ker \overline{f} = \{\overline{a} : \overline{f}(\overline{a}) = 0\} = \{\overline{a} : \tilde{f}(a) = 0\} = \{\overline{a} : f(a) = 0\} = \ker f = \overline{0}$, perquè els elements a tals que $f(a) = 0$ pertanyen al nucli i, per tant, en aquest cas, en el $\overline{0}$. Aleshores $\overline{f}$ és un morfisme bijectiu i tenim un isomorfisme entre $A/\ker f$ i $\mathrm{Im}\, f$. □

2.6 Ideals íntegres, primers i maximals

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

Definició 2.6.2. Un ideal $\mathfrak{p} \subset A$ d'un anell qualsevol s'anomena primer si $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Anomenarem l'espectre de A $\mathrm{Spec}(A) = \{\mathfrak{p} \subset A; \mathfrak{p} \text{ primer}\}$.

Proposició 2.6.3. Sigui $\mathfrak{p} \subset A$ un ideal. Llavors $\mathfrak{p}$ primer $\iff A/\mathfrak{p}$ és un anell íntegre.

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

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

Definició 2.6.4. Un ideal $m \subsetneq A$ s'anomena maximal si no està contingut en cap altre ideal propi d'A.

Proposició 2.6.5. $m \subsetneq A$ és un ideal. Llavors, m maximal $\iff A/m$ és un cos.

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

$\implies$) Els ideals de A/m són de la forma J/m amb $m \subset J$ ideal d'A (és una propietat que hem vist anteriorment). Com que m és maximal, o $J = m$ o bé, $J = A$, en el primer cas $J/m = (0)$ i, en el segon, $J/m = A/m$. Per tant, els únics ideals de A/m són el zero i el total $\implies A/m$ és un cos (propietat dels cossos que vam veure). □

Corol·lari 2.6.6. Sigui A un anell i m un ideal. Aleshores, m maximal $\implies m$ primer.

Demostració. Utilitzant les caracteritzacions d'ideals primers i maximals, si m és maximal, tenim que A/m és un cos i, en conseqüencia, és íntegre, per tant m és un ideal primer. □

2.7 Anell de fraccions

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

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

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

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

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

Proposició 2.7.4. Les operacions anteriors estan ben definides.

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

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

Observació 2.7.5. Aquestes operacions compleixen totes les propietats necessàries per tal que $\mathrm{Fr}(A)$ sigui un anell. On el $0_{\mathrm{Fr}(A)} = \frac{0}{1}$ i $1_{\mathrm{Fr}(A)} = \frac{1}{1}$. A més, tot element no nul té invers. Si $\frac{a}{s} = \frac{0}{1}$, llavors $a1 = 0s = 0 \implies a = 0$. Llavors si $\frac{a}{s} \neq \frac{0}{1} \implies a \neq 0$, el seu element invers és $\frac{s}{a}$ ja que $\frac{a}{s}\frac{s}{a} = \frac{1}{1}$, per tant $\mathrm{Fr}(A)$ és un cos.

Observació 2.7.6. L'aplicació natural

$$i : A \longhookrightarrow \mathrm{Fr}(A)$$
$$a \longmapsto i(a) = \frac{a}{1}$$

és un morfisme injectiu entre anells.

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

Exemple 2.7.1. $\mathbb{Q} := \mathrm{Fr}(\mathbb{Z})$ o $\mathbb{Q}(x) := \mathrm{Fr}(\mathbb{Q}[x])$ o també $\mathbb{Q}(x) = \mathrm{Fr}(\mathbb{Z}[x])$

Proposició 2.7.7. Propietat universal del cos de fraccions. Sigui A un anell íntegre.

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

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

Demostració.

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

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

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

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

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

□

2.8 Anell factorial

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

Definició 2.8.1. Un element $a \in A \setminus (A^* \cup \{0\})$ és irreductible si quan el poguem escriure com $a = bc$ llavors b o c són unitats ($\in A^*$).

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

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

Demostració. Suposem que $a = bc$ llavors $bc \in (a)$ llavors, per ser (a) un ideal primer, o bé b, o bé c pertanyen a (a). Sense pèrdua de generalitat, suposem $b \in (a)$, aleshores existeix un $d \in A$ tal que $b = ad$, i podem escriure $a = adc$, per tant, $a(1 - dc) = 0$ que per ser A íntegre i $a \neq 0 \implies dc = 1$, llavors $c \in A^*$. En conseqüència, a és irreductible. □

Exemple 2.8.1. Considerem l'anell $A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. En aquest anell 2 és irreductible. Suposem que $2 = (\alpha+\beta\sqrt{-5})(\gamma+\delta\sqrt{-5})$, llavors $2 = (\alpha-\beta\sqrt{-5})(\gamma-\delta\sqrt{-5})$, per tant, $4 = (\alpha^2+5\beta^2)(\gamma^2+5\delta^2)$, que és una igualtat entre enters positius llavors els divisors són 1,2 o 4. Fixem-nos que 2 no es pot escriure de la forma $1 \leq \alpha^2 + 5\beta^2 \leq 4$, per tant, els factors són 4 i 1, com que $1 \in \mathbb{Z}[\sqrt{-5}]^*$ és una unitat, 2 és irreductible. En canvi, 2 no és primer, perquè $2|6$ però com $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, però 2 no divideix a cap dels dos perquè 2 no divideix a 1.

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

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

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

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

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

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

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

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

Exemple 2.8.2. No sempre existeix. Per exemple, en l'anell $A = \mathbb{Z}[\sqrt{-5}]$, $2|6$, $2|2+2\sqrt{-5}$ i $1+\sqrt{-5}|6$ i $1+\sqrt{-5}|2+2\sqrt{-5}$ i tant 2 com $1+\sqrt{-5}$ són irreductibles i, per tant, no es divideixen entre ells. Llavors el $\gcd(6,2+2\sqrt{-5})$ no existeix.

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

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

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

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

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

Demostració.

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

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

□

Definició 2.8.11. Dos ideals I, J d'un anell A s'anomenen coprimers si $I + J = A$. Dos elements $a, b \in A$ s'anomenen coprimers si $(a)+(b) = (1) = A$. En aquest cas tindrem una identitat de Bézout.

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

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

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

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

Demostració. Només cal veure $\implies$ perquè el recíproc és sempre cert per anells íntegres.
Suposem que $a|bc$ i a no divideix a b. Tenim $(a)+(b)=(d)$, llavors $a \in (d) \implies d|a \implies d \in A^*$ o bé que $d = au$ amb $u \in A^*$, perquè a és irreductible. Però com que $b \in (d) \implies d|b$, però $au = d|b$ llavors $a|b$ cosa que contradiu amb la hipòtesi que a no divideix a b.
Per tant, $d \in A^* \implies (d) = A = (1)$, podem suposar que $d = 1$. Per la identitat de Bézout, $\exists \lambda, \mu \in A$ tal que $\lambda a + \mu b = 1$. Llavors, $\lambda ac + \mu bc = c$, ara, com que $a|bc$ per hipotesi i $a|ac$ tenim que $a|c$. □

Proposició 2.8.13. A DIP. Aleshores

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

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

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

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

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

Podria passar que no acabéssim mai? Llavors tindríem elements $a, a_1, \cdots$ tal que

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

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

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

2.9 Anell euclidià

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

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

Aleshores, δ és una norma d'A.

Exemple 2.9.1. En el enters podem fer valor absolut i en el anell de polinomis sobre un cos, la funció que retorna el grau del polinomi. Per cossos, simplement la funció 0 compleix els requisits.

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

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

Exemple 2.9.2. $\mathbb{Z}[\sqrt{-5}]$ no és euclidià. La gran majoria d'anells quadràtics $\mathbb{Z}[\sqrt{d}]$ no són euclidians.

Proposició 2.9.3. Propietats bàsiques de $K[x]$, K un cos

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

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

Demostració.

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

Lema 2.9.4. $f(\alpha)=0 \iff x-\alpha | f(x)$.

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

Ara, siguin $\alpha_1,\dots,\alpha_m$, m arrels diferents, en particular, no són associats, tals que anul·len f, pel lema $x-\alpha_i | f$ i aquests $x-\alpha_i$ no són associats. Ara, per una proposició anterior, la multiplicació de tots els $x-\alpha_i$ divideix a f, és a dir, $\prod(x-\alpha_i)|f(x)$. Per tant, tenim que $f(x)=g(x)\prod(x-\alpha_i)$, per l'apartat anterior, $n=\deg(f)=\deg(g)+\deg(\prod(x-\alpha_i))=\deg(g)+m$, en conseqüència, $m\leq n$.

3. El ser $K[x]$ euclidià, és factorial i per tant, tot element no nul té una factorització única en irreductibles (o primers). Llavors el màxim comú divisor sempre existeix i és únic, ja que és la unió de tots els primers compartits (amb la multiplicitat compartida més gran que tinguin els dos alhora). Llavors, com és principal $(h(x))=(f(x))+(g(x))$ i per tant, $h\in(f(x))+(g(x))$, és a dir, h es pot escriure com a suma de dos elements, un de $(f(x))$ i un de $(g(x))$.

□

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

2.10 Polinomis amb coeficients en un anell factorial

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

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

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

Observació 2.10.2. Com que estem en un anell factorial, el mcd està determinat llevat d'unitats. Aleshores, el contingut d'un polinomi està definit llevat d'unitats.

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

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

Demostració. Tenim que $f(x)=\sum_{j=0}^m a_jx^j$ i que $g(x)=\sum_{j=0}^n b_jx^j$, llavors $f(x)g(x)=\sum_{j=0}^{m+n}c_jx^j$ on $c_j=\sum_{k=0}^j a_kb_{j-k}$.
Si $p(x)q(x)$ no fos primitiu, existiria $p\in A$ irreductible tal que $p|c(fg)$. Llavors $p|c_0$, $p|c_1$, $\cdots$, $p|c_{m+n}$. Siguin $r=\min\{j:p\nmid a_j\}$ i $s=\min\{j:p\nmid b_j\}$. Aleshores, $c_{r+s}=a_0b_{r+s}+\cdots+a_rb_s+\cdots+a_{r+s}b_0$. Els primers són dividits per p perquè $p|a_{j<r}$ i els últims també perquè $p|b_{j<s}$. Per tant, p sí divideix a a_rb_s i per tant, o bé divideix a a_r o a b_s, contradicció. □

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

$$f(x)=cf_0(x)\qquad c\in K,\ f_0(x)\in A[x]\text{ primitiu}$$

Demostració. (Obviant l'abús de notació) Sigui $d\in A$ tal que $g(x)=df(x)\in A[x]$ (ha d'existir, almenys multiplicant tots el denominadors). Sigui $k=c(g(x))$, llavors $g_0(x)=\frac{1}{k}g(x)\in A[x]$ és primitiu, i $f(x)=\frac{k}{d}g_0(x)=\frac{k}{d}\left(\frac{d}{k}f(x)\right)$.
Unicitat: Suposem que $c_1f_1(x)=c_2f_2(x)$ amb $c_1,c_2\in K$, $f_i(x)\in A[x]$ primitiu. Podem suposar que $c_1,c_2\in A$ i que són coprimers (si tenen factors comuns, els podem simplificar). Sigui $p\in A$ irreductible tal que $p|c_1$

$$p|c_1\implies p|c_2f_2(x)\implies p|c(c_2f_2(x))=c_2c(f_2(x))=c_2$$

Per tant, $c_1\in A^*$. Simètricament $c_2\in A^*$. Aleshores, c_1 i c_2 són associats i, automàticament, f_1 i f_2 també. Per tant, es tracta de la mateixa factorització (llevat d'unitats). Naturalment, si $f(x)\in A[x]$ la descomposició serà

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

□

Corol·lari 2.10.6. Si $f(x), g(x) \in A[x]$ implica que $c(f(x)g(x)) = c(f(x))c(g(x))$.

Demostració. $f(x) = af_0(x)$ i $g(x) = bg_0(x)$, on $a = c(f)$ i $b = c(g)$, $f_0, g_0 \in A[x]$ primitius. Per tant, $f(x)g(x) = (ab)(f_0(x)g_0(x)) \implies ab = c(f(x)g(x))$ (per unicitat). □

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

Demostració.
$\Longleftarrow$) Immediat per ser $A[x]$ subconjunt de $K[x]$.
$\Longrightarrow$) Suposem $f(x) = a(x)b(x)$ amb $a(x), b(x) \in K[x]$ (amb els graus més grans o iguals que 1), llavors $a(x) = \alpha a_0(x)$ i $b(x) = \beta b_0(x)$, $\alpha, \beta \in K$ i $a_0(x), b_0(x) \in A[x]$ primitius. $f(x) = \alpha\beta a_0(x)b_0(x)$, posem $\alpha\beta = \frac{\gamma}{\delta}$ amb $\gamma, \delta \in A$ coprimers, llavors $\delta f(x) = \gamma a_0(x)b_0(x)$, com que la banda de l'esquerra està a $A[x]$ la dreta també. Així que tenim que $\delta = c(\delta f(x)) = c(\gamma a_0(x)b_0(x)) = \gamma$ i per tant, podem escriure $f(x) = a_0(x)b_0(x)$. Però al ser f irreductible en $A[x]$: o bé, $a_0(x) \in A[x]^* = A^*$ (llavors el grau de a_0 és 0), o bé $b_0(x) \in A[x]^* = A^*$ (llavors el grau de b_0 és 0) i, per tant, f també és irreductible en $K[x]$. □

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

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

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

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

2.11 Criteris d'irreductibilitat.

Sigui A un anell factorial i $K = \mathrm{Fr}(A)$.

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

Demostració. Tenim que $f(\alpha) = 0 \implies a_0v^n + a_1v^{n-1}u + \cdots + a_{n-1}vu^{n-1} + a_nu^n = 0$. Com que $v|a_0v^n + \cdots + a_{n-1}vu^{n-1}$ i $a_nu^n = -(a_0v^n + \cdots + a_{n-1}vu^{n-1})$, llavors $v|a_nu^n$ i com que u, v són coprimers $v|a_n$.
Anàlogament s'obté $u|a_0$. □

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

Demostració. Podem suposar que $f(x)$ és primitiu i demostrarem que és irreductible en $A[x]$. Suposem que tenim una descomposició de $f(x) = q(x)h(x)$ amb $q(x) = \sum_{i=0}^{r} b_ix^i$ i $h(x) = \sum_{i=0}^{s} c_ix^i$, on $r \geq 1$ i $s \geq 1$. Com que f primitiu, g i h són primitius.
Tenim que $a_0 = b_0c_0$ i $p|a_0$ i $p^2 \nmid a_0$. Llavors podem suposar que $p|c_0$ però $p \nmid b_0$. Com que $p \nmid a_n$ tenim que $p \nmid c_s$. Ara sigui $t = \min\{j : p \nmid c_j\} \leq s < r + s = n$ (que ha d'existir perquè h és primitiu). Com que tenim $a_t = b_0c_t + b_1c_{t-1} + \cdots + b_tc_0$, amb p que divideix a a_t i divideix a $c_0, \cdots, c_{t-1}$, per tant, divideix a b_0c_t però com que no divideix a b_0 ha de dividir a c_t, contradicció amb que t és el mínim tal que $p \nmid c_t$, per tant, o bé q o bé h tenen grau 0 i, per tant, són unitats, així que $f(x)$ és irreductible. □

Exemple 2.11.1. El polinomi en els enters $f(x) = x^4 - 4x^2 + 6x - 18$ és 2-Eisenstein i, per tant, és irreductible.

Lema 2.11.3. Extensió de morfismes a l'anell de polinomis. Siguin A, B dos anells qualssevol i sigui $f : A \to B$ un morfisme. Aleshores,

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

és un morfisme d'anells.

Demostració. Tenim que $\tilde{f}(1_A) = f(1_A) = 1_B$ que és l'element neutre de $B[x]$.
Siguin $p, q \in A[x]$, $p = a_0 + a_1 x + \ldots + a_n x^n$ i $q = b_0 + b_1 x + \ldots + b_m x^m$. Ara

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

I

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

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

Aleshores, és un morfisme d'anells. □

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

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

Aleshores, $f(x)$ és irreductible.

