Estructures algebraiques

Contingut basat en les notes del curs 2016-2017

Artur Travesa

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Artur **Travesa Grau**
Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Classificació AMS (revisió de 2010):
Primària: 00-01, 08-01, 08Axx, 20-01, 97H40
Secundària: 13A05, 13B25, 13B30, 13F07, 13F10, 20A05, 20B05, 20B30, 20B35, 20Dxx, 20D20, 20F05, 20Kxx.

Universitat de Barcelona
Facultat de Matemàtiques i Informàtica
Barcelona, 2017, 2019

Contingut

Introducció

Aquest tractat té l'origen en les meves notes de l'assignatura "Estructures algebraiques" del grau de Matemàtiques de la Universitat de Barcelona que vaig impartir el curs 2016-2017. A l'hora de fer el plantejament del desenvolupament del curs, he tingut presents quines assignatures, i amb quins continguts nominals segons els seus plans docents corresponents, la precedeixen en els diferents itineraris recomanats per la Facultat de Matemàtiques i Informàtica, encarregada d'impartir el grau.

Així, cal suposar que l'estudiantat d'Estructures algebraiques cursa aquesta assignatura després d'haver adquirit, entre molts d'altres, un coneixement elemental de llenguatge matemàtic, que inclou els conceptes bàsics de conjunt, aplicació, relació d'ordre, relació d'equivalència, conjunt quocient per una relació d'equivalència, i la construcció dels conjunts dels nombres naturals, a partir dels axiomes de Dedekind-Péano, dels nombres enters, i dels nombres racionals, així com també de la propietat d'inducció del conjunt dels nombres naturals. D'altra banda, també cal suposar que l'estudiantat ha adquirit un coneixement bàsic d'àlgebra lineal: concepte d'espai vectorial, dependència i independència lineal, generació de subespais, intersecció i suma de subespais, bases, dimensió, sistemes d'equacions lineals, matrius, productes de matrius, inversió de matrius invertibles, matrius elementals, aplicacions lineals, nuclis i imatges, sumes directes, productes, quocients, teoremes d'isomorfia, canvis de base, l'espai dual, ortogonalitat, valors i vectors propis d'endomorfismes, polinomis característic i mínim d'un endomorfisme, subespais invariants, descomposició en components primaris, formes canòniques de Jordan.

A més a més, una bona part de l'estudiantat ha cursat una assignatura d'Aritmètica en què, entre altres continguts, s'hi treballen els conceptes bàsics de divisibilitat, tant a l'anell dels nombres enters com a l'anell de polinomis de coeficients en un cos, incloent el teorema fonamental de l'aritmètica i l'algoritme d'Euclides; de congruències, inicialment les lineals, incloent el teorema xinès del residu, però també les polinòmiques, especialment les quadràtiques, incloent els símbols de Legendre i de Jacobi; les propietats multiplicatives de les congruències, en particular, l'existència o no d'arrels primitives mòdul un nombre enter qualsevol; l'aritmètica dels nombres complexos, incloent les arrels de la unitat, arrels de polinomis i l'enunciat del teorema fonamental de l'àlgebra; tests i certificats de primeritat; algoritmes bàsics de factorització; i aplicacions de l'aritmètica, essencialment a la criptografia elemental i a la criptografia de clau pública.

Tot aquest bagatge inclou, òbviament, les definicions i les primeres propietats de les estructures algebraiques més bàsiques: grups (commutatius, cíclics, simètrics, lineals) i anells (cossos dels nombres racionals, reals, o complexos, anells de classes de congruència, anells de polinomis, anells d'endomorfismes, anells de matrius), a més a més d'altres conceptes algebraics, com morfisme o aplicació lineal, productes o sumes directes, o bases, per exemple, associats inicialment a l'àlgebra lineal.

I, encara, una altra part de l'estudiantat ha cursat altres assignatures amb continguts algebraics i geomètrics —topologia, geometria lineal, geometria projectiva—, de manera que cal suposar que disposa d'una base més sòlida de coneixements relacionats amb les diferents estructures.

D'acord amb el pla docent de l'assignatura d'Estructures algebraiques, en el temari i els objectius d'aprenentatge que cal treballar-hi, hi ha l'estudi dels grups –incloent grups cíclics, abelians, simètrics, diedrals, de simetries, resolubles—, grups lliures i presentacions d'un grup, accions d'un grup en un conjunt, teoremes de Sylow, i grups abelians finitament generats; i també l'estudi d'anells –incloent lema de Zorn, ideals maximals, ideals primers—, anells de fraccions, dominis euclidians, dominis principals, dominis de factorització única, factorialitat dels anells de polinomis, i reconeixement d'elements irreductibles en alguns anells.

Es desprèn d'aquest plantejament que l'assignatura està pensada més per a un assentament i una consolidació dels conceptes bàsics, amb una certa generalització d'alguns resultats, que no pas per al desenvolupament profund d'una teoria de grups —que inclogués temes tan importants com, per exemple, representacions lineals—, ni de teoria d'anells —amb estudi de temes d'àlgebra commutativa o geometria algebraica bàsiques, noetherianitat, multilinealitat, o teoria de Galois, per exemple.

Així, doncs, amb aquest esperit d'assentament i consolidació de coneixements, he dividit el contingut del curs en set capítols i un apèndix. El primer capítol conté una formalització dels conceptes bàsics subjacents a les estructures que s'estudien; després, tres capítols contenen un estudi dels conceptes relacionats amb l'estructura de grup en general, d'acció d'un grup en un conjunt, i dels conceptes de llibertat i de resolubilitat de grups; a continuació, dos capítols contenen conceptes bàsics relacionats amb l'estructura d'anell, l'un, i de la factorialitat, l'altre; i un darrer capítol conté un estudi dels mòduls finitament generats sobre dominis d'ideals principals, com a descripció comuna dels teoremes de reducció de matrius regulars a la identitat, que es demostra a Matrius i vectors, de resolució de sistemes d'equacions diofantines lineals, de la qual se'n parla a Aritmètica, o de classificació d'endomorfismes i forma de Jordan, que es treballa a Àlgebra lineal. Finalment, he recollit en un apèndix qüestions bàsiques relatives a l'axioma de l'elecció, el lema de Zorn, o el teorema de Zermelo, sense entrar en la demostració de la seva equivalència en el marc de la teoria de conjunts; m'he limitat a fer una discussió intuïtiva d'aquests conceptes i a veure exemples de la seva aplicació.

En el desenvolupament dels temes he procurat donar les definicions de manera precisa, per a no donar lloc a confusions, però sense esquivar les dificultats ni els casos generals; i proporcionar, de seguida, nombrosos exemples d'allò que es tracta. I, després, enunciar i demostrar els teoremes de manera completa, i només obviar una mínima part d'algunes demostracions, normalment per la seva simplicitat o la seva semblança amb altres ja treballades. D'altra banda, he inclòs alguns enunciats d'exercicis amb una finalitat doble; d'una banda, que l'estudiantat pugui ampliar o consolidar millor els coneixements, i, de l'altra, per a ajudar a destacar els límits de validesa d'alguns resultats; per exemple, per a posar de manifest situacions semblants en les quals no se satisfà la tesi d'un teorema. Finalment, he inclòs un índex de diagrames i un índex terminològic a fi de facilitar la recerca de material concret.

Barcelona, estius de 2017 i de 2020

Capítol 1

Conceptes bàsics

El contingut d'aquest primer capítol és pensat, d'una banda, per a proporcionar una base formal per a les estructures algebraiques més habituals, i de l'altra, per a fixar les notacions i les hipòtesis bàsiques de treball.

Comencem, doncs, el curs, amb el repàs d'alguns conceptes de teoria de conjunts i aplicacions i, de seguida, discutim amb un cert deteniment el concepte de producte cartesià de conjunts, per al qual posem un èmfasi especial en la seva propietat universal. A continuació, definim el concepte d'operació i considerem algunes de les seves propietats més habituals: commutativa, associativa, elements neutres, elements inversos, i distributives. Després d'estudiar amb una mica de detall les operacions associatives, de manera que donem sentit a les notacions habituals per a les sumes o els productes de successions finites d'elements, definim les estructures algebraiques bàsiques de grup i d'anell i en donem exemples, però deixem per a capítols posteriors el seu estudi més sistemàtic. Acte seguit, considerem el concepte d'acció d'un conjunt en un altre i algunes propietats associades a aquest concepte, i definim les estructures lineals de mòdul i d'espai vectorial, amb el mateix esperit que hem fet amb les de grup i d'anell. Acabem el capítol amb la definició, de manera unificada per a les diferents estructures algebraiques, de morfisme i d'isomorfisme; però, en canvi, deixem per a més endavant (capítol 5) la discusió dels conceptes de monomorfisme i d'epimorfisme.

1.1 Repàs de llenguatge matemàtic bàsic

Com a referències bàsiques per a la teoria elemental de conjunts, podem citar, per exemple, [Pla 2006], [Halmos 1960], o [Kelley 1975]; altres referències, més avançades i que contenen desenvolupaments més profunds d'alguns dels temes tractats aquí, poden ser, per exemple, [Barnes-Mack 1978], [Malitz 1979], [Mendelson 1979], o [Monk 1976].

1.1.1. Des del punt de vista de la teoria de conjunts, podem pensar qualsevol nombre natural n com el conjunt $\{0, 1, \ldots, n-1\}$, format pels n nombres naturals anteriors a n; recordem que, si $n \neq 0$, el nombre $n-1$ s'anomena el predecessor de n. En particular,

- $0 := \varnothing$ és el conjunt buit, també anomenat zero;
- $1 := \{0\} = \{\varnothing\}$ és un conjunt d'un sol element, també anomenat u o bé un;
- $2 := \{0, 1\} = \{\varnothing, \{\varnothing\}\}$ és un conjunt de dos elements, també anomenat dos;

• $3 := \{0,1,2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ és un conjunt de tres elements, anomenat tres;

• i, per inducció, $n+1 := \{0,1,\dots,n\} = n \cup \{n\}$ és un conjunt de $n+1$ elements, que s'anomena successor de n.

És usual fer servir la notació $\mathbb{N}$ per al conjunt de tots els nombres naturals; en particular, $\mathbb{N} := \{0,1,2,\dots,n,n+1,\dots\}$ és el conjunt reunió de tots els nombres naturals. Molta altra informació bàsica sobre continguts d'aritmètica, diferent de la construcció formal de $\mathbb{N}$ o del conjunt $\mathbb{Z}$ dels nombres enters es pot trobar, per exemple, en [Travesa 1998].

1.1.2. També des del punt de vista de la teoria de conjunts, donats conjunts A, B, la notació A^B es fa servir per a denotar el conjunt de totes les aplicacions de B en A, encara que, segons el context, també es fan servir les notacions $\mathcal{F}(B,A)$ o $\mathrm{Apl}(B,A)$. En particular, per a tot conjunt A i tot nombre natural n, té sentit considerar A^n. Ens interessa revisar d'una manera especial aquests conjunts.

• Per a qualsevol conjunt A i $n = 0$, A^0 és un conjunt d'un sol element; és a dir, un singletó. En efecte, hi ha una única aplicació de $\varnothing$ en A: l'aplicació buida de $\varnothing$ en A. Podem identificar, doncs, el singletó A^0 amb 1.

• Per a qualsevol conjunt A i $n = 1$, podem identificar A^1 amb A; en efecte, donar una aplicació de 1 en A equival a donar un element de A: la imatge de l'únic element de 1.

• En general, per a un conjunt A i un nombre natural $n \geq 1$, qualssevol, podem identificar A^n amb el producte de n còpies de A, $\overbrace{A \times \cdots \times A}^{n}$. En efecte, un element qualsevol $a = (a_0,\dots,a_{n-1}) \in \overbrace{A \times \cdots \times A}^{n}$ es pot identificar amb l'aplicació $a : n \longrightarrow A$ que envia el nombre natural k, $0 \leq k \leq n-1$, a l'element a_k de A (cf. la demostració de **1.2.5**).

• En particular, per a qualsevol conjunt A i $n = 2$, podem identificar A^2 amb $A \times A$, el producte de dues còpies de A. Els seus elements són les parelles ordenades (a,b) d'elements $a, b \in A$. Recordem que si $a, b \in A$ i $a \neq b$, llavors $(a,b) \neq (b,a)$, mentre que, com a subconjunts de A, és $\{a,b\} = \{b,a\}$.

1.1.3. Siguin A, B, C, D conjunts i $f : A \longrightarrow B$, $g : B \longrightarrow D$, $h : A \longrightarrow C$, $k : C \longrightarrow D$, aplicacions. Podem considerar les aplicacions composició $g \circ f$, $k \circ h : A \longrightarrow D$,

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle g\circ f}\searrow & \downarrow{\scriptstyle g} \\ & & D, \end{array} \qquad\qquad \begin{array}{ccc} A & & \\ {\scriptstyle h}\downarrow & \searrow{\scriptstyle k\circ h} & \\ C & \xrightarrow{k} & D, \end{array}$$

definides, per a tot $a \in A$, per $(g \circ f)(a) := g\big(f(a)\big)$ i per $(k \circ h)(a) := k\big(h(a)\big)$, respectivament. I pot succeir que sigui $g \circ f \neq k \circ h$, o bé que sigui $g \circ f = k \circ h$; en el primer cas, l'escriptura del diagrama

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{k} & D \end{array}$$

Diagrama 1.1: El diagrama és commutatiu si $k \circ h = g \circ f$.

és ambigua, perquè no és el mateix anar per dalt i la dreta que anar per l'esquerra i

per baix. En canvi, en el segon, l'escriptura no és ambigua i es diu que el diagrama és commutatiu. Només s'acostumen a escriure diagrames com aquest en el cas que siguin commutatius; ho farem així, llevat que especifiquem quelcom contrari.

1.2 Producte de conjunts

De les estructures algebraiques que tracta aquest curs —grups, anells, grups abelians—, ens interessa parlar de l'estructura producte corresponent —grup producte, anell producte, grup abelià producte—; i per a totes, el producte es basa en el conjunt producte. Estudiem-ne, doncs, la definició i recordem-ne les propietats principals.

Definició 1.2.1. Sigui $\{A_i\}_{i\in I}$ una família no buida de conjunts. Això és dir que I és un conjunt no buit i que per a cada $i \in I$ considerem un conjunt A_i. Un producte (també anomenat producte cartesià) de la família de conjunts $\{A_i\}_{i\in I}$ és un conjunt A i una família d'aplicacions $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$, anomenades les projeccions del producte A en els seus factors A_i, tals que per a tot conjunt B i tota família $\{\psi_i : B \longrightarrow A_i\}_{i\in I}$ d'aplicacions, existeix una única aplicació $\psi : B \longrightarrow A$ tal que tots els diagrames següents són commutatius:

$$\forall\{\psi_i\}_{i\in I}\ \exists!\psi\ \forall i \in I$$

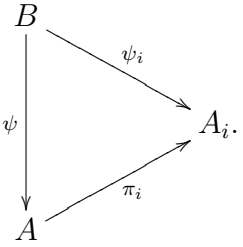
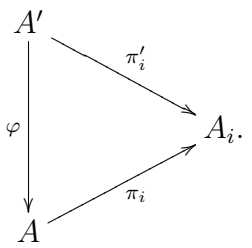


Diagrama 1.2: Propietat universal del producte de conjunts

1.2.2. Així, doncs, donar una aplicació ψ d'un conjunt en un producte equival a donar les seves projeccions $\psi_i = \pi_i \circ \psi$.

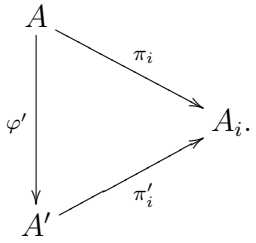
Observació 1.2.3. Notem que no sabem que el producte d'una família no buida de conjunts existeixi; només sabem que si per a algun conjunt A i alguna família d'aplicacions $\{\pi_i\}_{i\in I}$ se satisfà la propietat anterior, llavors hi ha producte de la família $\{A_i\}_{i\in I}$; però encara no n'hem provat l'existència, ni en general ni en cap cas particular. D'altra banda, fins i tot si suposem que hi ha existència, podem dir alguna cosa sobre la unicitat del producte? Comencem per veure que, en cas que existeixi, el producte és essencialment únic, amb la precisió del significat de l'adverbi "essencialment".

Proposició 1.2.4 (Unicitat del producte de conjunts)**.** *Sigui $\{A_i\}_{i\in I}$ una família no buida de conjunts, i suposem que $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$, $\{\pi'_i : A' \longrightarrow A_i\}_{i\in I}$, són productes de la família. Llavors, existeix una única aplicació $\varphi : A' \longrightarrow A$ tal que per a tot $i \in I$ és*



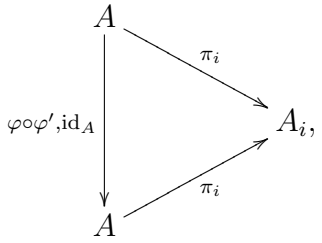
(1)

Aquesta aplicació φ és bijectiva i la seva inversa és l'única aplicació $\varphi' : A \longrightarrow A'$ tal que per a tot $i \in I$ és



(2)

Demostració: Per ser $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$ un producte, en considerar la família d'aplicacions $\{\pi'_i : A' \longrightarrow A_i\}_{i\in I}$ obtenim l'existència d'una única aplicació φ per a la qual el diagrama (1) és commutatiu per a tot $i \in I$. I anàlogament, per ser $\{\pi'_i : A' \longrightarrow A_i\}_{i\in I}$ un producte, en considerar la família d'aplicacions $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$ obtenim l'existència d'una única aplicació φ' per a la qual el diagrama (2) és commutatiu per a tot $i \in I$. En particular, per a les aplicacions id_A i $\varphi \circ \varphi'$, tenim la commutativitat de tots els diagrames



per a $i \in I$; i com que $\{\pi_i : A \longrightarrow A_i\}_{i\in i}$ és un producte, de la unicitat de la definició obtenim que $\varphi \circ \varphi' = \mathrm{id}_A$. I, anàlogament, per a les aplicacions $\mathrm{id}_{A'}$ i $\varphi' \circ \varphi$, obtenim que $\varphi' \circ \varphi = \mathrm{id}_{A'}$. Per tant, φ i φ' són aplicacions bijectives, i inverses l'una de l'altra. □

Proposició 1.2.5 (Existència del producte de conjunts)**.** *Sigui $\{A_i\}_{i\in I}$ una família no buida de conjunts. Llavors, existeix un producte $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$.*

Demostració: Considerem el conjunt $A := \prod_{i\in I} A_i$ de totes les famílies $\{a_i\}_{i\in I}$, amb $a_i \in A_i$ per a $i \in I$; és a dir, de totes les funcions d'elecció $a : I \longrightarrow \bigcup_{i\in I} A_i$ (cf. **A.1.2**).

Observació: Notem que l'axioma de l'elecció (cf. **A.1.1**) assegura que, si per a tot $i \in I$ és $A_i \neq \varnothing$, llavors $A \neq \varnothing$; però, en qualsevol cas, podem considerar el conjunt A, encara que no poguem dir si és o no buit. De seguida tornarem sobre aquesta qüestió.

Ara, per a tot $i \in I$, sigui $\pi_i : A \longrightarrow A_i$ l'aplicació donada per $\{a_k\}_{k\in I} \mapsto a_i$. Només cal comprovar la propietat universal del producte.

Suposem donats, doncs, un conjunt B i una família d'aplicacions $\{\psi_i : B \longrightarrow A_i\}_{i\in I}$. Definim l'aplicació $\psi : B \longrightarrow A$ per l'assignació $b \mapsto \{\psi_i(b)\}_{i\in I}$. Llavors, és clar que per a tot $i \in I$ i tot $b \in B$ és $\pi_i\big(\psi(b)\big) = \psi_i(b)$, i que aquesta aplicació $\psi : B \longrightarrow A$ és l'única per a la qual se satisfà aquesta propietat. □

Observació 1.2.6. Suposem que existeix algun conjunt $B \neq \varnothing$ i alguna família d'aplicacions $\{\psi_i : B \longrightarrow A_i\}_{i\in I}$. Llavors, per a tot $i \in I$ és $A_i \neq \varnothing$ i $A \neq \varnothing$, sense necessitat de l'axioma de l'elecció. En efecte, si $B \neq \varnothing$ i existeix una aplicació $\psi_i : B \longrightarrow A_i$, llavors $A_i \neq \varnothing$. I l'existència de $\psi : B \longrightarrow A$ tal que $\pi_i \circ \psi = \psi_i$ per a tot $i \in I$ implica que $A \neq \varnothing$, perquè hi ha una aplicació de $B \neq \varnothing$ en A.

Definició 1.2.7. El producte d'una família $\{A_i\}_{i\in I}$ es denota usualment per $\prod_{i\in I} A_i$. D'altra banda, l'aplicació $\psi : B \longrightarrow \prod_{i\in I} A_i$ determinada unívocament per les aplicacions $\psi_i : B \longrightarrow A_i$, $i \in I$, s'anomena l'aplicació producte de $\{\psi_i : B \longrightarrow A_i\}_{i\in I}$ i s'acostuma a denotar com $\psi =: \prod_{i\in I} \psi_i$. En particular, per al producte d'una quantitat finita de conjunts, $A_1, \ldots, A_n$, $n \in \mathbb{N}$, $n \geq 2$, el producte s'acostuma a denotar per $A_1 \times \cdots \times A_n$ i l'aplicació $\psi : B \longrightarrow A_1 \times \cdots \times A_n$ determinada per les projeccions $\psi_i : B \longrightarrow A_i$, $1 \leq i \leq n$, es denota per $\psi = \psi_1 \times \cdots \times \psi_n$ o també per $\psi = (\psi_1, \ldots, \psi_n)$.

Observació 1.2.8. Notem, també, que les projeccions $\pi_i : A \longrightarrow A_i$, són indexades pel conjunt I; per tant, encara que per a alguna parella $j, k \in I$, $j \neq k$, fos $A_j = A_k$, les projeccions π_j, π_k són diferents (si $\#A_j > 1$). En efecte, si $a, b \in A_j$ $a \neq b$, i considerem una família $\alpha := \{a_i\}_{i\in I} \in A$ tal que $a_j = a$, $a_k = b$, resulta que $\pi_j(\alpha) = a \neq b = \pi_k(\alpha)$, de manera que $\pi_j \neq \pi_k$.

Observació 1.2.9. Sigui A un conjunt no buit. Llavors, la identitat de $A \times A$ coincideix amb l'aplicació $(\pi_1, \pi_2) : A\times A \longrightarrow A\times A$ determinada per les projeccions $\pi_i : A\times A \longrightarrow A$ donades per $\pi_i(a_1, a_2) := a_i$, $i = 1, 2$. En canvi, l'aplicació $(\pi_2, \pi_1) : A \times A \longrightarrow A \times A$ és donada per $(a_1, a_2) \mapsto (a_2, a_1)$; és a dir, per transposició de les variables. En particular, si $\#A > 1$, llavors (π_2, π_1) no és la identitat de $A \times A$.

1.3 Concepte d'operació

Definició 1.3.1. Siguin $A \neq \varnothing$ un conjunt no buit i $n \geq 0$ un nombre natural. Una operació n-ària en A és una aplicació qualsevol $A^n \longrightarrow A$.

1.3.2. Mirem-nos amb una mica de deteniment alguns casos particulars especialment interessants.

• $n = 0$. Donar una operació 0-ària en un conjunt A equival a destacar un element de A. En efecte, podem identificar qualsevol element fixat $a \in A$ amb l'operació 0-ària

$$\begin{array}{rccc} a : A^0 & \longrightarrow & A. \\ \varnothing & \mapsto & a \end{array}$$

El concepte d'operació 0-ària serà útil per a parlar, per exemple, dels elements neutres (cf., més avall, **1.4.3**). Com a exemples d'operacions 0-àries, podem considerar les operacions

$$\begin{array}{rccc} 0 : \mathbb{Z}^0 & \longrightarrow & \mathbb{Z}, \\ \varnothing & \mapsto & 0 \end{array} \qquad \begin{array}{rccc} 1 : \mathbb{Z}^0 & \longrightarrow & \mathbb{Z}, \\ \varnothing & \mapsto & 1 \end{array}$$

que proporcionaran els elements neutres per a la suma i per a la multiplicació de nombres enters. Però també podem destacar altres elements; per exemple, el nombre π o el nombre e; ho faríem si consideréssim les operacions 0-àries, en el conjunt $\mathbb{R}$ dels nombres reals,

$$\begin{array}{rccc} \pi : \mathbb{R}^0 & \longrightarrow & \mathbb{R}, \\ \varnothing & \mapsto & \pi \end{array} \qquad \begin{array}{rccc} e : \mathbb{R}^0 & \longrightarrow & \mathbb{R}. \\ \varnothing & \mapsto & e \end{array}$$

• $n = 1$. Una operació 1-ària en A és qualsevol aplicació de A en A. Per exemple:

$$\begin{array}{ccccccccccccccc} \mathbb{N} & \longrightarrow & \mathbb{N}, & \mathbb{Z} & \longrightarrow & \mathbb{Z}, & \mathbb{Q} & \longrightarrow & \mathbb{Q}, & \mathbb{R} & \longrightarrow & \mathbb{R}, & \mathbb{R} & \longrightarrow & \mathbb{R}. \\ n & \mapsto & n^2 & n & \mapsto & 0 & a & \mapsto & a^2-3a+2 & r & \mapsto & e^{2\pi r} & a & \mapsto & \cos a \end{array}$$

Utilitzarem aviat el concepte d'operació 1-ària per a parlar d'elements inversos (cf., més avall, **1.4.5**). Com a exemples, podem considerar

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}, \\ n & \mapsto & -n \end{array} \qquad \begin{array}{ccc} \mathbb{Q}_{>0} & \longrightarrow & \mathbb{Q}_{>0}, \\ \frac{a}{b} & \mapsto & \frac{b}{a}, \end{array} \quad a,b \in \mathbb{Z},\ a,b>0,$$

oposats per a la suma de nombres enters i inversos per a la multiplicació de nombres racionals positius.

• $n = 2$. Les operacions que tenim més interioritzades com a tals són les operacions binàries. Donar una operació binària $f : A \times A \longrightarrow A$ en un conjunt no buit A és donar, per a cada parella ordenada (a, b) d'elements de A un element $f(a, b) \in A$.

El fet que les operacions binàries s'apliquin a parelles ordenades fa que, si $a \neq b$, pugui ser $f(a, b) \neq f(b, a)$, ja que $(a, b) \neq (b, a)$. Però també pot ser que per a tota parella d'elements $a, b \in A$ sigui $f(a, b) = f(b, a)$; en aquest cas, es diu que per a l'operació f se satisfà la propietat commutativa (cf., més avall, la propietat, a **1.4.1**).

Per a les operacions binàries se sol utilitzar una notació especial: el símbol d'operació es posa entre els dos elements que cal operar; així, per exemple, per a l'operació suma de nombres enters,

$$\begin{array}{ccc} + : \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}, \\ (a, b) & \mapsto & +(a, b) \end{array}$$

s'acostuma a escriure $a + b$ en lloc de $+(a, b)$. I anàlogament per a la majoria de les operacions binàries que es consideren.

Com a exemples d'operacions binàries molt habituals podem posar la suma de nombres naturals, la suma de nombres enters, la suma de nombres racionals, la suma de nombres reals, la multiplicació de nombres naturals, la multiplicació de nombres enters, la multiplicació de nombres racionals, o la multiplicació de nombres reals; totes aquestes operacions són commutatives.

Alguns altres exemples d'operacions binàries habituals són la suma vectorial en $\mathbb{Q}^n$,

$$\begin{array}{ccc} \mathbb{Q}^n \times \mathbb{Q}^n & \longrightarrow & \mathbb{Q}^n, \\ \big((a_0,\dots,a_{n-1}),(b_0,\dots,b_{n-1})\big) & \mapsto & (a_0+b_0,\dots,a_{n-1}+b_{n-1}) \end{array}$$

que és commutativa, o bé la potenciació-exponenciació en $\mathbb{N}$,

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N}, \\ (a, b) & \mapsto & a^b \end{array}$$

que no és commutativa (per exemple, $2^3 = 8 \neq 9 = 3^2$). Notem que per a una operació que no és commutativa encara pot haver-hi commutativitat per a certs valors dels operands (per exemple, $2^4 = 16 = 4^2$).

1.4 Propietats possibles per a operacions

Donats un conjunt no buit A, un nombre natural n i una operació n-ària en A, podem pensar en una multitud de propietats que es poden satisfer o no. Destacarem algunes de les propietats que són considerades habitualment; més concretament, les que farem servir més endavant.

1.4.1. Comencem per les propietats que volem destacar que pot tenir (o no) una operació binària $* : A \times A \longrightarrow A$ en un conjunt no buit A.

• **Commutativa.** Per a tots els elements $a, b \in A$, és $a * b = b * a$.

Una manera equivalent d'expressar aquesta propietat és dir que el diagrama següent de conjunts i aplicacions és commutatiu.

$$\begin{array}{ccc} A \times A & \xrightarrow{*} & A \\ {\scriptstyle \pi_2 \times \pi_1}\downarrow & & \downarrow{\scriptstyle id} \\ A \times A & \xrightarrow[*]{} & A \end{array}$$

Diagrama 1.3: Propietat commutativa

Aquí, $id : A \longrightarrow A$ és la identitat en A i $\pi_1 : A \times A \longrightarrow A$ i $\pi_2 : A \times A \longrightarrow A$ són les primera i segona projeccions, definides per $\pi_1(a, b) := a$, $\pi_2(a, b) := b$, respectivament, de manera que $\pi_2 \times \pi_1$ és l'aplicació determinada per l'assignació $(a, b) \mapsto (b, a)$.

• **Associativa.** Per a tots els elements $a, b, c \in A$, és $(a * b) * c = a * (b * c)$.