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

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

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

Exemple 2.11.2. Per veure que el polinomi en els enters $f(x) = x^2 + 3x - 11$ és irreductible, podem considerar φ que envia a les classes d'equivalència mòdul 3. En aquest anell $\tilde{\varphi}(f(x)) = x^2 + 1$ és irreductible, aleshores $f(x)$ també ho és. Per altra banda, podem considerar el polinomi $f(x) = x^5 + 2x + 6$, que mòdul 5 és $f(x) \equiv (x^4 + 3x^3 + 4x^2 + 2x + 3)(x + 2)$ i mòdul 11 $f(x) \equiv (x^3 + 8x^2 + 6x + 2)(x^2 + 3x + 2)$, on cada un dels factors són irreductibles. Llavors f és irreductible perquè les descomposicions són incompatibles per grau.

Capítol 3

Cossos

3.1 Motivació

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

Exemple 3.1.1. Sigui $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}\}$, aquest anell és un cos perquè és isomorf a $\mathbb{Q}[x]/(x^3 - 2)$, ja que $x^3 - 2$ és irreductible a $\mathbb{Q}$ (2-Eiseinstein) i, per tant, l'ideal és maximal i el quocient és un cos. A més, podem veure-ho com un espai vectorial: $\mathbb{Q}\langle 1, \sqrt[3]{2}, \sqrt[3]{4}\rangle$, $3 = \dim Q[\sqrt[3]{2}]$.

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

És $\mathbb{Q}[\pi]$ un cos? Ho és si, i només si $a \in \mathbb{Q}[\pi]$ tal que $a\pi = 1$, reordenant, només passa si existeix algun $f(x) \in \mathbb{Q}[\pi]$ tal que $f(\pi) = 0$. És a dir, si existeix un polinomi amb coeficients a $\mathbb{Q}$ tal que tingui una arrel a π. Que és un dels temes d'interès d'aquest capítol.

3.2 Extensió d'un cos

Definició 3.2.1. Direm que el cos F és una extensió del cos K si $K \subset F$ i tenen el mateix neutre, és a dir, si K és un subcòs de F. Ho denotarem com F/K. En aquesta situació tenim una aplicació.

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

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

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

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

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

Exemple 3.2.1. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{R}\langle 1, i\rangle$. Com que $1, i$ són $\mathbb{R}$-l.i. Llavors $[\mathbb{C} : \mathbb{R}] = 2$.

El cos $\mathbb{Q}(x_1, x_2, x_3, \ldots)$ (polinomis d'infinites variables) és una extensió infinita de $\mathbb{Q}$. Si hi hagués una base finita d'aquesta extensió involucra una quantitat finita de x_i.

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

Demostració.

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

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

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

Podem escriure-ho com:

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

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

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

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

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

3.3 Algebraic i transcendent

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

Exemple 3.3.1. $\sqrt{2}$ és algebraic sobre $\mathbb{Q}$ perquè $f(x) = x^2 - 2$ compleix que $f(\sqrt{2}) = 0$. π és algebraic sobre $\mathbb{R}$ però no sobre $\mathbb{Q}$.

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

Observació 3.3.3. El polinomi irreductible és únic.

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

Proposició 3.3.4. Podem caracteritzar el polinomi irreductible d'una altra manera: anem a considerar l'aplicació

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

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

Demostració.

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

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

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

i F és un cos, en particular, tenim que és íntegre, per tant, $\mathrm{Im}\, \varphi_\alpha$ és íntegre, llavors $p(x)$ és primer i com estem en $K[x]$ que és un euclidià, en particular, factorial, primer és el mateix que irreductible. Pel que hem vist abans, com que $\mathrm{Irr}(\alpha, K, x)$ ha de dividir a tots els polinomis que s'anul·len a α, si tenim un polinomi irreductible mònic que s'anul·la a α ja hem trobat $\mathrm{Irr}(\alpha, K, x)$. □

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

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

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

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

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

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

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

Demostració.

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

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

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

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

Lema 3.3.8. Sigui $L/M/K$ extensió de cossos, aleshores

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

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

Proposició 3.3.9. Sigui L/K una extensió de cossos, si α, β són algebraics sobre $/K$, llavors $\alpha \pm \beta$, $\alpha\beta$, α/β són tots algebraics sobre K.

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

3.4 Aplicacions lineals entre extensions

Definició 3.4.1. Fixem una K-base $w_1, \ldots, w_n$ de L. Donat $\alpha \in L$ considerem l'aplicació

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

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

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

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

Proposició 3.4.2. L'aplicació

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

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

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

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

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

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

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

Partint que estem en un cos commutatiu tenim que $w_\alpha \circ w_\beta = w_{\alpha\beta} = w_\beta \circ w_\alpha$ i el mateix per matrius, $M_\alpha M_\beta = M_{\alpha\beta} = M_\beta M_\alpha$, així que el producte commuta. □

Corol·lari 3.4.3. Si $\alpha = \sum \lambda_i w_i$, aleshores $M_\alpha = \sum \lambda_i M_{w_i}$.

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

Proposició 3.4.4. El polinomi $\mathrm{Irr}(\alpha, K, x)$ coincideix amb el polinomi mínim de M_α. En particular, els VAP's de M_α són les arrels de $\mathrm{Irr}(\alpha, K, x)$.

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

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

3.5 Teorema de l'element primitiu

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

Exemple 3.5.1. Tenim que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ i volem saber de quin grau és $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

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

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

Lema 3.5.1. Si $\mathrm{char}\, K = 0$ tot polinomi irreductible $/K$ és separable (té totes les arrels diferents).

Demostració. Suposem que $f(x) \in K[x]$ és un polinomi irreductible amb una arrel doble i $f'(x)$ la seva derivada. Tenim que

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

tindrà grau major o igual que 1 (perquè els dos tenen almenys una arrel en comú). Però com que f és irreductible, tenim que $h(x)|f(x) \implies h(x) = f(x)$ llavors $f(x) = h(x)|f'(x)$. Però com que el grau de $f'(x)$ és més petit estricte que el grau de $f(x)$, la derivada ha de ser 0. Ara utilitzem que al ser K de característica 0, si la derivada és de grau $n-1$, només pot ser que l'original sigui de grau n (altrament la característica seria finita). Aleshores, $f(x)$ és una constant, així que no pot tenir una arrel doble. □

Teorema 3.5.2. Teorema de l'element primitiu. Sigui K un cos amb $\operatorname{char} K = 0$ i sigui L/K una extensió finita. Llavors, existeix un element $\gamma \in L$ tal que $L = K(\gamma)$. És a dir, L és el cos generat per K i γ.

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

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

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

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

Nota. Més endavant veurem que existeix una versió del teorema de l'element primitiu per extensions finites de cossos finits.

3.6 Arrels de polinomis

Proposició 3.6.1. Sigui K cos qualsevol i sigui $p(x) \in K[x]$ irreductible. Existeix una extensió L/K finita en la qual $p(x)$ té una arrel.

Demostració. Si $\deg p(x) = 1$ és un polinomi lineal i l'arrel està sobre K, trivialment $L = K$. En cas contrari considerem

$$L := K[x]/(p(x))$$

Anem a veure que L és un cos. Com que $K[x]$ és principal i $p(x)$ és irreductible, tenim que $(p(x))$ és maximal, per tant, L és un cos. Tenim que la projecció

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

és un morfisme d'anells. Podem incloure K dins de L via l'aplicació

$$\begin{array}{ccccc} \iota : K & \longhookrightarrow & K[x] & \longhookrightarrow & L \\ a & \longmapsto & a & \longmapsto & \overline{a} \end{array}$$

que està clar que és un morfisme i és injectiva perquè si $\iota(a) = \iota(b)$ tindriem dues constants les quals difereixen d'un múltiple de $p(x)$, que per grau, el múltiple ha de ser 0, llavors $a = b$. Això ens permet identificar K amb un subcòs de L i, per tant, veure L com a una extensió de K. Per tant, es pot pensar que $p(X) \in L[X]$ i anem a veure que $p(X)$ té una arrel en L. Considerem $\overline{x}$ i veiem que és una arrel de p:

$$p(X) = \sum_{i=0}^{n} \overline{a_i} X^i \quad a_i \in K \quad \overline{a_i} \in \iota(K) \subset L$$

$$p(\overline{x}) = \sum_{i=0}^{n} \overline{a_i}\, \overline{x}^i = \sum_{i=0}^{n} \overline{a_i x^i} = \overline{\sum_{i=0}^{n} a_i x^i} = \overline{p(x)} = \overline{0}$$

Aleshores L/K és una extensió finita i podem escriure $L = K\langle 1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1} \rangle$. □

Teorema 3.6.2. Teorema de Kronecker. Sigui K un cos qualsevol i sigui $p(x) \in K[x]$ qualsevol. Aleshores existeix una extensió finita L/K en la qual $p(x)$ descompon en factors lineals (té totes les arrels a L).

Demostració. Agafem $p(x)$ i fem la descomposició en factors irreductibles, si algun d'ells no és lineal apliquem la proposició anterior per trobar un cos on aquell factor sí té una arrel. Ara, fem la descomposició del polinomi en aquest cos i ara tenim que el factor s'ha reduït el grau almenys en un i el nombre de factors irreductibles ha augmentat en almenys un. Anem fent fins que tinguem un cos on $p(x)$ descompongui en $\deg p(x)$ factors i, per tant, tots ells siguin lineals.

El cos el qual haguem arribat és una extensió finita de K perquè hem fet com a molt $\deg p(x)$ extensions finites. □

Definició 3.6.3. Un cos de descomposició de $f(x) \in K[x]$ és una extensió L/K en la qual $f(x)$ descompon en un producte de factors lineals i que és minimal amb aquesta propietat. K_f denotarà sempre un cos de descomposició de f sobre K (llevat d'isomorfisme). Fixem-nos que K_f depèn de f i de K.

Nota. S'ha d'entendre la propietat de ser minimal com: si existeix una altre extensió M/K on f descompon completament, aleshores existeix un morfisme injectiu de L a M. D'aquesta manera es veu que si el cos de descomposició existeix és únic llevat d'isomorfisme. Ja que si dos extensions L, L' són minimals amb aquesta propietat, aleshores existeixen dues injeccions una d'L a L' i l'altre d'L' a L, llavors els cossos són isomorfs.

Definició 3.6.4. Siguin $K \subset M$, $L \subset M$ subcossos del cos M. Definirem la combinació de cossos KL com el menor subcòs de M que conté K i L.

Lema 3.6.5. $\forall f, g \in K[x]$. si existeixen K_f, K_g, 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}, llavors tenim $K_f \hookrightarrow K_{fg}$. Per tant, podem veure-ho com $K_f \subset K_{fg}$.
2. $K_f \subset K_{fg}$ i $K_g \subset K_{fg}$, tenim que $K_f K_g \subset K_{fg}$. Però com que fg descompon en factors lineals a $K_f K_g$, $K_{fg} \subset K_f K_g$.

□

Proposició 3.6.6. $f \in K[x]$ irreductible. L/K una extensió qualsevol on $f(x)$ descompon linealment.

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_r) \qquad \alpha_i \in L$$

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

Demostració. Per descomptat f descompon completament a $K(\alpha_1, \dots, \alpha_n)$. Sigui M/K una altra extensió on f descompon en termes lineals

$$f(x) = a(x - \beta_1)(x - \beta_2) \dots (x - \beta_n) \qquad \beta_i \in M$$

Volem veure que existeix una injecció de $K(\alpha_1, \dots, \alpha_n)$ a M i aplicarem inducció sobre el $\deg f = n$.

Per $n = 1$, és el cas en que f descompon en un factor lineal, llavors $K(\alpha_1) = K$. Aquí, la injecció $K \hookrightarrow M$ és l'identitat perquè M és una extensió de K.

Per $n > 1$, comencem fent el següent

$$\begin{aligned} \iota : K(\alpha_1) &\longhookrightarrow M \\ \alpha_1 &\longmapsto \beta_1 \\ \sum a_i \alpha_1^i &\longmapsto \sum a_i \beta_1^i \end{aligned}$$

Dins de $K(\alpha_1)$ tenim una descomposició en irreductibles $f = \widetilde{f_1} \cdot \widetilde{f_2} \cdot \ldots \cdot \widetilde{f_s}$ alguns dels quals són no lineals, la suma dels graus d'aquests últims és menor que el grau de f.

Fixem-nos que a $\iota(K(\alpha_i))$ hi ha les mateixes β_j que α_j a $K(\alpha_1)$ i a més estan identificades. És a dir, si α_j és igual a un cert polinomi en α_1 amb coeficients a K, llavors la seva imatge per ι és un cert polinomi per β_1 i si $f(\alpha_i)$ és 0, per morfisme, $f(\iota(\alpha_i)) = \iota(f(\alpha_i)) = 0$. I al revés, si hi ha una combinació de β_1 que és 0, la mateixa val per α_1. En general, f descompon amb els mateixos irreductibles a $K(\alpha_1)$ com a $\operatorname{Im} K(\alpha_1)$.

Ara, per a cada polinomi irreductible $\widetilde{f_j}$ que ens ha quedat fem el següent: si ja és lineal, ja tenim que $K(\alpha_1)$ és el seu cos de descomposició, sinó agafem una de les seves arrels $\alpha_k (\notin K(\alpha_1))$ i fem el mateix que abans. Ara però, enviant-la a una de les arrels β_k que anul·la al mateix polinomi irreductible dins de $\operatorname{Im} K(\alpha_1)$. Fixem-nos que estem separant les β en diferents sacs, cada un correponent a un polinomi irreductible $\widetilde{f_j}$. És a dir, per a cada polinomi irreductible que no està descomposat en termes lineals tornaríem a fer una altra injecció

$$\begin{aligned} (K(\alpha_1, \alpha_k) =) K(\alpha_1)(\alpha_k) &\hookrightarrow M \\ \alpha_k &\longmapsto \beta_k \\ \sum a_i \alpha_k^i &\longmapsto \sum a_k \beta_k^i \end{aligned}$$

Per hipotesi d'inducció, com que cada vegada hi ha menys irreductibles i el grau d'aquests arriba a 1 aquest procés ens portaria a tenir una injecció per cada polinomi irreductible cap a M. I com que aquest és arbitrari i també pot ser vist com una extensió de $K(\alpha_1)$, tenim que cada un és el cos de descomposició del seu polinomi irreductible original sobre $K(\alpha_1)$.

La combinació de tots ells és $K(\alpha_1)(\alpha_1, \alpha_2, \ldots, \alpha_n)$ perquè és el menor cos que els conté tots i hi ha d'haver totes les arrels. Pel lema anterior, aquesta combinació és el cos de descomposició del producte d'irreductibles. En definitiva, $K(\alpha_1)(\alpha_1, \alpha_2, \ldots, \alpha_n)$ és el cos de descomposició de f sobre $K(\alpha_1)$. I per definició de cos de descomposició de f, com que f també descompon sobre M, tenim una injecció

$$K(\alpha_1)(\alpha_1, \alpha_2, \ldots, \alpha_n) \hookrightarrow M$$

Però com que

$$K(\alpha_1)(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

hem vist que existeix un injecció de $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ cap a M i, com que ho hem fet per M arbitrari, $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ és el cos de descomposició de f sobre K. □

Corol·lari 3.6.7. Tot polinomi $f \in K[x]$ té un cos de descomposició.

Exemple 3.6.1. $K = \mathbb{Q}$ $f(x) = x^3 - 2$, $\sqrt[3]{2}$ a l'única arrel real d'f. I $w = e^{2\pi i/3}$. Llavors $\mathbb{Q}_f = \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, w)$.

3.7 Extensions normals

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

Exemple 3.7.1. K/K és una extensió normal per qualsevol polinomi lineal. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ és una extensió normal de, per exemple, $f(x) = (x^2 - 2)(x^2 - 3)$. És $\mathbb{Q}(\sqrt[3]{2})$ normal? Doncs no.

Proposició 3.7.2. Sigui L/K una extensió normal i $f(x) \in K[x]$ irreductible. Si $f(x)$ té una arrel en L, les hi té totes.

Demostració. Sabem que $L = K_\varphi$ és un cos de descomposició d'un polinomi $\varphi(x) \in K[x]$. Sigui α una arrel de f en L i considerem $\beta \in L_f$ una altra arrel de f diferent de α, suposant que no està en L. Considerem ara $L(\beta) = K_\varphi(\beta)$ (pensant $\varphi \in K(\beta)[x]$), llavors $L(\beta)$ és el menor cos on φ descompon linealment i conté β. I també, $L = L(\alpha) = K_\varphi(\alpha)$. Però com que α i β són arrels del mateix polinomi irreductible f, tenim que $K(\alpha) \simeq K[x]/(f(x)) \simeq K(\beta)$, per la unicitat (llevat d'isomorfisme) del cos de descomposició, tenim

$$L = L(\alpha) = K_\varphi(\alpha) \simeq K_\varphi(\beta) = L(\beta)$$

És a dir $L \simeq L(\beta)$, llavors $\beta \in L$ o, més ben dit, la imatge de β per l'isomorfisme és una arrel d'f. □

Observació 3.7.3. Aquesta propietat caracteritza les extensions normals.