Anàlogament al cas de la propietat commutativa, una manera equivalent d'expressar la propietat associativa és dir que el diagrama següent de conjunts i aplicacions és commutatiu.

$$\begin{array}{ccc} A \times A \times A & \xrightarrow{\pi_1 \times *} & A \times A \\ {\scriptstyle * \times \pi_3}\downarrow & & \downarrow{\scriptstyle *} \\ A \times A & \xrightarrow[*]{} & A \end{array}$$

Diagrama 1.4: Propietat associativa

Observació 1.4.2. Notem que, formalment, hauríem d'escriure el diagrama en la forma

$$\begin{array}{ccc} A \times A \times A & \xrightarrow{\pi_1 \times *_{2,3}} & A \times A \\ {\scriptstyle *_{1,2} \times \pi_3}\downarrow & & \downarrow{\scriptstyle *} \\ A \times A & \xrightarrow[*]{} & A \end{array}$$

on $*_{2,3} : A \times A \longrightarrow A$ és la composició de l'aplicació $\pi_2 \times \pi_3 : A \times A \times A \longrightarrow A \times A$ seguida de $* : A \times A \longrightarrow A$; és a dir, el producte sobre les dues darreres projeccions. I anàlogament per a $*_{1,2}$. Però el context ja deixa clar quines són aquestes aplicacions, i ens podem estalviar un excés de formalisme que faria la notació més feixuga sense millorar la comprensió del fenomen.

1.4.3. Mirem-nos, ara, algunes propietats que es poden satisfer o no per a una operació binària $* : A \times A \longrightarrow A$ i una operació 0-ària $e : A^0 \longrightarrow A$.

• **Element neutre per l'esquerra.** Per a tot element $a \in A$ és $e * a = a$. Si se satisfà, es diu que e és un element neutre per l'esquerra per a $*$. La propietat es pot expressar per la commutativitat del diagrama següent.

$$\begin{array}{ccc} A^0 \times A & \xrightarrow{e\times\pi_2} & A \times A \\ {\scriptstyle u\times id}\uparrow & & \downarrow{\scriptstyle *} \\ A & \xrightarrow[id]{} & A \end{array}$$

Diagrama 1.5: Element neutre per l'esquerra

Aquí, i més endavant, l'aplicació $u : A \longrightarrow A^0$ és l'única aplicació possible, que envia tots els elements de A a l'únic element de A^0.

• **Element neutre per la dreta.** Per a tot element $a \in A$ és $a * e = a$. Si se satisfà, es diu que e és un element neutre per la dreta per a $*$. La propietat es pot expressar per la commutativitat del diagrama següent.

$$\begin{array}{ccc} A \times A^0 & \xrightarrow{\pi_1\times e} & A \times A \\ {\scriptstyle id\times u}\uparrow & & \downarrow{\scriptstyle *} \\ A & \xrightarrow[id]{} & A \end{array}$$

Diagrama 1.6: Element neutre per la dreta

• **Element neutre.** Per a tot element $a \in A$ és $e * a = a$ i $a * e = a$. Si se satisfan, es diu que e és un element neutre per a $*$. La propietat es pot expressar per la commutativitat simultània dels dos diagrames anteriors.

$$\begin{array}{ccccc} A^0 \times A & \xleftarrow{u\times id} & A & \xrightarrow{id\times u} & A \times A^0 \\ {\scriptstyle e\times\pi_2}\downarrow & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \pi_1\times e} \\ A \times A & \xrightarrow[*]{} & A & \xleftarrow[*]{} & A \times A \end{array}$$

Diagrama 1.7: Element neutre

Observació 1.4.4. Notem que hem formulat les propietats d'element neutre com propietats associades a l'existència d'una operació 0-ària per a la qual se satisfan les propietats de commutació dels diagrames corresponents. Sovint les propietats d'element neutre es formulen com l'existència d'un element $e \in A$ per al qual se satisfan els axiomes corresponents.

Les dues formulacions són, òbviament, equivalents, perquè si existeix un element $e \in A$ per a la qual se satisfan els axiomes, es pot definir l'operació 0-ària com l'única aplicació $A^0 \longrightarrow A$ que envia $\varnothing$ a e; i, recíprocament, donada l'operació 0-ària, la imatge de $\varnothing$ per l'operació demostra l'existència d'un element $e \in A$ per al qual se satisfan els axiomes.

1.4.5. Mirem-nos, ara, algunes propietats que es poden satisfer o no per a una operació binària, $* : A \times A \longrightarrow A$, una operació 0-ària, $e : A^0 \longrightarrow A$, i una operació 1-ària, $i : A \longrightarrow A$.

• **Element invers per l'esquerra.** Per a tot element $a \in A$ és $i(a) * a = e$. Si se satisfà, es diu que $i(a)$ és l'invers per l'esquerra de a per a $*$ i e, o bé l'element simètric per l'esquerra de a per a $*$ i e. La propietat es pot expressar per la commutativitat del diagrama següent.

$$\begin{array}{ccc} A & \xrightarrow{i\times id} & A \times A \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle *} \\ A^0 & \xrightarrow[e]{} & A \end{array}$$

Diagrama 1.8: Element invers per l'esquerra

• **Element invers per la dreta.** Per a tot element $a \in A$ és $a * i(a) = e$. Si se satisfà, es diu que $i(a)$ és l'invers per la dreta de a per a $*$ i e, o bé l'element simètric per la dreta de a per a $*$ i e. La propietat es pot expressar per la commutativitat del diagrama següent.

$$\begin{array}{ccc} A & \xrightarrow{id\times i} & A \times A \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle *} \\ A^0 & \xrightarrow[e]{} & A \end{array}$$

Diagrama 1.9: Element invers per la dreta

• **Element invers.** Per a tot element $a \in A$ és $i(a) * a = e$ i $a * i(a) = e$. Si se satisfan, es diu que $i(a)$ és l'invers de a per a $*$ i e, o bé l'element simètric de a per a $*$ i e. La propietat es pot expressar per la commutativitat dels dos diagrames anteriors:

$$\begin{array}{ccccc} A \times A & \xleftarrow{i\times id} & A & \xrightarrow{id\times i} & A \times A \\ {\scriptstyle *}\downarrow & & {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle *} \\ A & \xleftarrow[e]{} & A^0 & \xrightarrow[e]{} & A \end{array}$$

Diagrama 1.10: Element invers

Observació 1.4.6. De manera semblant al cas de les propietats d'element neutre, hem formulat les propietats d'element invers com propietats associades a l'existència d'una operació 1-ària per a la qual se satisfan les propietats de commutació dels diagrames corresponents. Sovint, les propietats d'element invers es formulen com l'existència, per a cada element $a \in A$, d'un element $a^{-1} \in A$ per al qual se satisfan els axiomes corresponents. Això permet definir l'aplicació $i : A \longrightarrow A$ com aquella que envia cada element $a \in A$ al corresponent element a^{-1}. Notem, però, que, a fi que això sigui possible, cal que hi hagi unicitat dels elements inversos; en cas contrari, caldria poder triar d'alguna manera les imatges a fi de definir bé l'aplicació.

1.4.7. Mirem-nos, finalment, algunes propietats que es poden satisfer o no per a dues operacions binàries $* : A \times A \longrightarrow A$ i $\oplus : A \times A \longrightarrow A$.

• **Distributiva per l'esquerra de $*$ respecte a $\oplus$.** Per a tos els elements $a, b, c \in A$ és $a * (b \oplus c) = (a * b) \oplus (a * c)$. La propietat es pot expressar per la commutativitat del diagrama següent, en el qual el context deixa clares les definicions de les aplicacions.

$$\begin{array}{ccccc} A \times A \times A & & \xrightarrow{\quad\pi_1 \times \oplus\quad} & & A \times A \\ \Big\downarrow{\scriptstyle \pi_1\times\pi_2\times\pi_1\times\pi_3} & & & & \Big\downarrow{\scriptstyle *} \\ A \times A \times A \times A & \xrightarrow[*\times *]{} & A \times A & \xrightarrow[\oplus]{} & A \end{array}$$

Diagrama 1.11: Propietat distributiva per l'esquerra

• **Distributiva per la dreta de $*$ respecte a $\oplus$.** Per a tos els elements $a, b, c \in A$ és $(a \oplus b) * c = (a * c) \oplus (b * c)$. La propietat es pot expressar per la commutativitat del diagrama següent. De nou, el context deixa clares les definicions de les aplicacions.

$$\begin{array}{ccccc} A \times A \times A & & \xrightarrow{\quad\oplus\times\pi_3\quad} & & A \times A \\ \Big\downarrow{\scriptstyle \pi_1\times\pi_3\times\pi_2\times\pi_3} & & & & \Big\downarrow{\scriptstyle *} \\ A \times A \times A \times A & \xrightarrow[*\times *]{} & A \times A & \xrightarrow[\oplus]{} & A \end{array}$$

Diagrama 1.12: Propietat distributiva per la dreta

• **Distributiva de $*$ respecte a $\oplus$.** Per a tos els elements $a, b, c \in A$ és $a * (b \oplus c) = (a * b) \oplus (a * c)$ i $(a \oplus b) * c = (a * c) \oplus (b * c)$. La propietat es pot expressar per la commutativitat dels dos diagrames anteriors, que no repetim.

1.5 Operacions associatives

Siguin A un conjunt amb una operació binària $\otimes$, i $a_0, \ldots, a_n \in A$ elements qualssevol. Té sentit la notació $a_0 \otimes a_1 \otimes \cdots \otimes a_n$? Quin sentit té? O potser no en té, en general?

Tot i que aquestes poden semblar preguntes trampa, convé fixar-nos bé en la resposta que donarem. En efecte, estem habituats a veure expressions del tipus

$$a_0 + \cdots + a_n, \qquad \sum_{i=0}^{n} a_i, \qquad a_0 \cdots a_n, \qquad \text{o bé} \qquad \prod_{i=0}^{n} a_i;$$

per exemple, en el cas de suma o multiplicació de nombres enters, racionals, reals o complexos, o en el cas de sumes de vectors. I possiblement no ens hem aturat gaire a pensar detingudament quin sentit tenen. Hem fet malament? Hem comès algun error?

La resposta és que no hem comès cap error en aquests casos, perquè les operacions són associatives. Però, per exemple, per a l'operació binària en $\mathbb{N}$ donada per $(a, b) \mapsto a^b$ (cf. el darrer exemple en **1.3.2**), cal saber molt bé que a^{b^c} significa $a^{(b^c)}$ i no $(a^b)^c$. Per tant, en general, l'escriptura d'operacions binàries sense els parèntesis no admet la lectura en qualsevol ordre.

Definició 1.5.1. Siguin A un conjunt amb una operació binària associativa, $\otimes$, i considerem una successió finita d'elements $a_0, \ldots, a_n \in A$, $n \geq 0$. Definim, per inducció sobre n, els productes $\bigotimes_{i=0}^{0} a_i := a_0$, per a $n = 0$, i $\bigotimes_{i=0}^{n} a_i := a_0 \otimes \bigotimes_{i=1}^{n} a_i$, per a $n \geq 1$. En particular, si $a_0 = a_1 = \cdots = a_{n-1} = a \in A$, obtenim la definició de $a^{\otimes n} := \overbrace{a \otimes \cdots \otimes a}^{n}$, per a $n \geq 1$.

Exercici 1.5.2. Siguin A un conjunt amb una operació binària associativa, $\otimes$, i considerem una successió finita d'elements $a_0, \ldots, a_n \in A$, $n \geq 1$. Llavors,

$$a_0 \otimes \big(a_1 \otimes \big(\cdots \otimes (a_{n-1} \otimes a_n) \cdots\big)\big) = \big(\cdots \big((a_0 \otimes a_1) \otimes a_2\big) \otimes \cdots a_{n-1}\big) \otimes a_n;$$

és a dir, per a una operació associativa, hauríem pogut definir el producte, de manera equivalent, com $\bigotimes_{i=0}^{n} a_i = \left(\bigotimes_{i=0}^{n-1} a_i\right) \otimes a_n$, per a $n \geq 1$.

Exercici 1.5.3. Siguin A un conjunt amb una operació binària associativa, $\otimes$, i considerem una successió finita d'elements $a_0, \ldots, a_n, a_{n+1}, \ldots, a_{n+m} \in A$, $n, m \geq 1$. Llavors,

$$\bigotimes_{i=0}^{n+m} a_i = \left(\bigotimes_{i=0}^{n} a_i\right) \otimes \left(\bigotimes_{i=1}^{m} a_{n+i}\right).$$

Observació 1.5.4. Es pot demostrar (i no és difícil) que si A és un conjunt amb una operació associativa, $\otimes$, i considerem una successió finita d'elements $a_0, \ldots, a_n \in A$, el producte $\bigotimes_{i=0}^{n} a_i$ es pot calcular posant els elements ordenats en la forma $a_0 \otimes \cdots \otimes a_n$, i agrupant-los amb els parèntesis posats de qualsevol manera (cf. [Artin 1991, cap. 2.1], [Bourbaki 1970, cap. I, §1, n. 2, 3], [Jacobson 1974, cap. 1.4], [Lang 1971, cap. 1.1], o bé [Queysanne 1971, cap. 3, ex. 42]).

Observació 1.5.5. Només utilitzarem aquesta notació per a l'operació d'una successió finita —i ordenada— d'elements en el cas d'operacions associatives; si no ho són, caldrà fer explícit, en cada cas, el sentit exacte de la notació.

1.6 Estructures algebraiques bàsiques

Un cop revisats els conceptes més bàsics de conjunts, aplicacions i operacions, és un bon moment per a definir les estructures algebraiques més bàsiques amb què treballem.

Definició 1.6.1. Un grup $(G, *, e, i)$ és un conjunt no buit G amb tres operacions: una operació binària $* : G \times G \longrightarrow G$, que anomenarem, genèricament, el producte del grup, una operació 0-ària, $e : G^0 \longrightarrow G$, que anomenarem, genèricament, el neutre del grup, i una operació 1-ària, $i : G \longrightarrow G$ que anomenarem, genèricament, l'invers o el simètric del grup, per a les quals se satisfan les propietats següents: associativa de $*$ (cf. **1.4.1**); e és element neutre per a $*$ (cf. **1.4.3**); i i és invers per a $*$ i e (cf. **1.4.5**). Si, a més a més, el producte és commutatiu (cf. **1.4.1**), el grup s'anomena commutatiu (o també, abelià).

Observació 1.6.2. Per als grups commutatius, moltes vegades, però no sempre, s'utilitza la notació additiva; és a dir, s'escriu $+$ per a l'operació binària que, en aquest cas, s'anomena suma; s'escriu 0 per a l'element neutre, i s'anomena zero; i s'escriu $-a$ per a l'invers de a que, en aquest cas, s'anomena oposat.

Sovint s'utilitza la notació multiplicativa; i no només en el cas general, sinò també en el cas commutatiu. Quan es fa servir aquesta notació multiplicativa, l'operació binària s'escriu amb un punt volat o bé per juxtaposició, i s'anomena multiplicació o producte, l'element neutre es denota per 1, i s'anomena u, i els elements inversos es denoten per a^{-1}, o bé per $\dfrac{1}{a}$, i s'anomenen simplement inversos, o inversos multiplicatius.