Proposició 3.7.4. L/K normal $\iff \forall f \in K[x]$ irreductible, f té una arrel en L les té totes.

Demostració.
$\Longrightarrow$) Ja l'hem demostrat.
$\Longleftarrow$) Anem a veure-ho només per cossos que compleixen les hipòtesis de l'element primitiu. Per aquest teorema, existeix un γ tal que $L = K(\gamma)$. Sigui $f(x) = \mathrm{Irr}(\gamma, K, x)$, llavors totes les arrels de f estan a L i, per tant, $L = K(\gamma) \subseteq K(\alpha, \beta, \gamma, \ldots) \subseteq L$, és a dir, $L = K_f$. □

Definició 3.7.5. Sigui K cos qualsevol, la clausura algebraica de K és una extensió $\overline{K}/K$ en la qual tot polinomi sobre K descompon linealment, i és minimal entre les extensions que compleixen aquesta propietat.

Observació 3.7.6. Clarament, si α algebraic $/K \implies \alpha \in \overline{K}$.

Teorema 3.7.7. Tot cos té una clausura algebraica que és única (llevat d'isomorfisme).

Demostració. La demostració és massa tècnica. □

Proposició 3.7.8. $\overline{Q}$ és numerable.

Demostració. Recordem que hi ha un bijecció entre $\mathbb{Q}_n[x] = \{f \in \mathbb{Q}[x] : \deg f \leq n\} \leftrightarrow \mathbb{Q}^{n+1}$, com que el segon és numerable, el primer ho és. I $\mathbb{Q}[x] = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n[x]$ unió numerable d'espais numerables, la qual és numerable (utilitzant l'axioma d'elecció). Ara definim per tot $f \in \mathbb{Q}[x]$, $Z(f) = \{\text{arrels de } f \text{ en } \mathbb{C}\}$, observem que $\#Z(f) < +\infty$.
Per tant, ens queda que $\overline{\mathbb{Q}} = \bigcup_{f\in\mathbb{Q}[x]} Z(f)$ unió numerable de conjunts finits. Llavors $\overline{\mathbb{Q}}$ és un conjunt numerable. □

Corol·lari 3.7.9. Ajuntant la proposició anterior amb que $\mathbb{C}$ és no numerable tenim que $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$ i que hi ha una infinitat no numerable de nombres transcendents sobre $\mathbb{Q}$.

3.8 Cossos finits

Definició 3.8.1. Sigui $p \in \mathbb{N}$ un primer, llavors denotarem $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ el cos finit de p elements. Anomenarem a aquests cossos finits, cossos primers.

Observació 3.8.2. Tot i que cossos finits de p elements n'hi ha infinits, veurem que tots seran isomorfs a $\mathbb{Z}/p\mathbb{Z}$.

Proposició 3.8.3. Sigui F un cos finit qualsevol i $m = \mathrm{char}(F)$, aleshores m és un nombre primer.

Demostració. Ho demostrarem de dues maneres diferents.
1. Recordem que

$$\begin{aligned} \iota : \mathbb{Z} &\longrightarrow F \\ a &\longmapsto a \cdot 1_F \end{aligned}$$

és un morfisme que compleix que $\ker \iota = (m)$. Aleshores, el quocient $\mathbb{Z}/(m) \hookrightarrow F$ és un anell íntegre (perquè F ho és), per tant, m primer.
2. Suposem que m el podem escriure com $m = pq$, amb $p, q > 1$. Aleshores, considerem la suma de m 1's, la qual ha de donar 0. La podem escriure com

$$0 = \overbrace{1 + 1 + \ldots + 1}^{m} = \overbrace{\overbrace{1 + \ldots + 1}^{p} + \cdots + \overbrace{1 + \ldots + 1}^{p}}^{q}$$

Definim $x = \overbrace{1 + \ldots + 1}^{p}$ i $y = \overbrace{1 + \ldots + 1}^{q}$. Ara, la igualtat d'abans la podem escriure com:

$$= \overbrace{x + \cdots + x}^{q} = x(\overbrace{1 + \cdots + 1}^{q}) = xy$$

que recordem que és 0, per tant, tenim que $xy = 0$. Però com que estem en un cos i els cossos són integres, o bé $x = 0$, o bé $y = 0$. Per tant, sumant només o bé p, o bé q, 1's arribem a 0, cosa que contradiu que la característica de F sigui m, ja que p i q són estrictament més petits que m. Per tant, arribem a que m ha de ser un nombre primer. □

Teorema 3.8.4. Sigui F un cos finit de característica p, aleshores podem veure F com una extensió de $\mathbb{F}_p$, amb $[F:\mathbb{F}_p] < \infty$ i el cardinal de F és una potència de p.

Demostració. Considerem l'aplicació $\varphi : \mathbb{F}_p \to F$ que envia l'1 a l'1 i s'extèn per la suma, és a dir,

$$\begin{array}{rccc} \varphi: & \mathbb{F}_p & \longrightarrow & F \\ & \overline{1} = [1] & \longmapsto & 1_F \\ & \overline{a} = [a] & \longmapsto & \underbrace{1 + \ldots + 1}_{a} \end{array}$$

que està ben definida perquè si $\overline{b} = \overline{a}$ tenim que $a = b + kp$, llavors quan fem $\varphi(b)$ cada p 1's que sumem donarà 0 i, per tant, $\varphi(b) = \varphi(a)$. A més, clarament compleix que l'1 va a l'1 i que $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\forall a, b \in \mathbb{F}_p$. I només falta comprovar que $\varphi(ab) = \varphi(a)\varphi(b)$ per tal que φ sigui un morfisme, però això es compleix perquè

$$\varphi(ab) = \overbrace{1 + \ldots + 1}^{ab} = (\overbrace{1 + \ldots + 1}^{a})(\overbrace{1 + \ldots + 1}^{b}) = \varphi(a)\varphi(b)$$

Llavors, φ és un morfisme. A més, és injectiu perquè si $\varphi(a) = \varphi(b)$ implica que a 1's donen el mateix que b 1's, per tant, $a - b$ 1's donen 0. Per tant, $a - b$ ha de ser un múltiple de p, així que a i b pertanyen a la mateixa classe de $\mathbb{F}_p$. En definitiva, tenim que $\varphi : \mathbb{F}_p \hookrightarrow F$, així que podem pensar $\mathbb{F}_p$ com un subconjunt de F. Direm que $\mathbb{F}_p$ serà el cos primer de F.

Ara que tenim una extensió de cossos, veure que l'extensió és finita és trivial perquè tots dos són cossos finits. Així que amb un nombre finit d'elements de F podem formar una $\mathbb{F}_p$-base de F: $\mathcal{B} = \{w_1, \ldots, w_n\}$ de $n = [F:\mathbb{F}_p]$ elements. Per tant, podem escriure F com:

$$F = \{a_1 w_1 + \ldots + a_n w_n : a_i \in \mathbb{F}_p\}$$

Com que tuples $(a_1, \ldots, a_n)$ diferents donen elements d'F diferents i tenim $p^n = p^{[F:\mathbb{F}_p]}$ tuples, el cardinal de F és aquesta mateixa potència de p. □

Corol·lari 3.8.5. Tot cos finit de p elements és isomorf a $\mathbb{F}_p$

Demostració. La mateixa φ del teorema anterior ens proporciona un isomorfisme perquè és injectiva entre dos conjunts amb el mateix nombre d'elements. □

Corol·lari 3.8.6. Els únics cardinals possibles dels cossos finits són potències de primers.

Demostració. Perquè el cardinal d'un cos finit és potència de la seva característica i hem vist que la característica d'un cos finit és sempre un nombre primer. □

Corol·lari 3.8.7. Si un cos finit F té cardinal p^r, aleshores $p = \operatorname{char} F$ i el seu cos primer és $\mathbb{F}_p$.

Demostració. Tenim que els cossos finits tenen característica primer i que el cardinal és potència d'aquesta característica, aleshores l'única possibilitat és que $p = \operatorname{char} F$, conseqüentment, pel propi teorema anterior: $\mathbb{F}_p$ és el seu cos primer. □

Corol·lari 3.8.8. Si F és un cos finit i H/F és una extensió finita, aleshores H és també un cos finit amb la mateixa característica de F i, en particular, $\#F | \#H$.

Demostració. Una extensió finita d'un cos finit ha de ser per força finita, perquè les combinacions d'elements de la base són finites. Siguin p i p^n la característica i el cardinal de F, respectivament. Tenim que, per ser H una extensió de F: $\#H = (\#F)^{[H:F]} = p^{n[H:F]}$. Aleshores, pel corol·lari anterior $\operatorname{char} H = p$. Clarament, el cardinal de F divideix al de H perquè $p^n | p^{n[H:F]}$. □

Exemple 3.8.1. Sigui $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$, $f(x)$ és irreductible/primer a $\mathbb{F}_3[x]$ perquè és de grau 2 i no té arrels ja que $f(0) = 1$, $f(1) = 2$, $f(2) = 2$, que són diferents de 0. Ara, considerem $F := \mathbb{F}_3[x]/(f(x))$, com que $f(x)$ és irreductible, $(f(x))$ és primer, per tant, maximal i finalment, F és un cos. Sigui $\alpha = \overline{x}$ (la classe de x mòdul $f(x)$), llavors

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

Que té exactament 9 elements. Fixem-nos que si $f(x)$ fos un polinomi irreductible de grau n, tindríem que

$$F = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{F}\}$$

Llavors, en aquest cas tindria 3^n elements.

3.9 Polinomis sobre cossos finits

Proposició 3.9.1. Sigui F un cos finit amb $\#F = q = p^r$ i sigui $f(x) \in F[x]$ un polinomi irreductible de grau n. Aleshores, $H = F[x]/(f(x))$ és un cos finit i $\#H = q^n = p^{rn}$.

Demostració. Que sigui un cos finit ve del fet que $(f(x))$ és maximal. Ara podem escriure $\alpha = \overline{x} \in H$, com que $H = F\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$, tenim que

$$H = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_i \in F\}$$

Aleshores, $[H : F] = n$ i $\#H = q^n = p^{rn}$. □

Exemple 3.9.1. Sigui $g(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$ que és irreductible perquè és de grau 2 i $g(0) = 2$, $g(1) = 1$ i $g(2) = 2$. Tenim:

$$G = \mathbb{F}_3[x]/(g(x)) = \mathbb{F}_3(\beta) = \{a_0 + a_1\beta : a_0, a_1 \in \mathbb{F}_3\}$$

Llavors $\#G = 9$, però compte perquè no és igual a $\mathbb{Z}/9\mathbb{Z}$ ja que aquest últim ni tant sols és íntegre. En canvi, podem considerar $F = \mathbb{F}_3[x]/(x^2 + 1) = \mathbb{F}_3(\alpha)$. Aleshores, fixem-nos en la següent aplicació:

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

que si fem $\varphi(\alpha^2 + 1) = (\beta - 1)^2 + 1 = \beta^2 - 2\beta + 1 + 1 = \beta^2 + \beta - 1 = 0$. Llavors φ està ben definida. Clarament és un morfisme bijectiu i, per tant, tenim un isomorfisme entre els dos cossos. En general, sempre tindrem un isomorfisme entre dos cossos finits de mateix cardinal.

Lema 3.9.2. Sigui F un cos finit amb $\#F = q = p^r$ i $\alpha \in F$, aleshores $\alpha^q = \alpha$.

Demostració. Nota: en el cas $r = 1$ tindríem el Petit Teorema de Fermat.

El cas que $\alpha = 0$ és trivial i el cas $\alpha \neq 0$ es tracta del Teorema de Lagrange de grups, però ho demostrarem igualment.

Considerem el conjunt de les potències de α, $A = \{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$. Fixem-nos que ha de contenir l'1 perquè al tenir un cos finit en algun punt es repetiran les potències i quan això passi $\alpha^l = \alpha^m$ tindrem que $\alpha^{l-m} = 1$. A la primera n que α^n sigui 1 li direm k. Volem veure que k divideix a $q - 1$, així tindrem que $\alpha^{q-1} = (\alpha^k)^t = 1^t = 1$.

Clarament a A no hi ha elements repetits. Si a A hi ha tots els elements $F \setminus \{0\}$ ja hem acabat. En canvi, si existeix un $\beta \in F \setminus \{0\}$ que no estigui a A, considerem el conjunt $\beta A = \{\beta, \beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^{k-1}\}$ i si encara queda algun element de $F \setminus \{0\}$ que no estigui en aquests subconjunts fem el mateix que amb β fins que acabem (que acabarem perquè $F \setminus \{0\}$ és finit). Aleshores, aquests conjunts són tots disjunts. En efecte, si hi hagués algun $\gamma\alpha^l = \delta\alpha^m$ (on δ l'hem triat a posteriori que γ), tindríem que $\gamma\alpha^{l-m} = \delta$. Llavors δ estaria en el conjunt γA i això no pot passar perquè a δ l'haurem triat tal que no estigui en els conjunts anteriors, per tant, els conjunts són tots disjunts i la unió fa el total. Així que, com que tots els conjunts tenen k elements i podem dir que tenim t conjunts, es complexi que $q - 1 = tk$, per tant, $k|q - 1$ i, en definitiva, $\alpha^q = \alpha\alpha^{q-1} = \alpha$, que és el que volíem veure. □

Corol·lari 3.9.3. A tota extensió de grau r de $\mathbb{F}_p$, el polinomi $/\mathbb{F}_p$, $\varphi_{p^r}(x) = x^{p^r} - x$ descompon completament.

Demostració. Per a tot α de l'extensió, pel lema anterior, $\alpha^{p^r} - \alpha = 0$. Aleshores α és una arrel de $\varphi_{p^r}(x)$. Així que

$$\prod_{\alpha \in \mathbb{F}_{p^r}} (x - \alpha) | \varphi_{p^r}(x)$$

Però com que φ_{p^r} té grau p^r, és mònic i tota extensió de grau r de $\mathbb{F}_p$ té p^r elements, es té que a l'extensió es compleix la igualtat

$$\prod_{\alpha\in\mathbb{F}_{p^r}}(x-\alpha)=\varphi_{p^r}(x)$$

Així que $\varphi_{p^r}(x)$ descompon completament. □

Teorema 3.9.4. Per a cada primer $p\in\mathbb{N}$ i per a cada $q=p^n$ existeix un cos finit de q elements, que és únic llevat d'isomorfisme. El denotarem genèricament per $\mathbb{F}_q$.

Demostració. Considerem $\mathbb{F}_q$ com el cos de descomposició del polinomi $\varphi_q(x)=x^q-x$ sobre $\mathbb{F}_p$. Agafem el subconjunt de q elements format per totes les arrels de φ_q (algunes d'elles estan a $\mathbb{F}_p$). Efectivament té q elements perquè $\varphi_q(x)$ és separable, ja que si considerem la derivada $\varphi_q'(x)=qx^{q-1}-1=-1\neq 0$, llavors $\varphi_q'(x)$ no té factors comuns amb $\varphi_q(x)$ i, per tant, $\varphi_q(x)$ no pot tenir arrels múltiples. Aquest subconjunt és realment un cos ja que és subcòs de $\mathbb{F}_q$. En efecte, el 0 i l'1 són arrels. Si a i b són arrels de $\varphi_q(x)$ (per tant, $a^q=a$ i $b^q=b$), aleshores $(a\pm b)^q=(a\pm b)^{p^n}=((a\pm b)^p)^{p^{n-1}}=(a^p\pm b^p)^{p^{n-1}}=\ldots=a^q\pm b^q=a\pm b$, llavors la suma i resta d'arrels és arrel. Fem $(ab)^q=a^qb^q=ab$, per tant, ab és també arrel. Per últim, prenem $b\neq 0$ i com que $b^q=b$ tenim que $b^{-q}=b^{-1}$, per tant, l'invers és arrel. En definitiva, $\mathbb{F}_q$, el cos de descomposició de $\varphi_q(x)$, és el conjunt de les seves arrels.