I altres vegades s'utilitzen altres notacions; per exemple, per a conjunts d'aplicacions, l'operació binària habitual s'anomena composició i es denota per $\circ$, l'element neutre s'anomena identitat i es denota per id, o per 1, i l'element invers es denota per a^{-1}.

En els exemples següents veurem algunes d'aquestes notacions diferents.

Exemples 1.6.3. Els primers exemples que s'acostumen a posar de grups ho són de grups commutatius; de fet, la majoria són els grups additius d'alguns anells (cf. la definició d'anell més endavant, **1.6.5**) o d'estructures lineals (mòduls o espais vectorials, cf. **1.8.1**); probablement, no siguin els millors exemples de grups com a tals, però, per la seva importància, no podem obviar-los.

• $(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}, +, 0, -)$, $(\mathbb{R}, +, 0, -)$, on $+$ és la suma usual en cadascun dels conjunts $\mathbb{Z}$, dels nombres enters, $\mathbb{Q}$, dels nombres racionals, o $\mathbb{R}$, dels nombres reals. L'element neutre de tots els grups és 0, en cada cas ($0 \in \mathbb{Z}$, $0 \in \mathbb{Q}$, o $0 \in \mathbb{R}$, respectivament), i l'oposat és l'aplicació que canvia el signe, definida, també en cada cas, per $x \mapsto -x$.

• $(\mathbb{Q}_{\neq 0}, \cdot, 1, (\ )^{-1})$, $(\mathbb{Q}_{>0}, \cdot, 1, (\ )^{-1})$, $(\mathbb{R}_{\neq 0}, \cdot, 1, (\ )^{-1})$, $(\mathbb{R}_{>0}, \cdot, 1, (\ )^{-1})$, on $\cdot$ és la multiplicació usual, cadascuna en el conjunt corresponent (dels nombres racionals no nuls, $\mathbb{Q}_{\neq 0}$, dels nombres racionals estrictament positius, $\mathbb{Q}_{>0}$, dels nombres reals no nuls, $\mathbb{R}_{\neq 0}$, o dels nombres reals estrictament positius, $\mathbb{R}_{>0}$), i on, en cada cas, l'element neutre per a la multiplicació és el corresponent 1 ($1 \in \mathbb{Q}_{\neq 0}$, $1 \in \mathbb{Q}_{>0}$, $1 \in \mathbb{R}_{\neq 0}$, $1 \in \mathbb{R}_{>0}$), i l'invers multiplicatiu, $(\ )^{-1}$, és donat, en cada cas, per l'aplicació $x \mapsto x^{-1} := 1/x$.

• $(\mathbb{Z}^3, +, 0, -)$, on $+, 0, -$ són la suma vectorial usual, $+ : \mathbb{Z}^3 \times \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$, donada per $(a_0, a_1, a_2) + (b_0, b_1, b_2) = (a_0 + b_0, a_1 + b_1, a_2 + b_2)$; el zero, $0 := (0, 0, 0) \in \mathbb{Z}^3$; i l'oposat, $- : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$, donat per $-(a_0, a_1, a_2) = (-a_0, -a_1, -a_2)$, en el conjunt de les ternes ordenades de nombres enters.

• Per a tot nombre natural $n \geq 0$, tenim el grup additiu $(\mathbb{Q}^n, +, 0, -)$, on $+, 0, -$ són la suma vectorial usual en $\mathbb{Q}^n$, $+ : \mathbb{Q}^n \times \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$, determinada per l'assignació $(a_0, a_1, \ldots, a_{n-1}) + (b_0, b_1, \ldots, b_{n-1}) := (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})$; el zero, determinat per $0 := (0, 0, \ldots, 0) \in \mathbb{Q}^n$; i l'oposat, l'aplicació $- : \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$ determinada per l'assignació $-(a_0, a_1, \ldots, a_{n-1}) := (-a_0, -a_1, \ldots, -a_{n-1})$, ara en el conjunt de les n-ples de nombres racionals.

• El grup de dos elements, $(C_2, +, 0, -)$, on $C_2 := \{0, 1\}$, l'operació $+ : C_2 \times C_2 \longrightarrow C_2$ és donada per

$$0 + 0 := 0, \quad 0 + 1 := 1, \quad 1 + 0 := 1, \quad 1 + 1 := 0;$$

0 és l'element $0 \in C_2$, i $- : C_2 \longrightarrow C_2$ és la identitat (és a dir, $-0 := 0$ i $-1 := 1$). En efecte, $(C_2, +, 0, -)$ és un grup commutatiu. La comprovació que 0 és l'element neutre i que $-$ és l'oposat són immediates, i la comprovació de la propietat associativa és un

exercici senzill: podem escriure les vuit sumes possibles de tres sumands i comprovar que se satisfà la propietat:

$$\begin{array}{llllll}
0+(0+0)= & 0+0 & =0 & =0+0 & =(0+0)+0,\\
0+(0+1)= & 0+1 & =1 & =0+1 & =(0+0)+1,\\
0+(1+0)= & 0+1 & =1 & =1+0 & =(0+1)+0,\\
0+(1+1)= & 0+0 & =0 & =1+1 & =(0+1)+1,\\
1+(0+0)= & 1+0 & =1 & =1+0 & =(1+0)+0,\\
1+(0+1)= & 1+1 & =0 & =1+1 & =(1+0)+1,\\
1+(1+0)= & 1+1 & =0 & =0+0 & =(1+1)+0,\\
1+(1+1)= & 1+0 & =1 & =0+1 & =(1+1)+1.
\end{array}$$

• El grup de dos elements es pot veure com $(\{1,-1\},*,1,\mathrm{id})$, amb el poducte donat per

$$1*1=1,\quad 1*(-1)=-1,\quad (-1)*1=-1,\quad (-1)*(-1)=1,$$

on 1 és l'element neutre i cada element és el seu propi invers. La comprovació és anàloga al cas anterior.

Exemples 1.6.4. Més exemples de grups; aquests, en general, no commutatius.

• $(S_3,\circ,\mathrm{id},\mathrm{inv})$, on S_3 és el conjunt de les permutacions d'un conjunt de tres elements (aplicacions bijectives de $\{0,1,2\}$ en $\{0,1,2\}$), $\circ : S_3\times S_3 \longrightarrow S_3$ és la composició habitual d'aplicacions, $\mathrm{id}\in S_3$ és l'aplicació identitat en $\{0,1,2\}$, i $\mathrm{inv} : S_3 \longrightarrow S_3$ és l'aplicació que a cada permutació σ li fa correspondre la seva inversa σ^{-1} (notem que una aplicació bijectiva admet una inversa, que també és una aplicació bijectiva; és a dir, tota permutació admet una permutació inversa per al producte de permutacions).

• En general, el conjunt de les aplicacions bijectives d'un conjunt A en si mateix, $\mathrm{Bij}(A)$, amb la composició d'aplicacions, la identitat i l'aplicació inversa, constitueixen un grup. El grup S_3 de l'exemple anterior és el cas particular $A=\{0,1,2\}$. Aquests grups només són commutatius en el cas en què el conjunt A sigui buit, o bé que tingui un o dos elements; si A té estrictament més de dos elements, aquest grup no és commutatiu.

• Per a tot $n\geq 2$, el conjunt de les matrius quadrades invertibles de n files i n columnes i coeficients racionals, $\mathbf{GL}(n,\mathbb{Q})$, amb el producte usual de matrius, la matriu identitat com a element neutre, i l'aplicació que a cada matriu li associa la seva matriu inversa, és un grup, que és no commutatiu si $n\geq 2$; per exemple,

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}\cdot\begin{bmatrix}0&-1\\1&0\end{bmatrix}=\begin{bmatrix}1&-1\\1&0\end{bmatrix}\neq\begin{bmatrix}0&-1\\1&1\end{bmatrix}=\begin{bmatrix}0&-1\\1&0\end{bmatrix}\cdot\begin{bmatrix}1&1\\0&1\end{bmatrix},$$

per a $n=2$, i afegint la identitat de $n-2$ files i columnes a continuació de totes aquestes matrius, per a $n\geq 2$ qualsevol.

• També és un grup el conjunt de les matrius quadrades de n files i n columnes, coeficients racionals i determinant 1, amb el producte usual de matrius, la matriu identitat com a element neutre, i l'aplicació que a cada matriu li associa la seva matriu inversa. L'exemple anterior mostra que per a $n\geq 2$ aquest grup no és commutatiu. Es denota per $\mathbf{SL}(n,\mathbb{Q})$.

Definició 1.6.5. Un anell $(A,+,\cdot,0,1,-)$ és un grup commutatiu, que denotarem additivament, $(A,+,0,-)$ juntament amb una altra operació binària $\cdot : A\times A\longrightarrow A$, que anomenarem producte, que sigui associativa i distributiva respecte de la suma, i una altra operació 0-ària, que anomenarem 1, que sigui neutre per al producte. Si, a més a més, el producte és commutatiu, direm que l'anell és commutatiu. No es parla d'anells abelians!

Exemples 1.6.6. Alguns exemples bàsics d'anells, commutatius els primers, no commutatius els darrers, són els següents.

• $(\mathbb{Z}, +, \cdot, 0, 1, -)$, $(\mathbb{Q}, +, \cdot, 0, 1, -)$, $(\mathbb{R}, +, \cdot, 0, 1, -)$, els anells dels nombres enters, dels nombres racionals i dels nombres reals, amb la suma i la multiplicació usuals, amb neutres 0 per a la suma i 1 per a la multiplicació, i on l'oposat per a la suma és donat pel canvi de signe. Aquests anells són commutatius.

• L'anell de dos elements, $(C_2, +, \cdot, 0, 1, -)$, és l'anell definit en el conjunt $C_2 := \{0, 1\}$ de manera que $(C_2, +, 0, -)$ és el grup de dos elements de l'exemple corresponent de **1.6.3**, l'operació $\cdot$ és donada per

$$0 \cdot 0 := 0, \quad 0 \cdot 1 := 0, \quad 1 \cdot 0 := 0, \quad 1 \cdot 1 := 1;$$

i 1 és l'element $1 \in C_2$. La comprovació de les propietats d'anell es pot fer de manera semblant com s'han comprovat les de grup commutatiu amb la suma i es deixa com a exercici. Aquest anell és commutatiu.

• En tot anell se satisfà que per a tot element $a \in A$ és $0 \cdot a = a \cdot 0 = 0$. En efecte, per a tot element $a \in A$ és $0 + 0 \cdot a = 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, de manera que, en sumar l'oposat de $0 \cdot a$ i simplificar l'element 0 que en resulta, obtenim que $0 = 0 \cdot a$. I anàlogament per a $0 = a \cdot 0$.

• Si en un anell és $1 = 0$, llavors $A = \{0\}$. En efecte, per a tot element $a \in A$ es té que $a = 1 \cdot a = 0 \cdot a = 0$.

• Sigui $(K, +, \cdot, 0, 1, -)$ un anell commutatiu. Definim el conjunt de polinomis en la indeterminada X i coeficients en K, que escriurem en la forma $K[X]$, com el conjunt de les sumes formals

$$p(X) := \sum_{k=0}^{n} a_k X^k$$

(o sigui, expressions d'aquesta forma), amb $n \geq 0$ i $a_k \in K$ per a tot k. Donats polinomis $p(X)$ i

$$q(X) := \sum_{k=0}^{m} b_k X^k, \qquad b_k \in K,$$

definim la seva suma com el polinomi

$$(p + q)(X) := \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k,$$

on $a_k := 0$, si $k > n$ i $b_k = 0$, si $k > m$; definim el seu producte com el polinomi

$$(p \cdot q)(X) := \sum_{k=0}^{n+m} c_k X^k,$$

on

$$c_k := \sum_{i+j=k} a_i \cdot b_j;$$

i definim el polinomi $(-p)(X)$ per

$$(-p)(X) := \sum_{k=0}^{n} (-a_k) X^k.$$

Llavors, $(K[X], +, \cdot, 0, 1, -)$, on $0 \in K[X]$ i $1 \in K[X]$ són les sumes formals amb un sol sumand, $0, 1 \in K$, respectivament, és un anell commutatiu. S'anomena l'anell dels polinomis en la indeterminada X i coeficients en K. Els casos particulars que ens interessaran més són els casos en què l'anell de coeficients és l'anell dels nombres enters o bé un cos qualsevol (cf. la definició de cos, **1.6.7**).

Observació: Notem que hem suposat que l'anell de coeficients és commutatiu; això no és pas necessari. De fet, més endavant veurem una definició més formal de l'anell de polinomis (cf. **6.1.1**), sense suposar la commutativitat de l'anell de coeficients.

• $(\mathbf{M}(2, \mathbb{Z}), +, \cdot, 0, 1, -)$: l'anell de les matrius quadrades de dues files i dues columnes i coeficients enters, amb la suma i el producte habituals de matrius, + i ·, on 0 és la matriu $0 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $1 := \mathrm{id} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ és la matriu identitat, i $-\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$. Notem que aquest anell no és commutatiu; serveix com a exemple el mateix de més amunt (cf. **1.6.4**):

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

• Per a tot nombre natural $n \geq 1$, podem considerar els anells, que són no commutatius si $n > 1$, $(\mathbf{M}(n, \mathbb{Z}), +, \cdot, 0, 1, -)$, $(\mathbf{M}(n, \mathbb{Q}), +, \cdot, 0, 1, -)$, o $(\mathbf{M}(n, \mathbb{R}), +, \cdot, 0, 1, -)$, de les matrius de n files i n columnes i coeficients enters, racionals o reals, respectivament, amb les operacions habituals de suma i de multiplicació de matrius, on la matriu 0 és la matriu que té tots els coeficients iguals a 0, la matriu 1 és la identitat de n files i n columnes (amb 1 a la diagonal principal de la matriu i 0 fora de la diagonal), i on l'oposat per a la suma és donat per la matriu que s'obté en canviar el signe dels coeficients.

Definició 1.6.7. Un cos $(K, +, \cdot, 0, 1, -, (\ )^{-1})$, és un anell commutatiu $(K, +, \cdot, 0, 1, -)$ tal que $1 \neq 0$ juntament amb una operació 1-ària $(\ )^{-1} : K_{\neq 0} \longrightarrow K_{\neq 0}$ que sigui invers per a $\cdot$ i 1. Notem que això demana que, necessàriament, s'ha de poder restringir el producte a $K_{\neq 0} = K - \{0\}$, ja que hem de parlar de l'invers respecte del producte en $K_{\neq 0}$ i el neutre 1 en $K_{\neq 0}$. D'altra banda, també es demana la commutativitat de la multiplicació.

Exemples 1.6.8. Alguns exemples de cossos són els següents.

• L'anell $(\mathbb{Q}, +, \cdot, 0, 1, -, (\ )^{-1})$, dels nombres racionals, juntament amb l'invers multiplicatiu usual, és un cos.

• Anàlogament, l'anell $(\mathbb{R}, +, \cdot, 0, 1, -, (\ )^{-1})$, dels nombres reals, juntament amb l'invers multiplicatiu usual, és un cos.

• L'anell $(C_2, +, \cdot, 0, 1, -, (\ )^{-1})$, amb l'únic invers multiplicatiu possible, $1^{-1} := 1$, també és un cos. Notem que en aquest cos és $1 + 1 = 0$.

• En canvi, no hi ha cap invers multiplicatiu $(\ )^{-1} : \mathbb{Z}_{\neq 0} \longrightarrow \mathbb{Z}_{\neq 0}$ que faci de l'anell $(\mathbb{Z}, +, \cdot, 0, 1, -)$ un cos $(\mathbb{Z}, +, \cdot, 0, 1, -, (\ )^{-1})$; en efecte, per a la multiplicació usual, els únics nombres enters per als quals hi ha invers multiplicatiu són 1 i -1 que, a més a més, són els seus propis inversos.

• Tampoc no és un cos l'anell de polinomis en una indeterminada i coeficients en un anell commutatiu per al qual sigui $0 \neq 1$, ni tan sols en el cas en què l'anell de coeficients és un cos. Per exemple, no hi ha cap polinomi que multiplicat pel polinomi X sigui el polinomi 1, de manera que el polinomi X no admet invers multiplicatiu.

1.7 Concepte d'acció

Definició 1.7.1 (Acció d'un conjunt en un altre)**.** Siguin A, B conjunts, $A \neq \varnothing$. Una acció de A en B és una aplicació qualsevol $A \times B \longrightarrow B$.

Exemples 1.7.2. Comentem alguns exemples bàsics d'accions.

• Si A és un conjunt no buit i $n \geq 1$, tota operació n-ària en A és una acció de A^{n-1} en A. En particular, tota operació binària d'un conjunt no buit A és una acció de A en si mateix.

• (Potències d'exponents naturals, o multiplicacions per nombres naturals.) Si A és un conjunt no buit amb una operació binària associativa $*$ i amb neutre e, el conjunt dels nombres naturals actua en A de la manera

$$(0, a) \mapsto a^0 := e, \qquad (n, a) \mapsto a^n := \overbrace{a * \cdots * a}^{n}, \quad n \geq 1.$$

Notem que si l'operació no fos associativa, caldria definir el concepte de potència amb molta més cura; per exemple, caldria determinar si a^3 significa $(a*a)*a$ o bé $a*(a*a)$, o bé alguna altra cosa (cf. més amunt, **1.5.1**). Notem, també, que si denotem l'operació de manera additiva, amb el signe $+$, llavors l'acció és la multiplicació per un nombre natural: $n \cdot a = \overbrace{a + \cdots + a}^{n}$.

• El conjunt dels nombres racionals actua en $\mathbb{Q}^n$ per multiplicació escalar de la manera següent:

$$\mathbb{Q} \times \mathbb{Q}^n \longrightarrow \mathbb{Q}^n, \qquad \big(r, (a_0, a_1, \ldots, a_{n-1})\big) \mapsto (r \cdot a_0, r \cdot a_1, \ldots, r \cdot a_{n-1}).$$

Accions anàlogues es poden considerar per a $\mathbb{Z}$ o $\mathbb{R}$ en lloc de $\mathbb{Q}$:

$$\mathbb{Z} \times \mathbb{Z}^n \longrightarrow \mathbb{Z}^n, \qquad \big(r, (a_0, a_1, \ldots, a_{n-1})\big) \mapsto (r \cdot a_0, r \cdot a_1, \ldots, r \cdot a_{n-1});$$

$$\mathbb{R} \times \mathbb{R}^n \longrightarrow \mathbb{R}^n, \qquad \big(r, (a_0, a_1, \ldots, a_{n-1})\big) \mapsto (r \cdot a_0, r \cdot a_1, \ldots, r \cdot a_{n-1});$$

o bé accions de $\mathbb{Z}$ en $\mathbb{Q}^n$ o en $\mathbb{R}^n$; o bé accions de $\mathbb{Q}$ en $\mathbb{R}^n$.

• El conjunt dels nombres enters actua en qualsevol grup commutatiu $(G, +, 0, -)$ via l'aplicació

$$\mathbb{Z} \times G \longrightarrow G, \qquad (n, a) \mapsto n \cdot a := \begin{cases} 0, & \text{si } n = 0, \\ \overbrace{a + \cdots + a}^{n}, & \text{si } n > 0, \\ \overbrace{(-a) + \cdots + (-a)}^{-n}, & \text{si } n < 0. \end{cases}$$

Observació 1.7.3. Notem que tenir una acció de A en B, $\Phi : A \times B \longrightarrow B$, implica tenir, per a cada element $a \in A$, una operació 1-ària $h_a : B \longrightarrow B$, donada per $h_a(b) := \Phi(a, b)$, per a tot element $b \in B$.

I recíprocament, a qualsevol família $\{h_a : B \longrightarrow B\}_{a \in A}$ d'operacions 1-àries, podem associar-li una acció $\Phi : A \times B \longrightarrow B$ per $\Phi(a, b) := h_a(b)$.

1.7.4. Així, per exemple, tenir l'acció de multiplicació escalar en $\mathbb{Q}^n$,

$$\mathbb{Q} \times \mathbb{Q}^n \longrightarrow \mathbb{Q}^n, \qquad \big(r, (a_0, a_1, \ldots, a_{n-1})\big) \mapsto (r \cdot a_0, r \cdot a_1, \ldots, r \cdot a_{n-1}),$$

equival a tenir la família de totes les homotècies

$$h_r : \mathbb{Q}^n \longrightarrow \mathbb{Q}^n, \qquad (a_0, a_1, \ldots, a_{n-1}) \mapsto (r \cdot a_0, r \cdot a_1, \ldots, r \cdot a_{n-1}), \qquad r \in \mathbb{Q}.$$

1.8 Estructures algebraiques bàsiques (cont.)

Definició 1.8.1. Sigui K un anell commutatiu, del qual denotem les operacions per $+, \cdot, 0, 1, -$. Un K-mòdul, o també, un mòdul sobre K, és un grup commutatiu E, del qual denotem les operacions per $+, 0, -$, juntament amb una acció de K en E,

$$K \times E \longrightarrow E, \qquad (\lambda, v) \mapsto \lambda \cdot v,$$

per a la qual se satisfan les propietats següents, que reflecteixen unes certes propietats de compatibilitat de l'acció amb les operacions de K i les de E.

(a) (L'acció respecta la suma de E, en el sentit que la distribueix.) Per a tot $\lambda \in K$ i tota parella d'elements $v, w \in E$, és $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$.

(b) (L'acció respecta el neutre de E.) Per a tot $\lambda \in K$, $\lambda \cdot 0 = 0$.

(c) (L'acció respecta l'oposat de E.) Per a tot $\lambda \in K$ i tot $v \in E$, $\lambda \cdot (-v) = -(\lambda \cdot v)$.

(d) (L'acció és compatible amb les sumes de K i de E en el sentit que distribueix, en E, la suma de K.) Per a tota parella d'elements $\lambda, \mu \in K$ i tot element $v \in E$ és $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$.

(e) (L'acció és compatible amb els neutres de les sumes de K i de E.) Per a tot element $v \in E$ és $0 \cdot v = 0$.

(f) (L'acció és compatible amb els oposats per a les sumes de K i de E.) Per a tot element $\lambda \in K$ i tot element $v \in E$ és $(-\lambda) \cdot v = -(\lambda \cdot v)$.

(g) (L'acció és compatible amb el producte de K, en el sentit que s'hi associa.) Per a tota parella d'elements $\lambda, \mu \in K$ i tot element $v \in E$ és $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$.

(h) (L'acció del neutre del producte de K és la identitat.) Per a tot element $v \in E$ és $1 \cdot v = v$.

Per a la definició de mòduls sobre anells no necessàriament commutatius, cf. **5.5.1**.

Definició 1.8.2. Si K és un cos, un K-mòdul s'anomena un K-espai vectorial, o bé un espai vectorial sobre K.

Observació 1.8.3. Sovint es dóna la definició de K-espai vectorial (o la de K-mòdul) sense demanar la compatibilitat de l'acció de l'anell amb totes les operacions que tenim a l'anell i totes les que tenim en el grup commutatiu, com és desitjable per a l'estructura que definim, i només es consideren algunes de les compatibilitats possibles. De fet, això no és restrictiu, perquè algunes d'aquestes compatibilitats ja es dedueixen de les altres i dels axiomes d'anell i de grup commutatiu. Veiem-ne l'enunciat, la demostració del qual es proposa com a exercici.

Proposició 1.8.4. *Sigui K un anell commutatiu qualsevol. Un K-mòdul és un grup commutatiu E amb una acció de K en E, $K \times E \longrightarrow E$, $(\lambda, v) \mapsto \lambda \cdot v$, per a la qual se satisfà que per a tots els elements $\lambda, \mu \in K$ i tots els $v, w \in E$ és*

$$\lambda \cdot (v+w) = \lambda \cdot v + \lambda \cdot w, \quad (\lambda+\mu) \cdot v = \lambda \cdot v + \mu \cdot v, \quad (\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v), \quad 1 \cdot v = v. \ \square$$

Exemples 1.8.5. Sigui K un anell commutatiu qualsevol.

• Per a tot $n \geq 1$, considerem el conjunt producte K^n i definim-hi la suma, el neutre de la suma, l'oposat per a la suma, i l'acció de K, component a component; és a dir,

$$\begin{aligned}(a_0, a_1, \ldots, a_{n-1}) + (b_0, b_1, \ldots, b_{n-1}) &:= (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1}),\\ 0 &:= (0, 0, \ldots, 0),\\ -(a_0, a_1, \ldots, a_{n-1}) &:= (-a_0, -a_1, \ldots, -a_{n-1}),\\ \lambda \cdot (a_0, a_1, \ldots, a_{n-1}) &:= (\lambda \cdot a_0, \lambda \cdot a_1, \ldots, \lambda \cdot a_{n-1}).\end{aligned}$$

Amb aquestes operacions i acció, K^n és un K-mòdul. En particular, $\{0\}$ és un K-mòdul.

• Per a tot $m, n \geq 1$, el conjunt de les matrius $\mathbf{M}(n, m, K)$, de n files i m columnes, amb les operacions de suma, neutre per a la suma, oposat per a la suma, i l'acció de K definides component a component és un K-mòdul.

Notem que, de fet, el K-mòdul de les matrius, $\mathbf{M}(n, m, K)$, només es diferencia del K-mòdul $K^{n \cdot m}$ en la manera en què s'escriuen els seus elements: en forma de matriu $n \times m$, o bé en forma de vector de $n \cdot m$ components.

• Per a qualsevol conjunt X, considerem el conjunt de les aplicacions de X en K, K^X, i definim operacions de la manera següent.

Per a $f, g : X \longrightarrow K$ i per a $\lambda \in K$, posem $f + g : X \longrightarrow K$, $0 : X \longrightarrow K$, $-f : X \longrightarrow K$ i $\lambda \cdot f : X \longrightarrow K$ les aplicacions donades per

$$(f+g)(x) := f(x)+g(x), \qquad 0(x) := 0, \qquad (-f)(x) := -(f(x)), \qquad (\lambda \cdot f)(x) := \lambda \cdot f(x),$$

per a tot $x \in X$. Amb aquestes operacions i acció, K^X és un K-mòdul; el K-mòdul de les aplicacions de X en K.

• Com a cas particular, podem considerar $K^{\mathbb{N}}$, el K-mòdul de les successions d'elements de K.

• Amb l'acció de $\mathbb{Z}$ en G definida en l'exemple **1.7.2**, tot grup commutatiu G és un $\mathbb{Z}$-mòdul.

• Per a qualsevol anell commutatiu K, l'anell de polinomis, definit en **1.6.6**, admet una estructura de K-mòdul si ens limitem a considerar la seva estructura de grup commutatiu amb la suma i ens mirem la multiplicació només d'elements de K per polinomis com a acció de K en $K[X]$.

• Per a qualsevol anell commutatiu K i qualsevol nombre natural n, considerem el conjunt dels polinomis de grau menor o igual que n, $K[X]_{\leq n}$, com el dels polinomis de la forma

$$p(X) = \sum_{k=0}^{n} a_k X^k, \qquad a_0, \ldots, a_n \in K.$$

Llavors, $K[X]_{\leq n}$ és un K-mòdul.

1.9 Concepte general de morfisme

Així com per a relacionar uns conjunts amb altres ho fem amb les aplicacions, també ens interessa poder relacionar entre si i de manera satisfactòria, posem per exemple, els

grups, o bé els anells, o bé els K-mòduls. Això ho podem fer simplement com a conjunts, però llavors l'estructura algebraica no juga cap paper en aquesta relació. Ens interessen aquelles aplicacions que siguin compatibles amb l'estructura que considerem; és a dir, que es comportin bé respecte de totes les operacions (i les accions) que tinguem a l'estructura corresponent. Aquest és el concepte de morfisme (també se'n diu homomorfisme) algebraic. Anem a definir-lo amb més precisió.

Definició 1.9.1. Siguin A, B conjunts, $n \geq 0$ un nombre natural, i $*_A : A^n \longrightarrow A$, $*_B : B^n \longrightarrow B$ operacions n-àries en A i B, respectivament. Un morfisme de $(A, *_A)$ en $(B, *_B)$ és una aplicació $\varphi : A \longrightarrow B$ tal que el diagrama següent és commutatiu:

$$\begin{array}{ccc} A^n & \xrightarrow{\varphi\times\cdots\times\varphi} & B^n \\ {\scriptstyle *_A}\downarrow & & \downarrow{\scriptstyle *_B} \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

Diagrama 1.13: Definició de morfisme per a operacions n-àries

Això és dir que per a tots els elements $a_0, \ldots, a_{n-1} \in A$ se satisfà que

$$\varphi\big(*_A(a_0, a_1, \ldots, a_{n-1})\big) = *_B\big(\varphi(a_0), \varphi(a_1), \ldots, \varphi(a_{n-1})\big).$$

Definició 1.9.2. Siguin K, A, B conjunts, i $\circ_A : K \times A \longrightarrow A$, $\circ_B : K \times B \longrightarrow B$ accions de K en A i en B, respectivament. Un morfisme de A en B per a les accions de K, també anomenat K-morfisme, és una aplicació $\varphi : A \longrightarrow B$ tal que el diagrama següent és commutatiu:

$$\begin{array}{ccc} K \times A & \xrightarrow{\mathrm{id}_K\times\varphi} & K \times B \\ {\scriptstyle \circ_A}\downarrow & & \downarrow{\scriptstyle \circ_B} \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

Diagrama 1.14: Definició de K-morfisme

Això és dir que per a tots els elements $\lambda \in K$, $a \in A$ se satisfà que

$$\varphi(\lambda \circ_A a) = \lambda \circ_B \varphi(a).$$

Exemples 1.9.3. • Per a l'operació 0-ària que proporciona l'element neutre d'un grup, es demana que la imatge per φ de l'element neutre de A, e_A, sigui l'element neutre de B, e_B; és a dir, que $\varphi(e_A) = e_B$.