Pel corol·lari anterior, a tot cos de q elements F, el polinomi $\varphi_q(x)$ descompon completament. Aleshores, per definició de cos de descomposició existeix un morfisme injectiu de $\mathbb{F}_q$ a F, però com que els dos tenen el mateix nombre d'elements, es tracta d'un isomorfisme. □

Observació 3.9.5. Com s'ha vist a la demostració del teorema anterior $\mathbb{F}_{p^n}=\{\text{arrels de }\varphi_{p^n}(x)=x^{p^n}-x\}$ és el cos de descomposició de $x^{p^n}-x\in\mathbb{F}_p[x]$.

Observació 3.9.6. A la demostració del teorema anterior hem vist que el polinomi $x^{p^n}-x\in F_{p^n}[x]$ és separable, és a dir, totes les seves arrels són diferents.

Proposició 3.9.7. $\mathbb{F}_{p^n}\subseteq\mathbb{F}_{p^m}$ si i només si $n|m$.

Demostració.
$\Longrightarrow$) Suposem que $\mathbb{F}_{p^m}\subseteq\mathbb{F}_{p^n}$, ja hem vist algun cop que $\#\mathbb{F}_{p^n}=(\#\mathbb{F}_{p^m})^r$ per tant $p^n=(p^m)^r=p^{mr}$. Així que $n|m$.

$\Longleftarrow$) Suposem que $n|m$ i veiem que $\mathbb{F}_{p^n}\subseteq\mathbb{F}_{p^m}$. Sigui $r=m/n$ i sigui $\alpha\in\mathbb{F}_{p^n}$, hem de veure que $\alpha\in\mathbb{F}_{p^m}$, per la observació anterior, només ens fa falta veure que $\alpha^{p^m}-\alpha=0$. Per $\alpha=0$ és trivial. En cas contrari, sabem que $\alpha^{p^n-1}=1$ i podem escriure $p^m-1=(p^n)^r-1=(p^n-1)(1+p^n+p^{2n}+\ldots+p^{(r-1)n})$. Aleshores,

$$\alpha^{p^m-1}=\alpha^{(p^n-1)(1+p^n+p^{2n}+\ldots+p^{(r-1)n})}=(\alpha^{p^n-1})^{(1+p^n+p^{2n}+\ldots+p^{(r-1)n})}=1^{(1+p^n+p^{2n}+\ldots+p^{(r-1)n})}=1$$

Per tant, $\alpha^{p^m}-\alpha=0$ que és el que volíem veure. □

Observació 3.9.8. Sabent que les arrels de $x^{p^n}-x$ són els elements de $\mathbb{F}_{p^n}$ i que les de $x^{p^m}-x$ són els elements de $\mathbb{F}_{p^m}$. De la proposició anterior traiem que

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

Lema 3.9.9. Com que $F_p[x]$ és un anell euclidià, podem considerar la descomposició en irreductibles de $x^{p^n}-x\in F_p[x]$. Si $f(x)$ és un d'aquests irreductibles, aleshores el grau de $f(x)$ divideix a n.

Demostració. Com que $f(x)|x^{p^n}-x$, per una observació anterior, tenim que les arrels de $f(x)$ estan totes a F_{p^n} (ja que aquest és el conjunt de les arrels de $x^{p^n}-x$). Aleshores, considerem $\mathbb{F}_p(\alpha)$, on α és una arrel de $f(x)$, llavors $\alpha\in\mathbb{F}_{p^n}$, per tant, tenim que $\mathbb{F}_p(\alpha)\subseteq\mathbb{F}_{p^n}$. Com que α és algebraic $\mathbb{F}_p(\alpha)\simeq\mathbb{F}_p[x]/(f(x))$, que per una proposició anterior sabem que té cardinal p^d on d és el grau de $f(x)$, per tant, $\mathbb{F}_{p^d}\simeq\mathbb{F}_p(\alpha)$. Utilitzant una proposició anterior, com que $\mathbb{F}_{p^d}\simeq\mathbb{F}_p(\alpha)\subseteq F_{p^n}$ tenim que $d|n$, és a dir, el grau de $f(x)$ divideix a n. □

Proposició 3.9.10. Sigui $f(x)\in\mathbb{F}_p[x]$ un polinomi irreductible de grau d, aleshores el cos $\mathbb{F}_p[x]/(f(x))$ conté totes les arrels de $f(x)$. És a dir, $f(t)$ descomposa completament a $\mathbb{F}_p[x]/(f(x))[t]$.

Demostració. Fixem-nos que si a $\mathbb{F}_p[x]/(f(x))[t]$ substituim $t = x^{p^i}$ a $f(t)$ obtenim $f(x^{p^i}) = f(x)^{p^i} = 0^{p^i} = 0$, on hem utilitzat que si $f(x) = a_m x^m + \ldots + a_1 x + a_0$, aleshores

$$f(x)^{p^i} = (a_m x^m + \ldots + a_1 x + a_0)^{p^i} = a_m^{p^i}(x^{p^i})^m + \ldots + a_1^{p^i} x^{p^i} + a_0^{p^i}$$

Els productes de més d'un element se'n van perquè queden multiplicats per una constant múltiple de p i estem a un cos de característica p. A més, tenim que $a_k^{p^i} = (a_k^p)^{p^{i-1}} = a_k^{p^{i-1}} = \ldots = a_k$, per $0 \leq k \leq m$. Així, si continuem l'igualtat anterior tenim el que abans hem utilitzat $f(x)^{p^i} = \ldots = f(x^{p^i})$.

Així obtenim una arrel per a cada i natural, però a priori n'hi ha repetides i, de fet, sabem que n'hi ha d'haver menys de d. Anem a veure que per $0 \leq i \leq d-1$ les arrels que hem trobat són totes diferents. Suposem que dues arrels $x^{p^i} = x^{p^j}$ són iguals amb $i > j$. Com que aquests elements són classes de $\mathbb{F}_p[x]/(f(x))$, tenim que $f(x)$ ha de dividir als polinomis vists com elements de $\mathbb{F}_p[x]$: $x^{p^i} - x^{p^j} = (x^{p^{i-j}} - x)^{p^j}$, on estem tornant a utilitzar que els productes de més d'un element se'n van perquè queden multiplicats per p. Ara bé, per ser $f(x)$ irreductible, si ha de dividir a $(x^{p^{i-j}} - x)^{p^j}$ necessàriament, pel lema anterior, $d|i-j$, però com que $0 \leq i, j \leq d-1$ és impossible que això passi a menys que $i = j$. En definitiva, hem trobat d arrels diferents de $f(t)$ dins de $\mathbb{F}_p[x]/(f(x))$ (són de la forma x^{p^i}), com que f és de grau d no en pot tenir més, per tant, les hi té totes. □

Observació 3.9.11. Com hem vist a la demostració, el polinomis irreductibles de $\mathbb{F}_p[x]$ tenen sempre totes les arrels diferents, per tant, són separables.

Corol·lari 3.9.12. Si $f(x)$ és un polinomi irreductible de grau d amb coeficients a $\mathbb{F}_p$, aleshores, el seu cos de descomposició és $\mathbb{F}_{p^d}$.

Demostració. Sigui $(\mathbb{F}_p)_f$ el cos de descomposició de $f(x)$ a $\mathbb{F}_p$. Per la proposició anterior, $\mathbb{F}_p[x]/(f(x))$ té totes les arrels de $f(x)$, per tant, tenim que $(\mathbb{F}_p)_f \hookrightarrow \mathbb{F}_p[x]/(f(x))$. Per altra banda, si α és una arrel de $f(x)$ tenim que $\mathbb{F}_p(\alpha) \hookrightarrow (\mathbb{F}_p)_f$ perquè aquest últim les hi té totes. (Ambdues aplicacions són morfismes injectius de cossos). Ara, per propietats que ja hem vist, sabem que $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_p[x](f(x)) \simeq \mathbb{F}_{p^d}$, aleshores, ens queda que

$$\mathbb{F}_{p^d} \hookrightarrow (\mathbb{F}_p)_f \hookrightarrow \mathbb{F}_{p^d}$$

Que per estar en cossos finits, es tracta d'un isomorfisme entre cossos i, per tant, el cos de descomposició de $f(x)$ és $\mathbb{F}_{p^d}$.

El mateix raonament també té una versió en graus d'extensions. Ja que tenim una extensió de grau d amb totes les arrels, que és $\mathbb{F}_p[x]/(f(x))$ i qualsevol extensió de $\mathbb{F}_p$ que tingui almenys una arrel ja té grau d, per tant, el cos de descomposició és una extensió de grau d de $\mathbb{F}_p$, per unicitat, $\mathbb{F}_{p^d}$. □

Teorema 3.9.13. Es compleix que

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

i, per tant, els elements de $\mathbb{F}_{p^n}$ són les arrels de tots els polinomis irreductibles i mònics de grau $d|n$ de $\mathbb{F}_p$.

Demostració. Definim $H(x)$ com el polinomi descrit a la dreta de l'equació. Ara, anem a pensar en la descomposició en irreductibles de $x^{p^n} - x$ els quals els podem pensar com a mònics ja que el producte de totes les primeres components és 1. Aleshores sigui $g(x)$ un d'aquests irreductibles, per un lema anterior, grau de $g(x)$ divideix a n, aleshores $g(x)$ és un dels que hi ha a la dreta. És a dir, $g(x)|H(x)$, ara usant que les arrels de $x^{p^n} - x$ són totes diferents (per tant, els irreductibles en que descomposa també) i usant que polinomis irreductibles mònics diferents són no associats tenim que $x^{p^n} - x|H(x)$.

Suposem ara, que tenim un polinomi irreductible i mònic $f(x) \in \mathbb{F}_p[x]$ de grau $d|n$. Com que el cos de descomposició de $f(x)$ és $\mathbb{F}_{p^d}$ i com que $d|n$, tenim que $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Per tant, les arrels de $f(x)$ són elements de $\mathbb{F}_{p^d}$ que al seu temps, és el conjunt de les arrels de $x^{p^d} - x$, és a dir, totes les arrels de $f(x)$ ho són també de $x^{p^n} - x$ i, per tant, $f(x)|x^{p^n} - x$. Això mateix, també es pot veure usant que $f(x) = \text{Irr}(\alpha, \mathbb{F}_p, x)$ i usant que α és també una arrel de $x^{p^n} - x$, tenim que $f(x)|x^{p^n} - x$. A més, com que cap d'ells és associat amb cap altre, perquè són irreductibles mònics diferents, tenim que la multiplicació de tots ells divideix a $x^{p^n} - x$, és a dir, $H(x)|x^{p^n} - x$.

En definitiva, hem vist $x^{p^n} - x = H(x)$, és a dir, que si descomposem $x^{p^n} - x$ en irreductibles mònics, ens apareixeran tots els polinomis irreductibles mònics de $\mathbb{F}_p[x]$ amb grau que divideixi a n. □

Exemple 3.9.2. A $\mathbb{F}_3[x]$, aplicant el teorema anterior podem veure que els següents són els únics polinomis irreductibles mònics de grau 1 o 2 de $\mathbb{F}_3[x]$:

$$x^9 - x = x(x-1)(x-2)(x^2+1)(x^2+x-1)(x^2-x-1)$$

Corol·lari 3.9.14. A $\mathbb{F}_p$ hi ha $\frac{p^2-p}{2}$ polinomis irreductibles no associats de grau 2.

Demostració. Està clar que d'irreductibles no associats de grau 1 n'hi ha exactament p perquè és el nombre d'elements de $\mathbb{F}_p$, aleshores, utilitzant el teorema anterior el grau de $x^{p^2} - x$ és igual a $p + 2m$ on m és el nombre d'irreductibles mònics de grau 2. Aleshores $p^2 - p = 2m$, per tant, hi ha $(p^2-p)/2$ irreductibles no associats de grau 2 a $\mathbb{F}_p[x]$. □

Nota. En general, podem saber quants irreductibles tenim de qualsevol grau. La resposta involucra μ de Möbius.

3.10 Teorema de l'element primitiu per cossos finits

Proposició 3.10.1. Sigui K un cos, aleshores el conjunt $(K^*, \times)$ té estructura de grup commutatiu.

Demostració. Per definició K^* són els elements de K excepte el 0. Així que quan multipliquem dos elements de K^* ens quedarem a K^* perquè al ser K un cos, K és íntegre. De K hereda les altres propietats: l'element neutre, l'invers, l'associativitat i la commutativitat. □

Definició 3.10.2. Al conjunt K^* l'anomenarem grup multiplicatiu.

Definició 3.10.3. Sigui G un grup, direm que l'ordre d'un element $\alpha \in G$ és n si $\alpha^n = 1$ i $\alpha^i \neq 1$, per tot $1 \leq i \leq n-1$.

Teorema 3.10.4. El grup multiplicatiu d'un cos finit és cíclic. És a dir, $\exists \zeta \in \mathbb{F}_q^*$ tal que $\mathbb{F}_q^* = \langle \zeta \rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{q-1}\}$, per tant, l'ordre de ζ és $q-1$.

Demostració. Primer de tot, per aquesta demostració utilitzarem els següents resultats de grups que veurem més endavant:

- Sigui G un grup i $a \in G$, si $a^n = 1$, aleshores $\operatorname{ord} a | n$.
- Si tenim $a_1, \ldots, a_r$ elements d'un grup G que compleixen que l'ordre dels a_i són coprimers tots amb tots, aleshores l'ordre de la multiplicació és multiplicació d'ordres.

Comencem factoritzant $q - 1 = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ amb p_i primers i $\alpha_i > 0$. Per a cada p_i triem $y_i \in \mathbb{F}_q$ tal que $y_i^{\frac{q-1}{p_i}} \neq 1$. Fixem-nos que

$$x^{\frac{q-1}{p_i}} - 1 | x^{q-1} - 1 = (x^{\frac{q-1}{p_i}})^{p_i} - 1 = (x^{\frac{q-1}{p_i}} - 1)(1 + x^{\frac{q-1}{p_i}} + \ldots + (x^{\frac{q-1}{p_i}})^{p_i - 1})$$

On el grau del primer és menor que el grau del segon i sabem que les arrels del segon són els elments de $\mathbb{F}_q$ excepte el 0. Aleshores, hi ha almenys un element $y_i \in \mathbb{F}_q^*$ que no és arrel de $x^{\frac{q-1}{p_i}} - 1$.

Sigui $\zeta_i = y_i^{\frac{q-1}{p_i^{\alpha_i}}}$, anem a veure que l'ordre de ζ_i és $p_i^{\alpha_i}$. En efecte, està clar que $\zeta_i^{p_i^{\alpha_i}} = y_i^{q-1} = 1$. Ara, suposem que $\operatorname{ord} \zeta_i = n < p_i^{\alpha_i}$, en aquest cas tindríem que $n | p_i^{\alpha_i}$, per tant, $n = p_i^k$, per algun $k < \alpha_i$. Ara fixem-nos que si imposem que $1 = \zeta_i^{p_i^k} = y_i^{\frac{q-1}{p_i^{\alpha_i - k}}}$, elevant l'expressió a $p_i^{\alpha_i - k - 1} \geq 0$, ens queda $1 = y_i^{\frac{q-1}{p_i}}$, cosa que no pot ser perquè havíem escollit y_i perquè no complís això. Per tant, $k = \alpha_i$ i tenim que $\operatorname{ord} \zeta_i = p_i^{\alpha_i}$.

Sigui $\zeta = \zeta_1 \zeta_2 \ldots \zeta_r$, com que els ordre són coprimers, l'ordre de ζ és la multiplicació d'ordre i, per tant, $\operatorname{ord} \zeta = \prod p_i^{\alpha_i} = q - 1$. Així que si l'ordre de ζ és $q-1$ tenim que la col·lecció $\{1, \zeta, \ldots, \zeta^{q-1}\}$ són tots diferents i, pertanyen tots a $\mathbb{F}_p^*$ que té $q-1$ elements, així que $\mathbb{F}_q^* = \langle \zeta \rangle$. □

Corol·lari 3.10.5. Tot cos finit és una extensió simple del seu cos primer. Si $q = p^n$ (amb $n > 0$) i $\mathbb{F}_q^* = \langle \zeta \rangle$, llavors $\mathbb{F}_q = \mathbb{F}_p(\zeta)$.