• Anàlogament, per a l'operació 1-ària que proporciona els inversos en un grup, es demana que la imatge de l'invers de $a \in A$ sigui l'invers (en B) de la imatge $\varphi(a) \in B$; és a dir, que $\varphi(a^{-1}) = \varphi(a)^{-1}$.

• Per a l'operació binària que proporciona el producte en un grup, es demana que la imatge per φ dels productes $a *_A a'$, $a, a' \in A$, sigui el producte (en B) de les imatges $\varphi(a), \varphi(a') \in B$; és a dir, que $\varphi(a *_A a') = \varphi(a) *_B \varphi(a')$.

• Per exemple, podem considerar l'aplicació $\exp : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ donada per $x \mapsto e^x$. Llavors, exp és un morfisme de $\mathbb{R}$ amb la suma en $\mathbb{R}_{>0}$ (conjunt dels nombres reals positius) amb

el producte, perquè $\exp(x+y) = \exp(x) \cdot \exp(y)$, per a $x, y \in \mathbb{R}$. També és un morfisme de $(\mathbb{R}, 0)$ en $(\mathbb{R}_{>0}, 1)$, i de $(\mathbb{R}, -)$ en $(\mathbb{R}_{>0}, (\ )^{-1})$, perquè $\exp(0) = 1$, i $e^{-x} = \dfrac{1}{e^x}$, per a tot $x \in \mathbb{R}$.

D'altra banda, si considerem les accions

$$* : \mathbb{Z} \times \mathbb{R} \longrightarrow \mathbb{R}, \qquad \circ : \mathbb{Z} \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0},$$

donades, respectivament, per

$$(\lambda, x) \mapsto \lambda * x := x \cdot \lambda, \qquad (\lambda, y) \mapsto \lambda \circ y := y^{\lambda},$$

per a $\lambda \in \mathbb{Z}$, $x \in \mathbb{R}$, $y \in \mathbb{R}_{>0}$, llavors exp és un morfisme per a les accions, ja que

$$\exp(\lambda * x) = \exp(x \cdot \lambda) = e^{x \cdot \lambda} = (e^x)^{\lambda} = \exp(x)^{\lambda} = \lambda \circ \exp(x).$$

Una propietat bàsica per als morfismes per a operacions i per a accions és reflectida en el resultat següent, una demostració del qual es proposa com a exercici, i que ens diu que l'aplicació identitat és un morfisme per a totes les operacions n-àries i per a totes les accions, i que la composició de morfismes per a operacions n-àries o per a accions també és un morfisme per a operacions n-àries o per a accions.

Proposició 1.9.4. *Considerem conjunts A, B, C, K, un nombre natural $n \in \mathbb{N}$, operacions n-àries $*_A : A^n \longrightarrow A$, $*_B : B^n \longrightarrow B$, $*_C : C^n \longrightarrow C$, en A, B, C, respectivament, accions $\circ_A : K \times A \longrightarrow A$, $\circ_B : K \times B \longrightarrow B$, $\circ_C : K \times C \longrightarrow C$, de K en A, B, C, respectivament, i aplicacions $\varphi : A \longrightarrow B$, $\psi : B \longrightarrow C$.*

(a) *L'aplicació identitat $\mathrm{id}_A : A \longrightarrow A$ és un morfisme per a l'operació $*_A$.*

(b) *L'aplicació identitat $\mathrm{id}_A : A \longrightarrow A$ és un morfisme per a l'acció $\circ_A$.*

(c) *Si φ és un morfisme de $(A, *_A)$ en $(B, *_B)$ i ψ és un morfisme de $(B, *_B)$ en $(C, *_C)$, llavors l'aplicació composició $\psi \circ \varphi : A \longrightarrow C$ és un morfisme de $(A, *_A)$ en $(C, *_C)$.*

(d) *Si φ és un morfisme per a les accions $\circ_A$ i $\circ_B$, i ψ és un morfisme per a les accions $\circ_B$ i $\circ_C$, llavors l'aplicació composició $\psi \circ \varphi : A \longrightarrow C$ és un morfisme per a les accions $\circ_A$ i $\circ_C$.* □

1.10 Isomorfismes

El concepte d'isomorfisme és clau en el desenvolupament de la teoria d'estructures algebraiques. De fet, dues estructures isomorfes són indistingibles des del sol punt de vista de l'estructura, i allò que val per a l'una, val per a l'altra.

Definició 1.10.1. Siguin A, B conjunts, $n \in \mathbb{N}$ un nombre natural, i $*_A : A^n \longrightarrow A$, $*_B : B^n \longrightarrow B$ operacions n-àries en A i B, respectivament. Un morfisme de $(A, *_A)$ en $(B, *_B)$, $\varphi : A \longrightarrow B$, s'anomena un isomorfisme si existeix un morfisme de $(B, *_B)$ en $(A, *_A)$, $\psi : B \longrightarrow A$, tal que $\psi \circ \varphi = \mathrm{id}_A$ i $\varphi \circ \psi = \mathrm{id}_B$.

Un morfisme $\varphi : A \longrightarrow A$ de $(A, *_A)$ en $(A, *_A)$ s'anomena un endomorfisme; un isomorfisme $\varphi : A \longrightarrow A$ de $(A, *_A)$ en $(A, *_A)$ s'anomena un automorfisme.

Definició 1.10.2. Siguin K, A, B conjunts i $\circ_A : K \times A \longrightarrow A$, $\circ_B : K \times B \longrightarrow B$ accions de K en A i en B, respectivament. Un K-morfisme $\varphi : A \longrightarrow B$, de $(A, \circ_A)$ en $(B, \circ_B)$, s'anomena un K-isomorfisme si existeix un K-morfisme $\psi : B \longrightarrow A$, de $(B, \circ_B)$ en $(A, \circ_A)$, tal que $\psi \circ \varphi = \mathrm{id}_A$ i $\varphi \circ \psi = \mathrm{id}_B$.

Un K-morfisme $\varphi : A \longrightarrow A$ de $(A, \circ_A)$ en $(A, \circ_A)$ s'anomena un K-endomorfisme; un K-isomorfisme $\varphi : A \longrightarrow A$ de $(A, \circ_A)$ en $(A, \circ_A)$ s'anomena un K-automorfisme.

S'escriu $\mathrm{End}(A, *_A)$ per a designar el conjunt dels endomorfismes de $(A, *_A)$. S'escriu $\mathrm{End}(A, \circ_A)$, o també $\mathrm{End}_K(A)$, quan l'acció $\circ_A$ es pot sobreentendre, per a designar el conjunt dels K-endomorfismes de $(A, \circ_A)$.

S'escriu $\mathrm{Aut}(A, *_A)$ per a designar el conjunt dels automorfismes de $(A, *_A)$. S'escriu $\mathrm{Aut}(A, \circ_A)$, o també $\mathrm{Aut}_K(A)$, quan l'acció $\circ_A$ es pot sobreentendre, per a designar el conjunt dels K-automorfismes de $(A, \circ_A)$.

Observació 1.10.3. En particular, si $\varphi : A \longrightarrow B$ és un isomorfisme per a operacions n-àries $*_A$, $*_B$, o un K-isomorfisme per a accions $\circ_A$, $\circ_B$, llavors φ és una aplicació bijectiva.

Recíprocament, es proposa com a exercici la demostració de les propietats següents. De fet, la prova es redueix a veure que l'única aplicació inversa és un morfisme.

Exercici 1.10.4. Siguin K, A, B conjunts, $n \in \mathbb{N}$ un nombre natural, $*_A : A^n \longrightarrow A$, $*_B : B^n \longrightarrow B$, operacions n-àries en A i B, respectivament, i $\circ_A : K \times A \longrightarrow A$, $\circ_B : K \times B \longrightarrow B$, accions de K en A i en B, respectivament. Suposem que una aplicació bijectiva $\varphi : A \longrightarrow B$ és un morfisme de $(A, *_A)$ en $(B, *_B)$, o bé un K-morfisme de $(A, \circ_A)$ en $(B, \circ_B)$. Llavors, φ és un isomorfisme.

Observació 1.10.5. En algun altre context en què també es parla de morfismes i en què els morfismes també són aplicacions entre conjunts, però en què els morfismes no ho són de conjunts amb operacions o amb accions, es pot donar el cas de morfismes que són aplicacions bijectives però que no són isomorfismes. Un cas típic es dóna en el context d'espais topològics.

Exercici 1.10.6. (a) Siguin A un conjunt, $n \in \mathbb{N}$ un nombre natural, i $* : A^n \longrightarrow A$ una operació n-ària en A. El conjunt $\mathrm{Aut}(A, *_A)$, amb la composició d'aplicacions com a operació binària, l'aplicació identitat com a operació 0-ària, i l'aplicació que a cada bijecció li assigna la seva inversa com a operació 1-ària, és un grup.

(b) Siguin K, A conjunts i $\circ : K \times A \longrightarrow A$ una acció de K en A. El conjunt $\mathrm{Aut}_K(A)$, amb la composició d'aplicacions com a operació binària, l'aplicació identitat com a operació 0-ària, i l'aplicació que a cada bijecció li assigna la seva inversa com a operació 1-ària, és un grup.

Exercici 1.10.7. Siguin I, J, A, conjunts, $\{K_j\}_{j \in J}$ una família de conjunts, $\{n_i\}_{i \in I}$ una família de nombres naturals, $n_i \in \mathbb{N}$, $\{*_i : A^{n_i} \longrightarrow A\}_{i \in I}$, una família d'operacions n_i-àries, $i \in I$, en A, i, per a cada $j \in J$, considerem accions $\circ_j : K_j \times A \longrightarrow A$, de K_j en A. Llavors, el conjunt $\mathrm{Aut}(A, \{*_i\}_{i \in I}, \{\circ_j\}_{j \in J})$ format per les aplicacions $\varphi : A \longrightarrow A$ que són alhora automorfismes per a totes les operacions $*_i$, $i \in I$, i totes les accions $\circ_j$, $j \in J$, amb la composició d'aplicacions com a operació binària, l'aplicació identitat com a operació 0-ària, i l'aplicació que a cada bijecció li assigna la seva inversa com a operació 1-ària, és un grup.

Capítol 2

Grups

Per a desenvolupar la teoria de grups utilitzarem majoritàriament la notació multiplicativa; és a dir, denotarem l'operació binària del grup per un punt volat, $\cdot$, o per juxtaposició, i l'anomenarem el producte, l'element neutre del grup per 1, i l'anomenarem u, i l'operació 1-ària del grup per $x \mapsto x^{-1}$, i direm que x^{-1} és l'element invers de l'element x. Així, si diem "sigui G un grup", sense especificar res més, donarem per entès que G és un conjunt no buit amb una operació binària associativa $(x, y) \mapsto x \cdot y$, o bé $(x, y) \mapsto xy$, un element neutre $1 \in G$, i una operació 1-ària $x \mapsto x^{-1}$, invers per al producte i el neutre.

En algun altre cas, sovint en el cas que els grups siguin commutatius, utilitzarem la notació additiva; això és dir que denotarem l'operació binària per $(x, y) \mapsto x + y$, i l'anomenarem suma, l'element neutre per 0, i l'anomenarem zero, i l'operació invers per $x \mapsto -x$, l'anomenarem oposat, i llegirem "meys x" per $-x$.

2.1 Propietats elementals de càlcul en un grup

Acabem de recordar que, en un grup G, l'operació producte és associativa, hi ha element neutre, i tot element té un invers; i que si l'operació producte també és commutativa, el grup s'anomena commutatiu o abelià (cf. **1.6.1**).

Proposició 2.1.1. *Sigui G un conjunt amb una operació binària $* : G \times G \longrightarrow G$. Si existeixen un element neutre per l'esquerra per a $*$, $1 \in G$, i un element neutre per la dreta per a $*$, $1' \in G$, llavors $1' = 1$ i 1 és un element neutre per a $*$. Per tant, una operació binària pot admetre com a màxim un sol element neutre.*

Demostració: Tenim que $1' = 1 \cdot 1' = 1$; la primera igualtat perquè 1 és neutre per l'esquerra, i la segona perquè $1'$ ho és per la dreta. Per tant, $1 = 1'$ és element neutre per a $*$. I si hi hagués dos elements neutres, un ho seria per l'esquerra i l'altre ho seria per la dreta, de manera que coincidirien. □

Proposició 2.1.2. *Sigui G un conjunt amb una operació binària $* : G \times G \longrightarrow G$ i una operació 0-ària $1 \in G$. Suposem que $*$ és associativa i que 1 és un element neutre per a $*$. Si un element $g \in G$ admet un invers per l'esquerra (per a $*$ i 1), $g' \in G$, i un un invers per la dreta (per a $*$ i 1), $g'' \in G$, llavors $g'' = g'$ i g' és un element invers de g per a $*$ i 1. Con a conseqüència, una operació binària associativa, $*$, i amb neutre, $1 \in G$, pot admetre, com a màxim, una sola operació invers per a $*$ i 1.*

Demostració: Se satisfà que $g' = g' \cdot 1 = g' \cdot (g \cdot g'') = (g' \cdot g) \cdot g'' = 1 \cdot g'' = g''$; la justificació de les igualtats és la següent: la primera i la cinquena, perquè 1 és neutre; la segona, perquè g'' és invers de g per la dreta; la tercera, perquè el producte és associatiu; i la quarta, perquè g' és invers de g per l'esquerra.

Així, si una operació associativa, $*$, i amb neutre, 1, admet dues operacions invers per a $*$ i 1, podem considerar-ne una com a invers per l'esquerra i l'altra com a invers per la dreta; acabem de veure que, aleshores, coincideixen. □

Proposició 2.1.3. *Sigui G un grup. Se satisfan les propietats següents.*

(a) L'invers de l'element neutre és l'element neutre: $1^{-1} = 1$.

(b) (L'invers és involutiu.) *Per a tot element $g \in G$ és $(g^{-1})^{-1} = g$.*

(c) (L'invers fa contravariar el producte.) *Per a tots els elements $g, h \in G$ és*

$$(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}.$$

(d) (Lleis de simplificació) *Per a tots els elements $g, h, k \in G$ se satisfà que*

$$k \cdot g = k \cdot h \quad \Longrightarrow \quad g = h, \qquad \textit{i que} \qquad g \cdot k = h \cdot k \quad \Longrightarrow \quad g = h.$$

Demostració:

(a) Immediat, de la igualtat $1 \cdot 1 = 1$ i la definició d'invers.

(b) La propietat que defineix g^{-1} com a invers de g també defineix g com a invers de g^{-1}.

(c) Per a l'element $h^{-1} \cdot g^{-1} \in G$ se satisfan les igualtats

$$(h^{-1} \cdot g^{-1}) \cdot (g \cdot h) = h^{-1} \cdot (g^{-1} \cdot (g \cdot h)) = h^{-1} \cdot ((g^{-1} \cdot g) \cdot h) = h^{-1} \cdot (1 \cdot h) = h^{-1} \cdot h = 1,$$

i

$$(g \cdot h) \cdot (h^{-1} \cdot g^{-1}) = g \cdot (h \cdot (h^{-1} \cdot g^{-1})) = g \cdot ((h \cdot h^{-1}) \cdot g^{-1}) = g \cdot (1 \cdot g^{-1}) = g \cdot g^{-1} = 1,$$

que defineixen $h^{-1} \cdot g^{-1}$ com a invers de $g \cdot h$.

(d) Si suposem que $k \cdot g = k \cdot h$, llavors

$$g = 1 \cdot g = (k^{-1} \cdot k) \cdot g = k^{-1} \cdot (k \cdot g) = k^{-1} \cdot (k \cdot h) = (k^{-1} \cdot k) \cdot h = 1 \cdot h = h,$$

i obtenim la primera propietat. Anàlogament, si suposem que $g \cdot k = h \cdot k$, llavors

$$g = g \cdot 1 = g \cdot (k \cdot k^{-1}) = (g \cdot k) \cdot k^{-1} = (h \cdot k) \cdot k^{-1} = h \cdot (k \cdot k^{-1}) = h \cdot 1 = h,$$

i obtenim la segona. □

Observació 2.1.4. A partir d'ara, utilitzarem aquestes propietats sense fer-hi cap més referència ni donar-ne cap més explicació. I, per causa de l'associativitat, sovint tampoc no escriurem els parèntesis (cf. la secció **1.5**).

2.2 Morfismes de grups

A la secció **1.9**, s'ha definit què és un morfisme per a conjunts amb una operació n-ària o per a conjunts amb una acció. Ara convé precisar què és un morfisme de grups i algunes propietats bàsiques dels morfismes de grups.

Definició 2.2.1. Siguin G, H, grups. Un morfisme de grups de G en H és una aplicació $\varphi : G \longrightarrow H$ que és morfisme per a cadascuna de les operacions de grup; és a dir, per als productes, els neutres, i els inversos. O sigui, cal que se satisfacin les propietats

(a) $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$, per a tot $g, g' \in G$;

(b) $\varphi(1) = 1$; i

(c) $\varphi(g^{-1}) = \varphi(g)^{-1}$, per a tot $g \in G$.

Les propietats especials que es demanen a les operacions de grup fan que no calgui comprovar totes les propietats per a assegurar-se que una certa aplicació entre grups és un morfisme de grups. En efecte, se satisfà el resultat següent.

Proposició 2.2.2. *Siguin G, H grups. Una aplicació $\varphi : G \longrightarrow H$ és un morfisme de grups si, i només si, és un morfisme per a les operacions binàries; és a dir, si per a tot $g, g' \in G$ és $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$.*

Demostració: Suposem que se satisfà aquesta propietat. Cal veure que $\varphi(1) = 1$ i que $\varphi(g^{-1}) = \varphi(g)^{-1}$, per a tot $g \in G$. Per a això, comencem per notar la igualtat

$$\varphi(1) \cdot \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) = 1 \cdot \varphi(1);$$

com que H és un grup, podem simplificar $\varphi(1)$ (o sigui, multiplicar a la dreta pel seu invers), i obtenim que $\varphi(1) = 1$. De manera similar, donat un element qualsevol $g \in G$, tenim que

$$\varphi(g)\cdot\varphi(g^{-1}) = \varphi(g\cdot g^{-1}) = \varphi(1) = 1, \qquad \text{i que} \qquad \varphi(g^{-1})\cdot\varphi(g) = \varphi(g^{-1}\cdot g) = \varphi(1) = 1,$$

igualtats que ens diuen que $\varphi(g^{-1})$ és l'invers, en H, de $\varphi(g)$. □

Exemples 2.2.3. • Sigui G un grup. L'aplicació identitat, $\mathrm{id} : G \longrightarrow G$, donada per $g \mapsto g$, és un morfisme de grups.

• La composició de morfismes de grups és un morfisme de grups. És a dir, si G, H, K, són grups i $\varphi : G \longrightarrow H$ i $\psi : H \longrightarrow K$ són morfismes de grups, llavors l'aplicació composició, $\psi \circ \varphi : G \longrightarrow K$, donada per $(\psi \circ \varphi)(g) = \psi(\varphi(g))$, per a tot $g \in G$, és un morfisme de grups.

• Siguin G, H grups. L'aplicació $G \longrightarrow H$ constant de valor el neutre de H, donada per $g \mapsto 1$, per a tot $g \in G$, és un morfisme de grups. S'anomena el morfisme trivial de G en H.

• Siguin G un grup i $g \in G$ un element qualsevol. L'aplicació $\varphi_g : G \longrightarrow G$ definida per $h \mapsto g \cdot h \cdot g^{-1}$ és un morfisme de grups. De fet, és un automorfisme, amb invers $\varphi_{g^{-1}}$. S'anomena l'automorfisme intern de G determinat per g o, sovint, la conjugació per g.

• El conjunt dels automorfismes d'un grup G, amb la composició d'aplicacions, la identitat, i l'aplicació que a cada automorfisme li associa el seu invers, és un grup (cf. **1.10.7**), que denotem per $\mathrm{Aut}(G)$. Llavors, l'aplicació $\varphi : G \longrightarrow \mathrm{Aut}(G)$ donada per $g \mapsto \varphi_g$, és un morfisme de grups.

2.3 Subgrups

Siguin G un conjunt i $H \subseteq G$ un subconjunt. Pot ser que algunes operacions definides en G es puguin restringir a H i proporcionar operacions en H i, en canvi, altres no.

Per exemple, si considerem el conjunt dels nombres enters, $\mathbb{Z}$, amb les operacions suma i zero, $+$ i 0, i considerem el subconjunt dels nombres naturals, $\mathbb{N}$, les dues operacions hi restringeixen. En canvi, l'oposat per a la suma en $\mathbb{Z}$, $-$, no es pot restringir a $\mathbb{N}$.

Ens interessarà tractar el cas en què les operacions es poden restringir a alguns subconjunts o, amb més precisió, els subconjunts als quals es poden restringir totes les operacions.

Definició 2.3.1. Siguin G un conjunt, $H \subseteq G$ un subconjunt, $n \in \mathbb{N}$ un nombre natural, i $*_G : G^n \longrightarrow G$ una operació n-ària en G. Es diu que $*_G$ restringeix a H si, per a tots els elements $h_0, \ldots, h_{n-1} \in H$ se satisfà que $*_G(h_0, \ldots, h_{n-1}) \in H$. Així, l'assignació $*_H(h_0, \ldots, h_{n-1}) := *_G(h_0, \ldots, h_{n-1})$, $h_0, \ldots, h_{n-1} \in H$, defineix una operació n-ària $*_H$ en H. S'anomena la restricció de $*_G$ a H.

Definició 2.3.2. Siguin K, G conjunts, $H \subseteq G$ un subconjunt i $\circ_G : K \times G \longrightarrow G$ una acció de K en G. Es diu que l'acció restringeix a H si, per a tot element $\lambda \in K$ i tot element $h \in H$ se satisfà que $\circ_G(\lambda, h) \in H$. D'aquesta manera, l'assignació $\circ_H(\lambda, h) := \circ_G(\lambda, h)$, $\lambda \in K$, $h \in H$, defineix una acció $\circ_H$ de K en H. S'anomena la restricció de $\circ_G$ a H.

Observació 2.3.3. Notem que, per a $n \geq 1$, tota operació n-ària, $*_G$, restringeix al conjunt buit. En canvi, una operació 0-ària, $*_G$, només restringeix als subconjunts $H \subseteq G$ que continguin l'element distingit per $*_G$; en particular, no restringeix al subconjunt buit.

Definició 2.3.4. Siguin G, un grup i $H \subseteq G$ un subconjunt qualsevol. Si les tres operacions de G restringeixen a H, llavors H, amb aquestes operacions restricció, és un grup (la comprovació és un exercici immediat). Es diu que és un subgrup de G.

Així, doncs, un subgrup d'un grup G és donat per un subconjunt $H \subseteq G$ per al qual se satisfà que

(a) per a tot $h, h' \in H$, és $h *_G h' \in H$;

(b) $1 \in H$; i

(c) per a tot $h \in H$ és $h^{-1} \in H$.

Observacions 2.3.5. • Notem que perquè un subconjunt $H \subseteq G$ sigui un subgrup d'un grup G, cal que totes tres operacions restringeixin al subconjunt. És a dir, per a elements $h, h' \in H$, el seu producte en H ha de ser el mateix element de H que el seu producte en G, l'element neutre de H ha de ser el mateix que l'element neutre de G, i per a $h \in H$, l'invers de h en H ha de ser el mateix que l'invers de h en G.

• Així, per exemple, el subconjunt dels nombres racionals positius amb la multiplicació, 1, i l'invers multiplicatiu, és un grup. Però no és un subgrup del grup additiu de tots els nombres racionals amb la suma, 0, i l'oposat, perquè les operacions de $(\mathbb{Q}_{>0}, 1, (\ )^{-1})$ no són restricció de les de $(\mathbb{Q}, +, 0, -)$.

• Notem, també, que si G és un grup abelià i $H \subseteq G$ és un subgrup, llavors H també és abelià. Però pot ser que H sigui abelià i, en canvi, G no ho sigui. Més endavant tindrem múltiples ocasions de veure exemples d'aquest fet.

Proposició 2.3.6. *Siguin G un grup i $H \subseteq G$ un subconjunt no buit. Llavors, H és un subgrup de G si, i només si, per a tot $h', h \in H$ se satisfà que $h' \cdot h^{-1} \in H$.*

Demostració: La condició és necessària, perquè si $h', h \in H$, llavors $h', h^{-1} \in H$ (l'invers pertany a H, perquè H és subgrup) i, per tant, $h' \cdot h^{-1} \in H$ (el producte pertany a H, perquè H és subgrup). Veiem-ne la suficiència. Com que H és no buit, existeix algun element $h \in H$; llavors, $1 = h \cdot h^{-1} \in H$; i per a $h \in H$, com que $1 \in H$, és $h^{-1} = 1 \cdot h^{-1} \in H$; i, finalment, per a $h', h \in H$, és $h', h^{-1} \in H$, de manera que $h' \cdot h = h' \cdot (h^{-1})^{-1} \in H$. És a dir, les operacions neutre, invers i producte restringeixen a H i, per tant, H és un subgrup de G. □

Observació 2.3.7. Notem que la condició que H sigui no buit és essencial. En efecte, per a $H = \varnothing$ se satisfà la propietat que si $h', h \in H$ llavors $h' \cdot h^{-1} \in H$; però H no conté 1, perquè és el conjunt buit. Per tant, $\varnothing$ no és un subgrup de G.

Definició 2.3.8. Per a tot grup G, els subconjunts $\{1\}$ i G de G són subgrups. El subgrup $\{1\}$ s'anomena els subgrup trivial de G; el subgrup G s'anomena el subgrup total de G.

Definició 2.3.9. Siguin G, G' grups i $\varphi : G \longrightarrow G'$ un morfisme de grups. És immediat comprovar que se satisfan les propietats següents.

(a) Si $H' \subseteq G'$ és un subgrup de G', llavors, la seva antiimatge, $\varphi^{-1}(H') \subseteq G$, és un subgrup de G. En particular,

$$\ker \varphi := \varphi^{-1}(\{1\}) = \{g \in G : \ \varphi(g) = 1\}$$

és un subgrup de G. S'anomena el nucli de φ.

(b) Si $H \subseteq G$ és un subgrup de G, llavors la seva imatge per φ, $\varphi(H) \subseteq G'$, és un subgrup de G'. En particular,

$$\operatorname{im} \varphi := \varphi(G) = \{g' \in G' : \ \text{existeix } g \in G \text{ tal que } g' = \varphi(g)\}$$

és un subgrup de G'. S'anomena el subgrup imatge de φ.

Proposició 2.3.10. *Siguin G, H grups i $\varphi : G \longrightarrow H$ un morfisme de grups. Llavors, φ, com a aplicació, és injectiva si, i només si,* $\ker \varphi = \{1\}$*, el subgrup trivial.*

Demostració: Suposem que φ és una aplicació injectiva; com que $\varphi(1) = 1$, per a tot element $g \in G$, $g \neq 1$, ha de ser $\varphi(g) \neq 1$; és a dir, $\ker \varphi = \{1\}$, com calia veure. Recíprocament, suposem que $\ker \varphi = \{1\}$. Donats elements $g, g' \in G$, si se satisfà que $\varphi(g') = \varphi(g)$, llavors $\varphi(g^{-1}g') = 1$, perquè φ és morfisme de grups. Ara bé, com que $\ker \varphi = \{1\}$, això implica que $g^{-1}g' = 1$; o sigui, que $g' = g$. Per tant, l'aplicació φ és injectiva. □

Observació 2.3.11. I clarament, un morfisme de grups $\varphi : G \longrightarrow H$ és, com a aplicació, exhaustiva, si, i només si, $\operatorname{im} \varphi = H$.

Definició 2.3.12. Si G és un grup i $\{H_i\}_{i \in I}$ és una família no buida de subgrups de G (recordem que no buida vol dir que $I \neq \varnothing$), llavors, $\bigcap_{i \in I} H_i$ és un subgrup de G (la comprovació és immediata). S'anomena el subgrup intersecció de la família $\{H_i\}_{i \in I}$.

Definició 2.3.13. Siguin G un grup i $S \subseteq G$ un subconjunt qualsevol (que pot ser un subgrup o no ser-ho). Com que G és un subgrup de G que conté S, el conjunt $\mathcal{C}_S$ format per tots els subgrups de G que contenen S és no buit; és a dir, la família $\{H\}_{H\in\mathcal{C}_S}$ és no buida. Llavors, el conjunt

$$\langle S\rangle := \bigcap_{H\in\mathcal{C}_S} H = \bigcap_{H\supseteq S,\ \text{subgrup}} H$$

és un subgrup de G. S'anomena el subgrup generat per S. És, doncs, el més petit dels subgrups de G que contenen el subconjunt S.

2.3.14. En particular, tenim que $\langle\varnothing\rangle = \langle\{1\}\rangle = \{1\}$, el subgrup trivial; i que si $H \subseteq G$ és un subgrup de G, llavors $\langle H\rangle = H$.

Proposició 2.3.15. *Siguin G un grup i $S \subseteq G$ un subconjunt qualsevol. Llavors, el subgrup de G generat per S és el subconjunt de G format per l'element neutre i els elements de G que són productes (finits) d'elements de S i d'inversos d'elements de S. És a dir, $\langle S\rangle = C$, on*

$$C := \{1\} \cup \{g \in G :\ \textit{existeixen } n \in \mathbb{N}, n \geq 1, s_1, \ldots, s_n \in S \cup S^{-1},\ \textit{i } g = s_1 \cdots s_n\},$$

i S^{-1} denota el subconjunt de G format pels inversos dels elements de S.