Demostració. Clarament $\zeta \notin \mathbb{F}_p$, perquè $\zeta^{p-1} \neq 1$. Ara, tenim la cadena d'extensions $\mathbb{F}_q/\mathbb{F}_p(\zeta)/\mathbb{F}_p$, suposem que $[\mathbb{F}_p(\zeta) : \mathbb{F}_p] = r$ amb $r \leq n$. Sabem que $\#\mathbb{F}_p(\zeta) = p^r$ llavors tenim que $\zeta^{p^r-1} = 1$, però vist a dins de $\mathbb{F}_q$, $\text{ord}(\zeta) = q-1$ llavors $q-1|p^r-1$, és a dir, $p^n-1|p^r-1$, així que $n \leq r$. Per tant, $n = r$, aleshores el grau de l'extensió $[\mathbb{F}_q : \mathbb{F}_p(\zeta)] = 1$, llavors $\mathbb{F}_q = \mathbb{F}_p(\zeta)$. □

Corol·lari 3.10.6. Teorema de l'element primitiu per a cossos finits. Tota extensió finita d'un cos finit és simple.

Demostració. Com s'ha vist en una proposició de la secció anterior, tota extensió finita d'un cos finit és de la forma $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$, necessàriament pel mateix $q = p^r$. Llavors, per la proposició i el corol·lari anterior tenim que $\mathbb{F}_{q^n}^* = \langle\zeta\rangle$ i $\mathbb{F}_{q^n} = \mathbb{F}_p(\zeta)$. Fixem-nos que $\mathbb{F}_p(\zeta) \subseteq \mathbb{F}_{q^m}(\zeta) \subseteq \mathbb{F}_{q^n}$, però com que el primer i l'últim són iguals, tenim que $\mathbb{F}_{q^m}(\zeta) = \mathbb{F}_{q^n}$, és a dir, el mateix ζ serveix. □

3.11 Aplicacions dels cossos finits

Els cossos finits tenen moltes aplicacions, algunes de les més inmediates es troben en l'àmbit de la criptografia.

Intercanvi de claus de Diffie-Hellman.

Dos usuaris A i B volem acordar una clau comuna sense haver de transmetre-la explícitament.

Primer triem $q = p^r$ gran. Triem un generador g de $\mathbb{F}_q^*$ amb $\mathbb{F}_q^* = \langle g\rangle$. L'usuari A tria a l'atzar una $a \in \{1, \dots, q-1\}$ i calcula $u_A = g^a$. L'usuari B fa el mateix $b \in \{1, \dots, q-1\}$ $u_B = g^b$. Llavors A i B intercanvien les claus u_A, u_B, aleshores la clau comuna serà $k = g^{ab} = (u_A)^b = (u_B)^a$, llavors cada una pot calcular la clau.

Si un espia vol saber k, no la pot deduir si no sap a o b. Per què? Fixem-nos que tots els càlculs es fan dins de $\mathbb{F}_q$ i, per tant, deduir g^{ab} no és fàcil i cal el logaritme discret que és un problema que no es sap resoldre eficientment.

Problema de Diffie-Hellman: Donats q, g, g^a, g^b calcular g^{ab}. Actualment aquest problema és *NP-Hard*, és a dir, no es coneixen algoritmes polinòmics per resoldre aquest problema.

Criptosistema d'ElGamal

Triem un cos finit $\mathbb{F}_q$ amb $q \gg 0$ i $g \in \mathbb{F}_q^*$ tal que $\mathbb{F}_q^* = \langle g\rangle$. El criptosistema consistirà en identificar cada missatge natural amb un element de $\mathbb{F}_q^*$.

Per xifrar missatges: cal transformar $m \in \mathbb{F}_q^*$ en $\widetilde{m} \in \mathbb{F}_q^*$ de forma que: m es pugui recuperar a partir de $\widetilde{m}$, però només si se sap una clau secreta. A més, el xifrat de m a $\widetilde{m}$ i el seu desxifrat han de ser eficients.

Cada usuari A_i tria una clau secreta $S_i \in \{1, \dots, q-1\}$ (la tria preferentment a l'atzar) i comparteix la seva clau pública, és a dir, $P_i = g^{S_i}$. Si algú li vol enviar un missatge tria un altre exponent $k \in \{1, \dots, q-1\}$ (a l'atzar) i li envia el parell $\widetilde{m} = (g^k, (P_i)^k m)$. Fixem-nos que aquests càlculs els pot fer tothom, encara que no sàpiga S_i, ja que només fa servir la clau pública.

L'usuari A_i pot desxifrar el missatge, ja que

$$m = \frac{(P_i)^k m}{(P_i)^k} = \frac{(P_i)^k m}{(g^{S_i})^k} = \frac{(P_i)^k m}{(g^k)^{S_i}}$$

Tot i que A_i no sap k, d'aquest últim quocient ho sap tot, per tant, pot recuperar m.

Per altra banda, un espia no pot desxifrar el missatge si no sap $(g^k)^{S_i}$, encara que sàpiga g^{S_i}, perquè hauria de trobar $k = \log_g g^k = \log_{g^{S_i}} g^{kS_i}$ que és calcular el logaritme discret perquè aquests càlculs es fan a $\mathbb{F}_q$. La seguretat del criptosistmea d'ElGamal en basa en la dificultat computacional del problema del logaritme discret en $\mathbb{F}_q^*$, per $q \gg 0$.

La segurar d'aquest criptosistema es pot reduir a la del protocol de Diffie-Hellman.

Codi corrector d'errors

Ara l'objectiu és detectar i intentar corregir errors de transimissió de missatges.

Suposem que tenim un número finit de missatges. Per exemple, paraules de 8 lletres, cada lletra configurada en el codi ASCII, llavors hi ha 2^{64} missatges possibles. Identificarem cada paraula amb un element de $\mathbb{F}_{2^{64}}$, però de la següent manera, triem $n > 0$ i a l'espai vectorial $\mathbb{F}_2^n$ triem un subespai V de dimensió 64, de forma que $\#V = 2^{64}$. Triant una base de V, hi ha un isomorfisme d'espais vectorials $\mathbb{F}_{2^{64}} \simeq V$. Pensarem els missatges com elements de V. Trobaré equacions de V, llavors $V = \{$ solucions d'un sistema lineal homogeni $\}$. Com que els missatges seran elements de V, determinar si $x \in \mathbb{F}_{2^n}$ és un missatge original o no, és mirar si x satisfà les equacions de V.

Per exemple, a $\mathbb{F}_{2^{64}}^3$ podriem prendre

$$V = \{(x, y, z) \in \mathbb{F}_{2^{64}}^3 : x = y = z\} = \{(m, m, m) : m \in \mathbb{F}_{2^{64}}\}$$

En aquest cas codifiquem un missatge repetint-lo tres cops. Aquesta codificació és bastant segura però cara.

Definim n com la longitud del codi, k com la dimensió del codi, k/n la ratio del codi. Definim el pes de Hamming:

$$\begin{array}{rccc} w: & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{N} \\ & v = (a_1, \ldots, a_n) & \longmapsto & w(v) = \#\{i : a_i \neq 0\} \end{array}$$

I definim $d(V) = \min\{w(v) : v \in V \setminus \{0\}\}$ com la distància minimal en V. Al seu torn, $d(V)$, per ser V e.v., es pot pensar com la menor distància entre dos elements de V.

Aleshores, si s'ha enviat un missatge m, però hem rebut $r \in V$ canviem r pel $c \in V$ tal que $w(r-c)$ minimal. L'objectiu seria que sempre passés que $w(r-m) < d(V)/2$, d'aquesta manera r tindria menys que $d(V)/2$ bits incorrectes, llavors escolliriem $c = m$, i per tant, haurem pogut corregir els errors.

En definitiva, ens interessa que $d(V)$ sigui gran per poder controlar millor els errors, però segurament augmentarem significativament la ratio del codi fent que cada cop sigui més difícil computacionalment corregir els errors. Aleshores, s'ha d'escollir bé la k i la V per tenir un bon equilibri entre aquestes dues magnituds.

Esquemes per compartir secrets de Shamir

Volem compartir un secret $s \in \mathbb{F}_p$ entre n persones de forma que calgui almenys t persones per reconstruir-lo.

Triem $p \gg n$, construim a l'atzar un polinomi $H(x) \in \mathbb{F}_p[x]$ tal que tingui grau com a molt $t-1$ i $H(0) = s$. Per a cada usuari triem un element $x_1, \ldots, x_n \in \mathbb{F}_p$ a l'atzar i calculem $s_i = H(x_i)$. A cada participant li enviem un parell (x_i, s_i).

Per tal de recuperar el missatge cal trobar $H(x)$ i, per tant, cal interpolar els punts (x_i, s_i). Com que $H(x)$ té grau t, necessitem t punts, és a dir, calen t participants. Amb com a molt $t-1$ no es pot determinar unívocament $H(x)$ i, per tant, no es pot deduir el secret.

3.12 Cossos ordenats

Definició 3.12.1. Un conjunt X es diu que és totalment ordenat o que té un ordre total si existeix una relació binària "$\leq$" tal que sigui antisimètrica, transitiva i total. És a dir, $\forall a, b, c \in X$ es té

1. Antisimetria. Si $a \leq b$ i $b \leq a$, aleshores $a = b$.
2. Transitivitat. Si $a \leq b$ i $b \leq c$, aleshores $a \leq c$.
3. Totalitat. O bé, $a \leq b$, o bé $b \leq a$.

També es pot afegir l'ordre total estricte "$<$" com:

4. $a < b$ si, i només si, $a \leq b$ i $a \neq b$.

Definició 3.12.2. Un anell ordenat és un anell A amb una relació "$<$" d'ordre total compatible amb les operacions d'A. $\forall x, y, x', y' \in A$:

1. Si $x > x'$, $y > y'$, aleshores $x + y > x' + y'$.
2. Si $x > 0, y > 0$, aleshores $xy > 0$.

Proposició 3.12.3. Donar "$>$" equival a donar el seu "con positiu", és a dir,

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

tal que $A = A_>^+ \sqcup \{0\} \sqcup (-A_>^+)$ i és tancat per la suma i el producte. D'aquesta manera, podem parlar de positiu, el zero i negatius, respectivament.

Demostració. Donat un ordre, està clar qui forma el conjunt $A^+_>$ i donat un con positiu, es pot definir l'ordre com $x > y$ si, i només si, $x - y \in A^+_>$. □

Lema 3.12.4. Si A és un anell ordenat

1. A íntegre i $\operatorname{char} A = 0$.
2. $\forall A \setminus \{0\}$, $x^2 > 0$. En particular, $1 > 0$.

Demostració. Siguin $x, y \in A \setminus \{0\}$. Podem suposar que $x > 0$ i $y > 0$ (els altres casos es fan treient el signe) i, per la propietat 2 $xy > 0$, així que $xy \neq 0$, per tant A és íntegre.

Si considerem el cas anterior, amb $y = x$ tenim que $x^2 = 0$ (podent ser x positiu o negatiu). En particular, $x = 1$ tenim $1 > 0$. Per tant, per la propietat 1 i inducció, tenim que $n1_A > 0$, cosa que ens diu que $n1_A \neq 0$, per tot n. Aleshores, $\operatorname{char} A = 0$. □

Corol·lari 3.12.5. No és possible definir un ordre complet a $\mathbb{C}$.

Demostració. Suposem que tenim un ordre complet. Pel lema anterior $-1 = i^2 > 0$, però, $0 = 1 + (-1) > 0 + (-1) = -1$, com no poden passar les dues coses alhora, contradicció. □

Proposició 3.12.6. Si A és ordenat, l'ordre en A s'estén de manera única al seu cos de fraccions $K = \operatorname{Fr}(A)$. Quan diem que s'estén volem dir que si $a, b \in A$ compleixen que $a < b$ aleshores, quan els mirem dintre de K, la desigualtat és la mateixa.

Demostració. Definim

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

I, per un proposició anterior, sabem que això defineix l'ordre en K, $x >_K y \iff x - y \in K^+$. Fixem-nos que si existeix un altre ordre en K haurà de verificar que $\frac{a}{b} > \frac{c}{d}$ si, i només si, $\frac{x}{y} = \frac{ad-bc}{bd} > 0$ que es compleix, si i només si, $xy = \frac{x}{y}y^2 > 0$ i com que aquest últim pertany a A, es té que $\frac{x}{y} \in K^+$, és a dir, $\frac{x}{y} >_K 0$, per tant, $\frac{a}{b} > \frac{c}{d}$. Com que ho hem fet per dos elements de K qualssevol, es tracta del mateix ordre i, per tant, és únic. □

Proposició 3.12.7. $\mathbb{Z}$ admet un únic ordre.

Demostració. Ja hem vist que $1 > 0$ i per inducció $\forall n \in \mathbb{N} \setminus \{0\}$, $n1 > 0$ i a tots aquests nombres els anomenem $\mathbb{Z}^+$. Clarament està tancat per la suma i multiplicació i tenim $\mathbb{Z}^+ \sqcup \{0\}^{\sqcup} - \mathbb{Z}^+$. Aleshores, tenim definit un ordre, $x > y$ si, i només si $x - y \in \mathbb{Z}^+$. Per construcció és únic perquè tots els passos han sigut obligats. □

3.13 Completació de cossos ordenats

Definició 3.13.1. Sigui K un cos ordenat, el valor absolut $a \in K$ és $|a|_K := \max\{-a, a\}$.

Proposició 3.13.2. El valor absolut satisfà

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

Demostració.

1. Sabem que, o bé $a \in K^+$ o bé $-a \in K^+$, aleshores un dels dos és positiu (i l'altre no), per tant, el més gran és positiu.
2. En definitiva, tot element de $x \in K$ negatiu es pot posar com $-y$ on $y = -x = |x| \in K^+$. Aleshores, fer valor absolut és treure el signe, per tant, tant $|ab|$ com $|a||b|$ és la multiplicació sense signes dels elements.

3. Si a, b tenen el mateix signe es compleix la igualtat. Si $a < 0$ i $b > 0$ tenim que $|a+b| = \max\{a+b, -a-b\} \leq \max\{b, -a\} \leq |a|_K + |b|_K$.

□

Definició 3.13.3. Direm que una successió $(a_n)_{n\geq 1}$ d'elements de K és una successió de Cauchy si $\forall \varepsilon \in K^+$, $\exists n_0 \geq 1$ tal que $\forall m, n \geq n_0$ es compleix que $|a_m - a_n|_K < \varepsilon$.

Definició 3.13.4. Direm que una successió $(a_n)_n$ d'elements en K convergeix a $L \in K$ si $\forall \varepsilon \in K^+$, $\exists n_0 \in \mathbb{N}$ tal que $\forall n \geq n_0$ es compleix que $|a_n - L|_K < \varepsilon$.

Definició 3.13.5. Anomenarem $SC(K) = \{(a_n)_n$ successions de Cauchy a $K\}$. $SCV(K) = \{(a_n)_n : \exists L \in K$ tal que $(a_n)_n \to L\}$. En particular, $S_0(K) = \{(a_n)_n : (a_n)_n \to 0\}$.

Proposició 3.13.6. Tota successió convergent és de Cauchy. És a dir, $SCV(K) \subseteq SC(V)$.

Demostració. Sigui (a_n) una successió convergent amb límit a, aleshores, per a cada $\varepsilon \in K^+$ existeix un nombre natural n_0 tal que

$$|a_n - a| < \frac{\varepsilon}{2} \qquad \forall n \geq n_0$$

Aleshores, per tot $p, q \geq n_0$ es té

$$|a_p - a_q| \leq |a_p - a| + |a_q - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

per tant, (a_n) és una successió de Cauchy a K. □

Observació 3.13.7. Per un K qualsevol, no tota successió de Cauchy és convergent.

Demostració. (Sense entrar en tots els detalls) A $\mathbb{Q}$ podem pensar en la successió

$$a_1 = 1 \quad a_2 = a + \frac{1}{2} \quad a_3 = \frac{1}{1 + \frac{1}{2}} \quad a_4 = \frac{1}{1 + \frac{1}{1+\frac{1}{2}}} \quad \cdots$$

Si tingués límit L, hauria de complir que $L = 1 + \frac{1}{1+L}$, llavors $L^2 = 2$, però a $\mathbb{Q}$ no hi ha cap nombre que compleixi això. A $\mathbb{R}$ sí tindrà límit $\sqrt{2}$, aleshores, per la proposició serà de Cauchy. Així que a $\mathbb{Q}$, (a_n) és de Cauchy però no convergent. □

Definició 3.13.8. Definim la següent relació a $SC(K)$

$$(a_n)_n \sim (b_n)_n \iff (a_n - b_n) \to 0 \iff (a_n - b_n) \in S_0(K)$$

Lema 3.13.9. La relació just acabada de definir és una relació d'equivalència.

Demostració. És reflexiva perquè $(a_n - a_n) = (0)$, per tant, convergeix a 0. És simètrica, perquè si $(a_n - b_n)$ convergeix a 0, $(b_n - a_n)$ també, ja que $\varepsilon > |a_n - b_n| = |b_n - a_n|$. És transitiva, perquè si $|a_n - b_n| < \varepsilon/2$ i $|b_n - c_n| < \varepsilon/2$, es té, aplicant la desigualtat triangular que $|a_n - c_n| \leq |a_n - b_n| + |b_n - c_n| < \varepsilon$. Aleshores, és una relació d'equivalència. □

Lema 3.13.10. Sigui K un cos ordenat.

1. $(a_n)_n$ successió de Cauchy, aleshores (a_n) és fitada a K.
2. Si $(a_n), (b_n)$ són successions de Cauchy, aleshores la suma de successions $(a_n + b_n)_n$ i el producte $(a_n b_n)_n$ són successions de Cauchy.
3. Si $(a_n) \to a$ i $(b_n) \to b$ aleshores, $(a_n) \pm (b_n) \to a \pm b$, $(a_n)(b_n) \to ab$ i (si $b_n \neq 0$ i $b \neq 0$) $(a_n)/(b_n) \to a/b$.
4. Si $(a_n) \to 0$ i (b_n) fitada, $(a_n)(b_n) \to 0$.
5. Si (a_n) és de Cauchy amb una parcial convergent, la successió és convergent.

Demostració. Les demostracions són de càlcul 1, que estiguem en un cos ordenat arbitrari K no canvia les demostracions. □

Corol·lari 3.13.11. El conjunt $SC(K)$ de les successions de Cauchy a K és un anell, amb les operacions suma i producte de succesions.

Demostració. Fixem-nos que l'element neutre de la suma és la successió $(0)_n$, que la suma és un commutativa, associativa, i té invers (signe oposat), són propietats que s'hereden de K. L'element neutre del producte és $(1)_n$ i les propietats associativa, commutativa del producte i la distributiva s'hereden de K. □

Corol·lari 3.13.12. El subconjunt $S_0(K)$ (succ. convergents a 0) és un ideal de $SC(K)$.

Demostració. Pel lema, si (a_n) i (b_n) són successions convergents a 0, aleshores, la successió $(a_n) + (b_n)$ convergeix a 0. Si (c_n) és una successió de Cauchy qualsevol, aleshores és fitada i, per tant, $(a_n)(c_n)$ tendeix a 0. □

Definició 3.13.13. Definim el quocient $\widehat{K} = SC(K)/S_0(K)$.

Proposició 3.13.14.

1. $\widehat{K}$ és un cos.
2. K es pot injectar a $\widehat{K}$. $\iota : K \hookrightarrow \widehat{K}$.
3. $\widehat{K}$ és ordenat tal que els ordres de K i $\widehat{K}$ són compatibles.
4. $\iota(K)$ és dens a $\widehat{K}$.
5. $\widehat{K}$ és complet.
6. $\widehat{K}$ és minimal entre tots els cossos ordenats que satisfan les propietats anteriors. És a dir, si $u : K \hookrightarrow L$ és una altra inmersió de K en un altre cos ordenat i complet L, que respecta l'ordre i la imatge de K és densa a L, llavors existeix un únic morfisme de cossos ordenats $\widehat{u} : \widehat{K} \to L$, tal que $\widehat{u} \circ \iota = u$.

Definició 3.13.15. $\widehat{K}$ s'anomena la completació de K com a cos ordenat o el cos completat de K.

Definició 3.13.16. Podem definir $\mathbb{R} := \widehat{\mathbb{Q}}$.

3.14 Valoracions

Definició 3.14.1. Una valoració discreta d'un anell íntegre A és una aplicació

$$v : A \setminus \{0\} \to \mathbb{Z}$$

tal que $\forall a, b \in A \setminus \{0\}$ tal que $a + b \neq 0$.

1. $v(ab) = v(a) + v(b)$
2. $v(a + b) \geq \min(v(a), v(b))$

Si $K = \mathrm{Fr}(A)$ podem estendre v a K, amb

3. $v(\frac{a}{b}) = v(a) - v(b)$

Es defineix $v(0) = +\infty$.

Observació 3.14.2. $v(1) = 0$ i $v(-1) = 0$.

Demostració. Per la primera propietat tenim que $v(1 \cdot 1) = v(1) + v(1)$, per tant, $v(1) = 2v(1)$, amb la qual cosa tenim que $v(1) = 0$. Per altra banda, podem fer $v(-1 \cdot -1) = v(-1) + v(-1)$, llavors $0 = 2v(-1)$ i, per tant, $v(-1) = 0$. □

Exemple 3.14.1. Sigui $A = K[x]$, és a dir, l'anell de polinomis d'un cos K. Definim la següent valoració

$$\begin{array}{rccc} v: & A & \longrightarrow & \mathbb{Z} \\ & v(p(x)) & \longmapsto & -\deg p(x) \\ & v(\frac{p(x)}{q(x)}) & \longmapsto & \deg q(x) - \deg p(x) \end{array}$$

Sigui $A = \mathbb{Z}$, p un primer, definim la valoració p-àdica

$$\begin{array}{rccc} v_p: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & -\max\{k : p^k | n\} \\ & \frac{n}{m} & \longmapsto & \max\{k : p^k | n\} - \max\{k : p^k | m\} \end{array}$$

Podem fer el mateix que amb $A = K[x]$ i $p(x)$ irreductible

$$\begin{array}{rccc} v_{p(x)}: & \mathbb{A} & \longrightarrow & \mathbb{Z} \\ & f(x) & \longmapsto & -\max\{k : p(x)^k | f(x)\} \\ & \frac{f(x)}{g(x)} & \longmapsto & \max\{k : p(x)^k | g(x)\} - \max\{k : p(x)^k | f(x)\} \end{array}$$

Proposició 3.14.3. Sigui $v : A \setminus \{0\} \to \mathbb{Z}$ una valoració.

1. $R_v = \{a \in K = \mathrm{Fr}(A) : v(a) \geq 0\}$ és un anell.
2. Les unitats són $R_v^* = \{a \in K : v(a) = 0\}$.
3. $m_v = \{a \in K : v(a) > 0\}$ és l'únic idea maximal de R_v.

El cos $R(v) = R_v/m_v$ s'anomena cos residual de v.

Exercici 3.14.4. Al segon exemple anterior, descriviu l'anell $\mathbb{Z}_{(p)} := \mathbb{Z}_{v_p}$ i comproveu que $\mathbb{Z}(v_p) = \mathbb{Z}/p\mathbb{Z}$.

Definició 3.14.5. Un valor absolut en un cos K és una aplicació

$$\begin{array}{rccc} |\cdot|: & K & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & |x| \end{array}$$

que satisfà $\forall x, y \in K$

1. $|x| = 0$ si, i només si, $x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \leq |x| + |y|$ (desigualtat triangular).

La tercera propietat es pot substituir per una de més forta,

4. $|x + y| \leq \max\{|x|, |y|\}$

Si $|\cdot|$ satisfà les tres primers, diem que és un valor absolut ariquimedià. Si satisfà la quarta diem que és un valor absolut ultramètric. Anomenarem a la parella $(K, |\cdot|)$ un cos valorat.

Exemple 3.14.2. $\mathbb{R}$ amb el valor absolut habitual és un cos valorat. També ho és $\mathbb{C}$ amb el mòdul. A $\mathbb{Q}(i)$ podem definir $|a + bi| = \sqrt{a^2 + b^2}$ i també és un cos valorat.

Proposició 3.14.6. Si $v : A \to \mathbb{Z}$ és una valoració a $K = \mathrm{Fr}(A)$, triem $\rho \in (0, 1)$, aleshores

$$\begin{array}{rccc} |\cdot|_v: & K & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & |x|_v = \rho^{v(x)} \end{array}$$

és un valor absolut ultramètric.

Definició 3.14.7. Un valor absolut en K ens permet definir una topologia mètrica en K. On la base d'oberts són les boles, per tot $a \in K$,

$$B(a, r) = \{b \in K : |b - a| < r\}$$

Observació 3.14.8. La topologia anterior està ben definida.

Proposició 3.14.9. Si $|\cdot|$ prové d'una valoració v, $|x| = \rho^{v(x)}$ amb $\rho \in (0,1)$. Dos ρ's diferents ens donen valors absoluts diferents però la topologia que generen tots dos és la mateixa.

Observació 3.14.10. Fixem-nos que a partir de la topologia mètrica ja definida a partir de $|\cdot|$ a K, podem definir les successions de Cauchy, successions convergents, ... Però ara en totes les definicions tant l'ε com els valors absoluts estan dins de $\mathbb{R}$ i no necessitem que K sigui ordenat.

Definició 3.14.11. Un cos valorat $(K, |\cdot|)$ és complet si totes les successions de Cauchy a K són convergents.

Teorema 3.14.12. Per a tot cos valorat $(K, |\cdot|_K)$ existeix un cos valorat complet $(\widehat{K}, |\cdot|_{\widehat{K}})$ amb una inmersió $\iota : K \to \widehat{K}$ tal que $|\iota(x)|_{\widehat{K}} = |x|_K$, per a tot $x \in K$ i que és minimal amb aquesta propietat.

Demostració. La demostració és equivalent per als cossos ordenats. □

Exemple 3.14.3. Recordem que la valoració p-àdica:

$$\begin{array}{rccc} v_p: & \mathbb{Q} & \longrightarrow & \mathbb{Z} \\ & \frac{a}{b} & \longmapsto & v_p(a) - v_p(b) \end{array}$$

on $v_p(a) = \max_k\{p^k | a\}$. Ara escollim $\rho = 1/p$ i tenim el valor absolut p-àdic $|x|_p = (1/p)^{v(x)}$. Es pot veure que per $p \neq q$, els valors absoluts $|\cdot|_p$ i $|\cdot|_q$ donen topologies diferents a $\mathbb{Q}$.

Definició 3.14.13. El cos dels nombres p-àdics és el completat de $\mathbb{Q}$ respecte el valor absolut p-àdic. $\mathbb{Q}_p = (\mathbb{Q}, |\cdot|_p)$.

Observació 3.14.14. A $\mathbb{Q}_p$ quan tenim $|p^r|_p = (1/p)^r$ i fem tendir $r \to +\infty$, encara que ens sembli que el nombre es fa gran, el valor absolut tendeix a zero. I al revés, quan fem tendir $r \to -\infty$ el valor absolut tendeix a infinit.

Per aquest motiu, tal i com podem escriure un nombre real α com $\sum_{i=-\infty}^{m} a_i 10^i$, podem escriure un nombre p-àdic com $\sum_{i=m}^{+\infty} b_i p^i$. És a dir, en els reals un nombre pot tenir infinits decimals, mentre que en els p-àdics en té un nombre finit, però, per l'altra banda, pot tenir un nombre infinit de xifres (cosa que amb els reals no pot passar).

Exemple 3.14.4. A $\mathbb{Q}_p$ tenim que $\sum_{i\geq 0} p^i = \frac{1}{1-p}$ i també $\sum_{n\geq 0}(p-1)p^n = -1$. A $\mathbb{Q}_7$ podem trobar $\sqrt{2}$ i a $\mathbb{Q}_5$ podem trobar $\sqrt{-1}$.

Nota. $\mathbb{Q}_7$ no és algebraicament tancat.

Teorema 3.14.15. Teorema d'Ostrowski. Tot valor absolut a $\mathbb{Q}$ és equivalent (dona lloc a la mateixa topologia) a $|\cdot|$ usual o $|\cdot|_p$ per algun p primer.

Exemple 3.14.5. Sigui K un cos qualsevol, considerem la valoració del grau a l'anell de polinomis $K[x]$. Aleshores, podem considerar el valor absolut a $K(x)$ amb $\rho \in (0,1)$ habitual, $|p(x)/q(x)| = \rho^{\deg q - \deg p}$. Aleshores, el completat de $(K(x), |\cdot|)$, és $K[\{x\}]$ sèries de Laurent (sèries de potències amb un nombre finit de termes amb exponent negatiu).

3.15 L'equació general de grau n.

Definició 3.15.1. Sigui K un cos qualsevol i considerem les següents $n+2$ indeterminades $a_n, X_1, \ldots, X_n, T$. Aleshores, el polinomi general de grau n sobre K és

$$f(T) = a_n(T - X_1)\cdots(T - X_n) \in K(a_n, X_1, \ldots, X_n)[T]$$

que es pot mirar com un polinomi sobre el cos $K(a_n, X_1, \ldots, X_n)$ amb una sola indeterminada T.

Observació 3.15.2. Podem desenvolupar el polinomi $f(T)$, els coeficients que ens trobem dependran de a_n i de les X_i, és a dir,

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

On $a_0 = (-1)^n a_n X_1 \cdots X_n$, $a_1 = (-1)^{n-1} a_n(\sum_{i=0}^{n} \prod_{j\neq i} X_j)$, el terme general és

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

I l'últim terme és $a_{n-1} = -a_n(\sum_{i=1}^{n} X_i)$

Definició 3.15.3. Anomenarem a $S_k(X_1,\dots,X_n)=\sum_{\#I=n-k}\prod_{i\in I}X_i$ el k-èssim polinomi simètric elemental.

Teorema 3.15.4. Tot polinomi simètric a $X_1,\dots,X_n$ es pot escriure com a polinomi en els polinomis simètrics elementals. (o bé, tot polinomi simètric p en les arrels d'un polinomi q es pot escriure com a un altre polinomi h amb els coeficients del polinomi q).

Teorema 3.15.5. Considerem el cos $M=K(a_n,X_1,\dots,X_n)$ i el subcòs $L=K(a_0,\dots,a_n)$, aleshores, M/L és una extensió algebraica de grau $n!$.

3.16 Nombres construïbles i Origami

Definició 3.16.1. Un regle és un instrument sense mesures que ens permet dibuixar rectes arbitràriament llargues a partir de dos punts. Un compàs és un instrument que ens permet dibuixar circumferències a partir del seu centre i un punt.

L'objectiu d'aquesta secció és, donats dos punts en el pla que identificarem com l'origen o 0 i l'1, veure quins nombres es poden construir utilitzant, de moment, només el regle i el compàs. És a dir, que l'únic que poden fer és donats dos punts, la recta que passa per ells o les dues circumferències amb origen un i que passa per l'altra. Després, podem obtenir nous punts a partir dels punts de tall de les rectes i circumferències que tenim. Podem considerar punts arbitraris però no podrem assumir res d'ells.

Definició 3.16.2. Direm que podem construir una distància, si podem dibuixar dos punts, amb regle i compàs, que estiguin a aquesta distància. Direm que un nombre complex es pot construir si, identificant $\mathbb{R}^2$ amb $\mathbb{C}$, podem dibuixar, amb regle i compàs, el punt que l'identifica.

Proposició 3.16.3. Alguns nombres i distàncies construïbles són

1. Els enters.
2. Els enters de Gauss.
3. Donada una distància d, podem construir la distància $\sqrt{d}$.

Proposició 3.16.4. Algunes coses que podem fer són

1. Mediatrius i paral·leles.
2. Transportar distàncies a l'origen.
3. Sumar i restar construïbles.
4. Multiplicar i dividir construïbles.

Teorema 3.16.5. $\alpha\in\mathbb{C}$ és construïble amb regle i compàs si, i només si, existeix una torre d'extensions que quadràtiques

$$\mathbb{Q}\overset{2}{\subsetneq}\mathbb{Q}(\alpha_1)\overset{2}{\subsetneq}\cdots\overset{2}{\subsetneq}\mathbb{Q}(\alpha_r)\overset{2}{\subsetneq}\mathbb{Q}(\alpha)$$

Corol·lari 3.16.6. Un polígon regular de n costats es pot construir amb regle i compàs si, i només si $n=2^\alpha p_1\cdots p_r$, amb els p_i diferents primers de Fermat. És a dir, de la forma $p_i=2^{2^k}+1$, encara que els únics coneguts són 3,5,17,257,66537. Alguns polígons que es poden construir són els que tenen 3,4,5,6,8,10,12,15,16,... costats.

Observació 3.16.7. Construir el polígon de n costats equival a construir el nombre complex $\zeta=e^{2\pi i/n}$. I sabem, $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(n)$.

Proposició 3.16.8. Alguns problemes clàssics, els quals no es poden resoldre només amb regle i compàs.

1. La duplicació del cub. Trobar un cub de volum 2.
2. Trisecar un angle. Trobar l'angle terços d'un angle qualsevol.
3. Quadratura del cercle. Donat un cercle, trobar un quadrat de la mateixa àrea.

Demostració.

1. Cal trobar $\sqrt[3]{2}$ que no es pot construir amb regle i compàs perquè $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
2. Cal resoldre l'equació cúbica $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$. En general no es pot, perquè $[\mathbb{Q}(\cos\alpha) : \mathbb{Q}(\cos 3\alpha)] = 3$.
3. π ni tan sols és algebraic.

□

Definició 3.16.9. Direm que un nombre es construir amb origami, a part de regle i compàs, podem fer plecs al paper per obtenir rectes.

Proposició 3.16.10. 1. Podem dibuixar una paràbola (considerant infinits plecs).

2. Trisecar un angle.

Teorema 3.16.11. $\alpha \in \mathbb{C}$ és construible amb origami si, i només si, existeix una torre d'extensions quadràtiques i/o cúbiques

$$\mathbb{Q} \overset{2,3}{\subsetneq} \mathbb{Q}(\alpha_1) \overset{2,3}{\subsetneq} \cdots \overset{2,3}{\subsetneq} \mathbb{Q}(\alpha_r) \overset{2,3}{\subsetneq} \mathbb{Q}(\alpha)$$

Corol·lari 3.16.12. Un polígon regular de n costats es pot construir amb origami si, i només si $n = 2^r 3^s p_1 \cdots p_l$, amb primers de la forma $p = 2^a 3^b + 1$. Alguns polígons construïbles amb origami són els que tenen 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, ... costats.

Capítol 4

Grups

4.1 Nocions bàsiques i propietats

Definició 4.1.1. Un grup és un conjunt G amb una operació

$$\begin{array}{rccc} \cdot : & G \times G & \longrightarrow & G \\ & a, b & \longmapsto & a \cdot b = ab \end{array}$$

que satisfà

1. Té element neutre: $\exists e \in G$ tal que $\forall x \in G\ xe = ex = x$.
2. És associativa, $\forall a, b, c \in G\ a(bc) = (ab)c$.
3. Tot element és invertible $\forall a \in G\ \exists a^{-1}$ tal que $aa^{-1} = a^{-1}a = e$.

Es diu que un grup és abelià si, a més, l'operació satisfà la propietat communtativa. Un grup es finit es té un nombre finit d'elements i, en aquest cas, anomenem l'ordre del grup $|G|$ es seu cardinal. Altrament, direm que el grup és infinit.

Proposició 4.1.2. Algunes propietats elementals són

1. Només cal demanar que el l'invers ho sigui per un costat.
2. Només cal demanar que l'element neutre ho sigui per un costat.
3. L'element neutre és únic.
4. Cada element té un únic invers

Demostració.

1. Anem a suposar que només existeix l'invers per l'esquerra (per la dreta es fa igual), és a dir, per tot $x \in G$, existeix y tal que $yx = e$, multiplicant per la dreta per y ens queda, $yxy = y$. Ara y també té invers, diem-li z i multipliquem a l'expressió anterior per z per l'esquerra, ens queda $zyxy = zy$, utilitzant que $zy = e$ tenim $xy = e$ que és el que volíem veure.
2. Anem a suposar que $e \in G$ compleix que $ex = x$ per tot x de G (per la dreta es fa igual). Com que x té invers, multipliquem a banda i banda per xx^{-1}, per l'esquerra, que en el fons és multiplicar per e, però ens queda $xx^{-1}ex = xx^{-1}x$, a la banda esquerra simplement substituim $xx^{-1} = e$, mentre que a la dreta utilitzem que l'invers ho és per les dues bandes per substituir $x^{-1}x = e$. Aleshores, ens queda $ex = xe$, per tant, $x = ex = xe$ que és el que volíem veure.
3. En efecte, si existisin 2 elements neutres, e i e', aleshores $e = ee' = e'$, amb la qual cosa, han de ser el mateix element.
4. En efecte, si $\exists b, c$ tals que $ab = ba = ac = ca = e$. En aquest cas, $b = b(ac) = (ba)c = c$, per tant, $b = c$ i són el mateix element.

□

Definició 4.1.3. Definim per $a \in G$ un grup i per $n \in \mathbb{Z}^+$, $a^n := a \cdot \ldots \cdot a$ (n vegades) i $a^{-n} := (a^{-1})^n$ (n vegades). On a^{-1} és l'invers d'a.

Observació 4.1.4. De manera natural obtenim $a^{n+m} = a^n a^m$.

Nota. En general, per treballar amb grups usarem la notació multiplicativa (l'operació és la $\times$) però amb grups abelians se sol usar la notació aditiva (l'operació és la $+$).

Exemple 4.1.1. Un dels grups més fàcils, a part del trivial, és $G = \{0, 1\}$ on les operacions són les intuïtives. $G = \mathbb{Z}/n\mathbb{Z}$ amb la suma módul n és un grup abelià. Propiament els $\mathbb{Z}$ també és un grup. També ho és el grup de les arrels n-éssimes de les unitats amb el producte. Un del grup més importants és el grup simètric, el conjunt de les permutacions de n elements. Els moviments del pla que deixen fix un quadrat també és un grup. Si V és un k-espai vectorial, els automorfismes d'un espai vectorial és un grup, és a dir, els isomorfismes de V a V. Les matrius invertibles amb coeficients a K un cos és un grup.

Definició 4.1.5. Si G i H són dos grups, definirem el grup $G \times H$ amb la operació component a component:

$$\begin{array}{rccc} \cdot : & (G \times H) \times (G \times H) & \longrightarrow & G \times H \\ & (a, b), (x, y) & \longmapsto & (a \cdot_G x, b \cdot_H y) \end{array}$$

Definició 4.1.6. Un subgrup d'un grup G és un subgrup $H \subseteq G$ tal que

1. $e \in H$
2. $x, y \in H \implies xy^{-1} \in H$

En particular, això ens diu que un subgrup conté els inversos dels seus elements i és tancada per l'operació. Per tant, H té estructura de grup.

Definició 4.1.7. Si $S \subseteq G$ un subconjunt qualsevol de G, anomenem subgrup generat per S al menor subgrup de G que conté a S. El denotarem $\langle S \rangle$.

Definició 4.1.8. Direm que $H \subseteq G$ és un subgrup cíclic si hi ha un element que el genera. És a dir, $H = \langle a \rangle$, amb $a \in G$.

Proposició 4.1.9. Si $H, K \subseteq G$ subgrups, aleshores $H \cap G$ és un subgrup.

Demostració. Fixem-nos que $e \in H \cap G$. I si $x, y \in H \cap G$, aleshores, en particular $x, y \in H$ implica que $xy^{-1} \in H$ i el mateix per G. Llavors $xy^{-1} \in H \cap G$. □

4.2 Classe laterals

Definició 4.2.1. Sigui G un grup i $H \subseteq G$, definim dues relacions a G

$$\begin{array}{rcccc} a \sim_E b & \iff & \exists h \in H & b = ah \\ a \sim_D b & \iff & \exists & b = ha \end{array}$$

Observació 4.2.2. Està clar que les dues relacions anterios són relacions d'equivaléncia.

Demostració. Són reflectives perquè sempre existeix $e \in H$ i compleix que $a = ea = ae$. Són simètriques perquè si H conté un element, conté el seu invers aleshores si $a = bh$, segur que tenim $ah^{-1} = b$ (el mateix per dreta). Per últim, és transitiva perquè si $a = bh$ i $b = ch'$ aleshores, $a = h'hc$, on $h'h \in H$ perquè tant h' com h i són de H (el mateix per dreta). □

Definició 4.2.3. Denotarem la classe d'equivalència de $a \in G$ per l'esquerra $\sim_E$ com aH i els de la dreta $\sim_D$ per Ha. Al conjunt d'aquestes classes s'anomenen classes laterals. Denotarem $G\backslash H$ les classes laterals d'H per l'esquerra i H/G les classes laterals per la dreta.

Observació 4.2.4. La notació aH per referir-se a la classe a és consistent amb el fet de multiplicar a per tots els elements d'H.

Demostració. En efecte, tot element $b \in G$ tal que $b \sim_E a$ és de la forma $b = ah$ per un element $h \in H$ i tot element de la forma ah està relacionat amb a (el mateix per la dreta). □

Exemple 4.2.1. $G = \mathcal{S}_3 = \{\mathrm{Id}, (12), (1,3), (2,3), (1,2,3), (1,3,2)\}$ i prenem $H = \langle(1,2,3)\rangle = \{\mathrm{Id}, (1,2,3), (1,3,2)\}$ i si fem la classe lateral de $(1,2)$ obtenim $(1,2)H = \{(1,2), (2,3), (1,3)\} = (2,3)H = (1,3)H$ en aquest cas coincideixen. A més, fixem-nos que no és un subgrup perquè no contene la identitat. A part, tenim que $H = \mathrm{Id}\, H = (1,2,3)H = (1,3,2)H$. Per tant, només tenim dues classes laterals per l'esquerra i cada una amb tres elements. En aquest cas, les classes laterals per la dreta coincideixen.

Considerem ara, $H = \langle(1,2)\rangle = \{\mathrm{Id}, (1,2)\}$. Fixem-nos que ara $(1,3)H = \{(1,3), (1,2,3)\} \neq H(1,3) = \{(1,3), (1,3,2)\}$, $(2,3)H = \{(2,3), (1,3,2)\} \neq H(2,3) = \{(2,3), (1,2,3)\}$ i $H = H\,\mathrm{Id} = \mathrm{Id}\, H = (1,2)H = H(1,2)$. Així que algunes classes laterals no coincideixen.

Observació 4.2.5. Tenim, $\forall a \in G$ tenim bijeccions entre H i aH (també per la dreta).

Demostració. Simplement, enviant un element $h \in H$ a $ah \in aH$, l'invers d'aquesta aplicació és enviar un element $b = ah' \in aH$ a $a^{-1}b = a^{-1}ah' = h' \in H$. És injectiva perquè si $ah = ah'$ alehsores, $h = h'$ i és exhaustiva per definició de aH. □

Definició 4.2.6. Sigui G un grup finit i H un subgrup. Anomenarem l'índex d'H a G al número de classes laterals, l'anotarem com $[G : H]$.

Observació 4.2.7. A la definició anterior no sabem si l'índex es refereix al nombre de classes laterals per la dreta o per l'esquerra, però el següent tereorema ens assegura que són el mateix.

Teorema 4.2.8 (Teorema de Lagrange)**.** Si G és un grup finit i $H \subset G$ un subgrup, aleshores

$$[G : H] = \#G/\#H$$

En particular $[G : H]$ no depèn de si ens referim a les classes laterals per l'esquerra o per la dreta.

Demostració. Hem vist que, $\forall a \in G$, $\#H = \#aH$ per les bijeccions d'abans, així que totes les classes laterals (perquè totes es poden posar d'aquesta forma) tenen el mateix nombre d'elements que H. A més, sabem que les classes laterals donen una partició del grup, ja que, per ser una relació d'equivalència, un mateix element no pot pertànyer a dues classes diferents. Per tant,

$$\#G = [G : H] \cdot \#H$$

□

4.3 Grup quocient

Definició 4.3.1. Podem intentar definir una operació en el que serà el grup quocient $G\backslash H$:

$$(aH) \cdot (bH) := (ab)H$$

Observació 4.3.2. Anem a veure que, en general l'operació anterior, no està ben definida, és a dir, el resultat depén dels representants escollits.

Demostració. Suposem que $a'H = aH$ i $b'H = bH$, equivalenment $a' = ah$ i $b' = bh'$, aleshores, hauríem de veure existeix un $\widetilde{h}$ tal que $(a'b')H = (ab)H$, és a dir, cal que $ab\widetilde{h} = a'b' = ahbh'$, amb $h, h', \widetilde{h} \in H$. Cosa que només passarà si $bh^{-1}b^{-1} = h'\widetilde{h}^{-1}$, és a dir, cal que $bh^{-1}b^{-1} \in H$, en general això no pasarà, ja que les classes laterals per l'esquerra haurien de coincidir amb les de la dreta. □

Definició 4.3.3. Un subgrup $H \subseteq G$ s'anomena normal si $\forall b \in G$ es té que $bH = Hb$. Equivalentment, $bHb^{-1} = H$, $\forall b \in G$. Escriurem $H \triangleleft G$ per denotar que H és un subgrup normal de G.

Exemple 4.3.1. Com hem vist a l'exemple anterior, $\mathcal{S}_3$ $H = \langle(1,2,3)\rangle \triangleleft G$, mentre que $\langle(1,2)\rangle$ no és un subgrup normal. Si G és abelià, tot subgrup és normal.

Proposició 4.3.4. Si $H \triangleleft G$ el conjunt $G\backslash H$ de classes laterals (per l'esquerra) mòdul H té estructura de grup amb l'operació

$$(aH)(bH) := (ab)H$$

Demostració. Suposem que $a'H = aH$ i $b'H = bH$, podem escriure $a' = ah$ i $b' = bh'$, per alguns $h, h' \in H$. Aleshores, hem de veure que $(a'b')H = (ab)H$, és a dir, cal que $ab\widetilde{h} = a'b' = ahbh'$, cosa que només passarà si $bh^{-1}b^{-1} = h'\widetilde{h}^{-1}$, per algun $\widetilde{h} \in H$. Però com que $bHb^{-1} = H$, tenim que, per qualsevol h^{-1} existirà un element $\widehat{h} \in H$ tal que $\widehat{h} = bh^{-1}b^{-1} = h'\widetilde{h}^{-1}$. Llavors, sempre es podrem escriure $\widetilde{h} = \widehat{h}^{-1}h'$, per tant, $\widetilde{h} \in H$. □

Observació 4.3.5. L'element neutre de l'operació anterior és $eH = H$, tota classe aH té invers i és $a^{-1}H$. L'associativitat s'hereda de G.

Exemple 4.3.2. $G = \mathcal{S}_3$ i $H = \langle(1,2,3\rangle$, tenim que $\#G/H = [G : H] = \#G/\#H = 6/3 = 2$ que són $G/H = \{(1,2)H, H\}$ on $H \cdot H = H$, $(1,2)H \cdot H = (1,2)H$ i $(1,2)H \cdot (1,2)H = H$.

Definició 4.3.6. Si $H \triangleleft G$, anomanem grup quocient de G mòdul H al conjunt G/H amb l'operació definida anteriorment.

Definició 4.3.7. Sigui G un grup, direm que un element $a \in G$ té ordre infinit si $\forall n \in \mathbb{Z}^+$ tal que $a^n = e$. Altrament, direm que a és un element de torsió i definim

$$\operatorname{ord}(a) = \min_{k \in \mathbb{Z}^+} \{a^k = e\}$$

Equivalenment $\operatorname{ord}(a) = \#\langle a\rangle = \#\{a^k : k \in \mathbb{Z}\}$.

Proposició 4.3.8. Sigui $a \in G$ un element de torsió

1. $a^m = e \iff \operatorname{ord}(a) | m$.
2. $a^m = a^n \iff m \equiv n \mod \operatorname{ord}(a)$.
3. Si $t | \operatorname{ord}(a)$, aleshores $\operatorname{ord}(a^t) = \operatorname{ord}(a)/t$.
4. $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$.
5. $\forall x \in G$, $\operatorname{ord}(xax^{-1}) = \operatorname{ord}(a)$.

Corol·lari 4.3.9. Si G és finit, tot element de G és de torsió, a més es té que $\operatorname{ord}(a) | G$ i $a^{|G|} = e$.

Demostració. Si G és finit, clarament fent a^m per $m \in \mathbb{Z}^+$ en algun moment apareixerà un element que ja hauria aperegut, del estil $a^m = a^n$, dividint pel l'exponent més petit, ens quedaria, $a^{m-n} = e$. Ara, pel teorema de Lagrange $\#G/\#\langle a\rangle = [G : \langle a\rangle] \in \mathbb{Z}^+$, aleshores, $\operatorname{ord}(a) = \#\langle a\rangle | \#G$, llavors, per una propietat anterior, $a^{\#G} = e$. □

Corol·lari 4.3.10. Si $\#G = p$ primer, tenim que G és cíclic, és a dir, $\exists a \in G$ tal que $G = \langle a\rangle$.

Demostració. En efecte, si $\forall a \neq e \in G$ tenim que $\operatorname{ord} a | \#G$, per tant, $\#\langle a\rangle = \operatorname{ord} a = p = \#G$, per tant, $\langle a\rangle = G$. □

4.4 Morfismes de grups

Definició 4.4.1. Una aplicació $f : G \to H$ entre dos grups G, H és un morfisme de grups si

$$\forall x, y \in G \qquad f(x \cdot_G y) = f(x) \cdot_H f(y)$$

Proposició 4.4.2. Propietat dels morfimes de grups.

1. $f(e_G) = e_H$
2. $f(x^{-1}) = f(x)^{-1}$

3. $f(x^n) = f(x)^n \ \forall n \in \mathbb{Z}$.

Demostració.

1. Sigui $u = f(e_G)$, aleshores, $u^2 = f(e_G)f(e_G) = f(e_G^2) = f(e_G) = u$, per tant, $u^2 = u$ i, ara multiplicant per u^{-1}, tenim $u = e_H$.
2. $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$, aleshores, $f(x^{-1}) = f(x)^{-1}$.
3. Si $n \geq 0$ procedim per inducció. Per $n = 0, 1$ trivial. Per $n \geq 2$, suposem el cas $n-1$, aleshores $f(x^n) = f(x^{n-1})f(x) = f(x)^{n-1}f(x) = f(x)^n$. Per $n \leq -1$, és aplicar el mateix per x^{-1}.

□

Exemple 4.4.1. Sigui $G = \langle g \rangle = \{g^\alpha\}_{\alpha \in \mathbb{Z}}$ un grup cíclic infinit format per poténcies d'un element. Aleshores, podem definir el següent morfisme de grups entre G i $\mathbb{Z}$:

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \mathbb{Z} \\ & g^k & \longmapsto & k \end{array}$$

Comprovem-ho, $\varphi(g^k g^l) = \varphi(g^{k+l}) = k + l = \varphi(g^k) + \varphi(g^l)$.

També podem definir el següent morfisme grups a partir de morfismes d'anells coneguts.

$$\begin{array}{rccc} \pi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & k & \longmapsto & \pi(k) = k \mod m \end{array}$$

També podem definir un morfisme entre $(\mathbb{R}, +)$ i $(\mathbb{R}^*, *)$, enviant $x \in \mathbb{R}$ a $e^x \in \mathbb{R}^*$. O bé, entre $(\mathbb{R}^+, *)$ i $(\mathbb{R}, +)$ podem considerar el morfisme que envia x a $\log x$.

Si $H \subseteq G$, la inclusió $H \hookrightarrow G$ és un morfisme de grups. Per últim, podem considerar el morfisme que envia una matriu de rang màxim sobre un cos K al seu determinant.

Proposició 4.4.3. Sigui $f : G \to H$ un morfisme.

1. Sigui $K \subseteq G$ un subgrup, aleshores $f(K) \subseteq H$ és un subgrup.
2. Sigui $M \subseteq H$ un subgrup, aleshores $f^{-1}(M) \subseteq G$ és un subgrup.

Demostració.

1. Com que $e_G \in K$, aleshores, $e_H = f(e_G) \in f(K)$. Siguin $x, y \in f(K)$, aleshores $\exists a, b \in K$ tals que $x = f(a)$ i $y = f(b)$. Llavors $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1})$, per tant $xy^{-1} \in f(K)$. Per tant, $f(K)$ és un subgrup de H.
2. Com que $e_H \in M$ i $f(e_G) = e_H$, clarament $e_G \in f^{-1}(M)$. Siguin $a, b \in f^{-1}(M)$, volem veure que $ab^{-1} \in f^{-1}(M)$. Tenim que existeixen un únics $x, y \in M$ tals que $x = f(a)$ i $y = f(b)$, per tant, $f(ab^{-1}) = f(a)f(b)^{-1} = xy^{-1} \in M$, que és el que volíem veure. Per tant, $f^{-1}(M)$ és un subgrup de G.

□

Definició 4.4.4. Sigui $f : G \in H$ morfisme. Definim $\ker f := f^{-1}(\{e_H\})$, el qual, per la propietat anterior, és un subgrup de G. I definim, $\operatorname{Im} f := f(G)$, també per la propietat anterior, és un subgrup de H.

Definició 4.4.5. Sigui $f : G \to H$ és un monomorfisme si f és injectiva, epimorfisme és f exhaustiva i isomorfisme si f és bijectiva.

Proposició 4.4.6.

1. f és monomorfisme si i només si $\ker f = \{e_G\}$.
2. f és un epimorfisme si i només si $\operatorname{Im} f = H$.
3. f és isomorfisme si i només si $\ker f = \{e_G\}$ i $\operatorname{Im} f = H$.

Demostració.

1. Sigui f un monorfime, com que sabem que $f(e_G) = e_H$ i tot element de H només pot tenir com a molt una antiimatge, $\ker f = \{e_G\}$. Suposem ara que $\ker f = \{e_G\}$ i que tenim $f(a) = f(b)$. Aleshores multipliquem a banda i banda per $f(b)^{-1}$, ens queda $e_H = f(a)f(b)^{-1} = f(ab^{-1})$, per tant $ab^{-1} = e_G$, és a dir, $a = b$, per tant, f és monomorfisme.

2. Per definició d'exhaustivitat.

3. Per definició de bijectiva s'han de complir les dues anteriors.

□

Exemple 4.4.2. El morfisme $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ que envia un element $x \in \mathbb{Z}/6\mathbb{Z}$ a $(x \mod 2, y \mod 3) \in \mathbb{Z}/3\mathbb{Z}$.

Teorema 4.4.7 (Teorema de Cayley)**.** Tot grup finit és isomorf a un subgrup simètric.

Demostració. Si G un grup finit qualsevol, $\forall x \in G$ definim $\varphi : G \to G$ tal que $\varphi_x(y) = xy$. φ_x és una bijecció és injectiva, si $xy = \varphi_x(y) = \varphi_x(z) = xz$, aleshores, $y = z$, i és G és un conjunt finit. Ara, sigui $n = \#G$ i enumenarem els elements de G d'alguna manera, és a dir, triem un bijecció ψ entre $\{1, \dots, n\}$ i G. Definim $\widetilde{\varphi_x} = \psi^{-1} \circ \varphi_x \circ \psi$, aquesta funció és una bijecció (per ser composició de bijeccions) entre $\{1, \dots, n\}$ i ell mateix. Aleshores, $\widetilde{\psi_x} \in \mathcal{S}_n$. L'aplicació

$$\begin{array}{rccc} \Phi: & G & \longrightarrow & \mathcal{S}_n \\ & x & \longmapsto & \widetilde{\varphi_x} \end{array}$$

és un morfisme de grups ja que $\Phi(xy) = \widetilde{\varphi_{xy}} = \psi^{-1} \circ \varphi_{xy} \circ \psi = \psi^{-1} \circ \varphi_x \circ \varphi_y \circ \psi = \psi^{-1} \circ \varphi_x \circ \psi \circ \psi^{-1} \circ \varphi_y \circ \psi = \Phi(x)\Phi(y)$, on hem utilitzat que $\varphi_{xy} = \varphi_x \circ \varphi_y$ i que l'operació de $\mathcal{S}_n$ és la composició. A més, $\Phi(e_G) = \psi^{-1} \circ \varphi_{e_G} \circ \psi = \mathrm{Id}$, ja que $\varphi_{e_G} = \mathrm{Id}$ (entre $G \to G$) i $\varphi^{-1} \circ \varphi = \mathrm{Id}$ (de $\mathcal{S}_n$). A part, Φ és un morfisme injectiu ja que si $\Phi(x) = \Phi(y) \implies \psi^{-1} \circ \varphi_x \circ \varphi = \psi^{-1}\varphi_y\psi$, aleshores $\varphi_x = \varphi_y$, però això només pot passar si $x = y$ ja que quan evaluem a e_G ens queda $xe_G = ye_G$. Finalment, si considerem $\widetilde{\Phi} : G \to \Im(\Phi)$, tal que $\widetilde{\Phi}(x) = \Phi(x)$ tenim un isomorfime de grups entre G i un subgrup de $\mathcal{S}_n$. □

Observació 4.4.8. Φ i $\mathrm{Im}(\Phi)$ no són canònics.

Demostració. Per exemple, $\mathbb{Z}/3\mathbb{Z}$ es pot enviar a $\mathcal{S}_3$ de diferents maneres, enviant l'1 a $(1,2,3)$ o bé a enviant-lo a $(1,3,2)$, d'aquesta manera dona el mateix subgrup però el morfisme és diferent. □

Proposició 4.4.9. Sigui $H \triangleleft G$ un subgrup normal, l'aplicació canónica

$$\begin{array}{rccc} \pi: & G & \to & G/H \\ & a & \longmapsto & \pi(a) = aH \end{array}$$

és un morfisme de grups i $\ker \pi = H$.

Demostració. Per definició la pròpia definició que vam donar de l'operació dins de G/H, $\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b)$. A més, si $aH = \pi(a) = e_{G/H}H = H$, necessàriament, $a \in H$ i, si $a \in H$ tenim que $\pi(a) = aH = H$, aleshores $\ker \pi = H$. □

Proposició 4.4.10.

1. Sigui $f : G \to H$ un morfisme de grups, aleshores $\ker f \triangleleft G$.
2. Recíprocament, si $K \triangleleft G$, sempre trobarem un morfisme de G en un altre grup H tal que $f : G \to H$ tal que $\ker f = K$.

Demostració. Hem de veure que $\forall a \in G$, $a \ker f = (\ker f)a$. Equivalentment, $a(\ker f)a^{-1} = \ker f$. Sigui $x \in \ker f$, és a dir, tal que $f(x) = e_H$, aleshores, $f(axa^{-1}) = f(a)f(x)f(a)^{-1} = f(a)f(a)^{-1} = e_H$, per tant, $axa^{-1} \in \ker f$. Tenim que $a \ker f a^{-1} \subseteq \ker f$. Ara considerem $x \in \ker f$, semblant a abans, $a^{-1}xa \in \ker f$ aleshores $a^{-1}xa = y$ per algun $y \in \ker f$. Per tant $x = aya^{-1} \in a(\ker f)a^{-1}$, per tant, $\ker f \subseteq a(\ker f)a^{-1}$. En definitiva, $\ker f = a(\ker f)a^{-1}$

Ara, per propietats ja vistes $K = \ker \pi$ on $\pi : G \to G/K$. □

Proposició 4.4.11. Donat $H \triangleleft G$, sigui $\pi : G \to G/H$. L'aplicació natural

$$\begin{array}{rccc} \varphi: & \text{Subgrups de } G \text{ que contenen } H & \longrightarrow & \text{Subgrups de } G/H \\ & H \subseteq M & \longmapsto & M/H := \pi(M) \end{array}$$

és una bijecció que

1. Respecte inclusions $M_1 \subseteq M_2 \iff M_1/A \subseteq M_2/A$
2. Envia subgrups normals a subgrups normals.

4.5 Teoremes d'isomorfismes

Teorema 4.5.1 (Primer Teorema d'isomorfisme)**.** Sigui $f : G \to H$ un morfime de grups, aleshores, tenim un isomorfisme canónic

$$G/\ker f \simeq \operatorname{Im} f$$

Demostració. Definim $\widetilde{f} : G/\ker f \to \operatorname{Im} f$, com $\widetilde{f}(a \ker f) := f(a)$, està ben definit perquè si $a \ker f = b \ker f$ vol dir que $a = bk$, per algun $k \in \ker f$, aleshores $f(a) = f(bk) = f(b)f(k) = f(b)e_G = f(b)$.

$\widetilde{f}$ és morfisme per que $\widetilde{f}((a \ker f)(b \ker f)) = \widetilde{f}((ab) \ker f) = f(ab) = f(a)f(b) = \widetilde{f}(a \ker f)\widetilde{f}(b \ker f)$.

$\widetilde{f}$ és injectiu perquè $\widetilde{f}(a \ker f) = e_G$ implica que $f(a) = e_G$, aleshores $a \in \ker f$, per tant, $a \ker f = \ker f$, que és la identitat de $G/\ker f$. $\widetilde{f}$ és exhaustiu perquè $\widetilde{f}(G/H) = f(G) = \operatorname{Im} f$. Aleshores, tenim un isomorfisme entre $G/\ker f$ i $\operatorname{Im} f$, per tant, són isomorfs. □

Lema 4.5.2. Sigui G un grup amb $H \subseteq K \subseteq G$, aleshores, $H \triangleleft G$ i $K \triangleleft G$, si i només si $H \triangleleft K$.

Teorema 4.5.3 (Tercer teorema d'isomorfisme)**.** Siguin $H \subseteq K \subseteq G$ dos subgrups normals de G.

1. $K/H \triangleleft G/H$.
2. $(G/H)/(K/H) \simeq (G/K)$.

Proposició 4.5.4. Sigui $H \triangleleft G$ i $K \triangleleft G$ dos subgrus normals d'un grup G. El conjunt $HK = \{hk : h \in H, k \in K\}$ és un subgrup de G que conté a H i K. A més, $H \triangleleft HK$ i $K \triangleleft HK$.

Demostració. Com que $e_G \in H, K$, aleshores. Veurem que si $x, y \in HK$, aleshores $xy^{-1} \in HK$. Tenim que podem escriure $x = h_1k_1$ i $y = h_2k_2$ amb $h_1, h_2 \in H$ i $k_1, k_2 \in K$, aleshores $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1kh_2$. Utilitzem que H és normal, aleshores $kH = Hk$, llavors $h_1kh_2 = h_1h_3k = hk \in HK$.

$H \subseteq HK$ perquè $H = He$ i $e \in K$. De la mateixa manera $K \subseteq HK$. Per altra banda, volem veure que $H \triangleleft HK$, és a dir, $\forall hk \in HK$, $\forall u \in H$, ens cal comprovar que $(hk)u(hk)^{-1} \in H$. Tenim que $(hk)u(hk)^{-1} = hkuk^{-1}h^{-1}$, ara, per ser $u \in H$ i H normal, tenim que $kuk^{-1} \in H$, aleshores, com que tot producte d'elements d'H és de H, tenim que $hkuk^{-1}h^{-1} \in H$. De la mateixa manera es pot raonar que $K \triangleleft HK$. □

Teorema 4.5.5 (Segon teorema d'isomorfisme)**.** Sigui G un grup i $H \triangleleft G$, $K \triangleleft G$ dos subgrups normals, aleshores

$$K/H \cup K \simeq HK/H$$

Demostració. Definim

$$\begin{array}{rccccc} \varphi : & K & \xhookrightarrow{\iota} & HK & \xrightarrow{\pi} & HK/H \\ & k & \longmapsto & ek = k & \longmapsto & kH \end{array}$$

Clarament φ és morfisme per ser composició de morfismes. φ és exhaustiu (epimorfisme). En efecte, un element de HK/H és de la forma hkH amb $h \in H$ i $k \in K$, a més, per $H \triangleleft G$ tenim que $(hk)H = H(hk)$ que per producte de classes és igual a $(Hh)(Hk) = H(Hk) = Hk = kH$, aleshores, $\varphi(k) = kH = (hk)H$. Per tant, tot element de HK/H és imatge d'algú.

A més, $\ker \varphi = H \cap K$, ja que si $k \in K$ és tal que $\varphi(k) = eH = H$ ha de passar que $kH = H$, és a dir, que $k \in H$. I si $k \in H$, clarament $\varphi(k) = kH = H$.

Aleshores, pel primer teorema d'isomorfisme $K/(H \cap K) \simeq HK/H$. □

4.6 Producte directe

Definició 4.6.1. El producte cartesià d'una família finita $G_1, \ldots, G_r$ de grups té una estructura natural de grup

$$\begin{array}{ccc} (G_1 \times \ldots \times G_r) \times (G_1 \times \ldots \times G_r) & \longrightarrow & G_1 \times \ldots \times G_r \\ (a_1, \ldots, a_r), (b_1, \ldots, b_r) & \mapsto & (a_1, \ldots, a_r) * (b_1, \ldots, b_r) := (a_1 *_1 b_1, \ldots, a_r *_r b_r) \end{array}$$

On $*_i$ denota l'operació del grup i-éssim.

Capítol 5

Moduls