Demostració: És clar que un subgrup de G que contingui S, en particular, $\langle S\rangle$, ha de contenir tots els elements de la forma $s_1 \cdots s_n$ tals que $s_i \in S$ o $s_i^{-1} \in S$; és a dir, $\langle S\rangle \supseteq C$. D'altra banda, aquest conjunt C és un subgrup de G: clarament, el producte d'elements de C és de C, l'element neutre pertany a C, i l'invers de $s_1 \cdots s_n \in C$, per a $s_i \in S \cup S^{-1}$, $1 \leq i \leq n$, és $s_n^{-1} \cdots s_1^{-1} \in C$. Així, com que $S \subseteq C$, tenim que C és un subgrup de G que conté S; per tant, $C \supseteq \langle S\rangle$, i obtenim la igualtat que volíem. □

Exemples 2.3.16. • Considerem el grup $(\mathbb{Q}_{>0}, \cdot, 1, (\ )^{-1})$, dels nombres racionals positius amb la multiplicació usual, 1, i $x \mapsto \dfrac{1}{x}$. El teorema fonamental de l'Aritmètica implica, entre altres coses, que el conjunt $\mathbb{P}$ format pels nombres naturals primers és un conjunt de generadors del grup; és a dir, que $\langle\mathbb{P}\rangle = \mathbb{Q}_{>0}$.

Exercici 2.3.17. Siguin G i H, grups, $\varphi : G \longrightarrow H$, un morfisme de grups, i $S \subseteq G$ un subconjunt qualsevol de G. La imatge de S per φ, $\varphi(S)$, és un conjunt de generadors de $\varphi(\langle S\rangle)$; és a dir, la imatge d'un conjunt de generadors d'un subgrup per un morfisme de grups és un conjunt de generadors del subgrup imatge.

2.4 Quocients. Teorema d'isomorfia

En aquesta secció, donarem la definició de conjunts quocient i demostrarem una versió general del teorema d'isomorfia; en una secció posterior, aplicarem aquests resultats al cas de grups.

Notem que donar una aplicació entre conjunts no buits, $\varphi : G \longrightarrow H$, es pot interpretar com l'assignació d'etiquetes als elements de G: la imatge d'un element $g \in G$ és l'etiqueta que assignem a g. Tots els elements de G tenen una etiqueta assignada, però

no necessàriament totes les etiquetes (elements de H) són assignades a algun element de G. Ara, podem pensar en les fibres de l'aplicació (és a dir, les antiimatges dels elements de H) com els conjunts dels elements de G als quals correspon la mateixa etiqueta en H. Això produeix una partició de G en subconjunts disjunts i, per tant, podem considerar la relació d'equivalència associada a aquesta partició (cada classe d'equivalència és formada per tots els elements de G que tenen associada la mateixa etiqueta en H). I podem considerar el conjunt de les classes d'equivalència; això és, el conjunt quocient de G per l'equivalència associada a φ. I també podem pensar en l'aplicació que a cada classe d'equivalència li fa correspondre l'etiqueta comuna a tots els seus elements. Anem a fer això d'una manera més formal.

Definició 2.4.1. Siguin G, H conjunts no buits qualssevol i $\varphi : G \longrightarrow H$ una aplicació. Definim una relació en G de la manera següent. Donats elements $g, g' \in G$, direm que g' és congru a g mòdul φ, i escriurem $g' \equiv g \pmod{\varphi}$, si, i només si, $\varphi(g') = \varphi(g)$. L'anomenarem la congruència mòdul φ.

2.4.2. La comprovació que la congruència mòdul φ, és a dir, $\equiv \pmod{\varphi}$, és una relació d'equivalència en G és immediata. Les classes d'equivalència són les fibres no buides de l'aplicació; és a dir, els subconjunts $\varphi^{-1}(h) := \{g \in G : \varphi(g) = h\}$, per a $h \in \operatorname{im}\varphi$. I podem considerar el conjunt quocient de G per aquesta relació d'equivalència; és a dir, el conjunt $G/\varphi := \{\varphi^{-1}(h) : h \in \operatorname{im}\varphi\}$, format per les classes d'equivalència per a aquesta relació. Notem que per a cada element $g \in G$, la classe d'equivalència que admet g com a representant, és a dir, la classe d'equivalència que conté g, és la classe $\varphi^{-1}\big(\varphi(g)\big)$.

Definició 2.4.3 (Descomposició canònica d'una aplicació)**.** Donada una aplicació qualsevol $\varphi : G \longrightarrow H$ entre conjunts no buits G, H, podem considerar la relació de congruència mòdul φ en G, el conjunt quocient G/φ i l'aplicació projecció $\pi : G \longrightarrow G/\varphi$, que assigna a cada element $g \in G$ la classe $\varphi^{-1}\big(\varphi(g)\big)$; notem que aquesta aplicació és exhaustiva. També podem considerar l'aplicació d'inclusió de $\operatorname{im}\varphi$ en H, $\psi : \operatorname{im}\varphi \longrightarrow H$; notem que aquesta aplicació és injectiva. I també podem considerar l'aplicació $\overline{\varphi} : G/\varphi \longrightarrow \operatorname{im}\varphi$ que assigna, a cada classe $\varphi^{-1}\big(\varphi(g)\big)$, l'element $\varphi(g)$; en efecte, $\varphi(g)$ és independent del representant g triat a la classe, perquè dir que $g \equiv g' \pmod{\varphi}$ és dir que $\varphi(g) = \varphi(g')$. Aquesta aplicació $\overline{\varphi}$ està, doncs, ben definida; a més a més, és bijectiva i se satisfà que el diagrama següent és commutatiu; s'anomena la descomposició canònica de l'aplicació φ.

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\psi} \\ G/\varphi & \xrightarrow[\ \overline{\varphi}\ ]{} & \operatorname{im}\varphi \end{array}$$

Diagrama 2.1: Descomposició canònica d'una aplicació

Definició 2.4.4 (Descomposició canònica d'un morfisme)**.** Suposem, ara, que G, H són conjunts, que $n \in \mathbb{N}$ és un nombre natural, que tenim operacions n-àries $*_G$ i $*_H$ en G, H, respectivament, i que $\varphi : G \longrightarrow H$ és un morfisme de $(G, *_G)$ en $(H, *_H)$.

Donats elements $g_0, \ldots, g_{n-1}, g'_0, \ldots, g'_{n-1} \in G$, suposem que $g'_i \equiv g_i \pmod{\varphi}$; és a dir, que $\varphi(g'_i) = \varphi(g_i)$, per a $0 \leq i \leq n-1$. Aleshores, afirmem que també és

$$*_G(g'_0, \ldots, g'_{n-1}) \equiv *_G(g_0, \ldots, g_{n-1}) \pmod{\varphi};$$

és a dir, que la relació d'equivalència $\equiv \pmod{\varphi}$ és compatible amb $*_G$. En efecte, com que φ és morfisme per a $*_G$ i $*_H$, i com que $\varphi(g'_i) = \varphi(g_i)$, per a $0 \leq i \leq n-1$, resulta que

$$\begin{aligned}\varphi\big(*_G(g'_0,\ldots,g'_{n-1})\big) &= *_H\big(\varphi(g'_0),\ldots,\varphi(g'_{n-1})\big)\\ &= *_H\big(\varphi(g_0),\ldots,\varphi(g_{n-1})\big) = \varphi\big(*_G(g_0,\ldots,g_{n-1})\big).\end{aligned}$$

Això permet definir una operació n-ària en el conjunt quocient G/φ de la manera següent: donades classes $\varphi^{-1}\big(\varphi(g_0)\big), \ldots, \varphi^{-1}\big(\varphi(g_{n-1})\big) \in G/\varphi$, de representants $g_0, \ldots, g_{n-1} \in G$, podem posar

$$*\Big(\varphi^{-1}\big(\varphi(g_0)\big),\ldots,\varphi^{-1}\big(\varphi(g_{n-1})\big)\Big) := \varphi^{-1}\Big(\varphi\big(*_G(g_0,\ldots,g_{n-1})\big)\Big),$$

perquè aquesta classe no depèn dels representants elegits. Així, $*$ és una operació n-ària en G/φ. A més a més, per la mateixa definició de $*$, l'aplicació $\pi : G \longrightarrow G/\varphi$ donada per $\pi(g) := \varphi^{-1}\big(\varphi(g)\big)$ és un morfisme exhaustiu per a les operacions $*_G$ i $*$.

D'altra banda, l'operació $*_H$ es pot restringir a una operació n-ària en $\operatorname{im}\varphi$. En efecte, donats $h_0, \ldots, h_{n-1} \in \operatorname{im}\varphi$, existeixen elements $g_0, \ldots, g_{n-1} \in G$ tals que $h_i = \varphi(g_i)$, per a $0 \leq i \leq n-1$; i, com que φ és morfisme per a $*_G$ i $*_H$, resulta que

$$*_H(h_0,\ldots,h_{n-1}) = *_H\big(\varphi(g_0),\ldots,\varphi(g_{n-1})\big) = \varphi\big(*_G(g_0,\ldots,g_{n-1})\big) \in \operatorname{im}\varphi.$$

Llavors, l'aplicació d'inclusió de $\operatorname{im}\varphi$ en H és un morfisme injectiu per a aquesta restricció, $*_{\operatorname{im}\varphi}$, i l'operació $*_H$.

Finalment, l'aplicació $\overline{\varphi} : G/\varphi \longrightarrow \operatorname{im}\varphi$, donada per $\varphi^{-1}\big(\varphi(g)\big) \mapsto \varphi(g)$, és un isomorfisme per a $*$ i $*_{\operatorname{im}\varphi}$. És a dir, el diagrama commutatiu que proporciona la descomposició canònica de l'aplicació φ,

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\psi} \\ G/\varphi & \xrightarrow[\ \overline{\varphi}\ ]{} & \operatorname{im}\varphi \end{array}$$

Diagrama 2.2: Descomposició canònica d'un morfisme

ho és de morfismes per a conjunts amb una operació n-ària; s'anomena la descomposició canònica del morfisme φ.

Definició 2.4.5 (Descomposició canònica d'un morfisme d'accions)**.** Siguin K, G, H, conjunts, $\circ_G : K \times G \longrightarrow G$ i $\circ_H : K \times H \longrightarrow H$ accions de K en G i H, respectivament, i $\varphi : G \longrightarrow H$ un morfisme d'accions.

Donats elements $g, g' \in G$ tals que $g' \equiv g \pmod{\varphi}$, i $\lambda \in K$, tenim que $\varphi(\lambda \circ_G g') = \lambda \circ_H \varphi(g') = \lambda \circ_H \varphi(g) = \varphi(\lambda \circ_G g)$, de manera que $\lambda \circ_G g' \equiv \lambda \circ_G g \pmod{\varphi}$ i la relació d'equivalència $\equiv \pmod{\varphi}$ és compatible amb $\circ_G$. Això permet definir una acció $\circ$ de K en el conjunt quocient G/φ: donada una classe $\varphi^{-1}\big(\varphi(g)\big) \in G/\varphi$, i donat un element $\lambda \in K$, posem $\lambda \circ \varphi^{-1}\big(\varphi(g)\big) := \varphi^{-1}\big(\varphi(\lambda \circ_G g)\big)$. Amb aquesta acció en G/φ, l'aplicació de projecció $\pi : G \longrightarrow G/\varphi$ és un morfisme exhaustiu per a les accions $\circ_G$ i $\circ$.

D'altra banda, l'acció $\circ_H$ es pot restringir a $\operatorname{im}\varphi$, perquè donats elements $h \in \operatorname{im}\varphi$ i $\lambda \in K$, podem posar $h = \varphi(g)$ per a algun $g \in G$, i llavors és $\lambda \circ_H h = \lambda \circ_H \varphi(g) = \varphi(\lambda \circ_G g) \in \operatorname{im}\varphi$; i amb aquesta acció en $\operatorname{im}\varphi$, l'aplicació d'inclusió $\psi : \operatorname{im}\varphi \longrightarrow H$ és un morfisme per a les accions.

Finalment, l'aplicació canònica $\overline{\varphi} : G/\varphi \longrightarrow \operatorname{im}\varphi$, donada per $\varphi^{-1}\big(\varphi(g)\big) \mapsto \varphi(g)$, per a tot $g \in G$, és un isomorfisme per a les accions de G/φ i de $\operatorname{im}\varphi$. Així, el diagrama commutatiu que proporciona la descomposició canònica de l'aplicació φ,

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\psi} \\ G/\varphi & \xrightarrow[\overline{\varphi}]{} & \operatorname{im}\varphi \end{array}$$

Diagrama 2.3: Descomposició canònica d'un morfisme d'accions

ho és de morfismes d'accions de K; s'anomena la descomposició canònica del morfisme d'accions φ.

El resultat següent resumeix aquests fets.

Teorema 2.4.6 (Teorema d'isomorfia)**.** *Siguin K, G i H conjunts, $n \in \mathbb{N}$ un nombre natural, $*_G : G^n \longrightarrow G$ i $*_H : H^n \longrightarrow H$ operacions n-àries, $\circ_G : K \times G \longrightarrow G$ i $\circ_H : K \times H \longrightarrow H$ accions de K, i $\varphi : G \longrightarrow H$ una aplicació.*

(a) *Si φ és un morfisme de $(G, *_G)$ en $(H, *_H)$, llavors, l'aplicació $\overline{\varphi} : G/\varphi \longrightarrow \operatorname{im}\varphi$, donada per $\varphi^{-1}\big(\varphi(g)\big) := \varphi(g)$, està ben definida i és un isomorfisme per a conjunts amb una operació n-ària. A més a més, el diagrama commutatiu que proporciona la descomposició canònica de l'aplicació φ,*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\psi} \\ G/\varphi & \xrightarrow[\overline{\varphi}]{} & \operatorname{im}\varphi, \end{array}$$

ho és de morfismes.

(b) *Si φ és un morfisme de $(G, \circ_G)$ en $(H, \circ_H)$, llavors, l'aplicació $\overline{\varphi} : G/\varphi \longrightarrow \operatorname{im}\varphi$, donada per $\varphi^{-1}\big(\varphi(g)\big) := \varphi(g)$, està ben definida i és un isomorfisme per a conjunts amb acció de K. A més a més, el diagrama commutatiu que proporciona la descomposició canònica de l'aplicació φ,*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\psi} \\ G/\varphi & \xrightarrow[\overline{\varphi}]{} & \operatorname{im}\varphi, \end{array}$$

ho és de morfismes d'accions de K. □

2.5 Subgrups normals. Grups quocient

Recordem que hem definit (cf. **2.3.9** (a)) el nucli d'un morfisme de grups $\varphi : G \longrightarrow G'$ com $\ker\varphi := \varphi^{-1}(1)$; i que sabem que $\ker\varphi$ és un subgrup de G.

Definició 2.5.1. Siguin G un grup i $N \subseteq G$ un subgrup de G. Es diu que N és un subgrup normal de G si existeixen un grup G' i un morfisme de grups $\varphi : G \longrightarrow G'$ tals que $N = \ker\varphi$. És a dir, els subgrups normals d'un grup G són els nuclis dels morfismes de grups de G en qualsevol grup.

2.5.2. Notació. Donats un grup G, un subconjunt $S \subseteq G$ no necessàriament subgrup, i un element $g \in G$, escriurem $g \cdot S := \{g'' \in G : \text{ existeix } g' \in S \text{ i } g'' = g \cdot g'\}$; i, anàlogament, $S \cdot g := \{g'' \in G : \text{ existeix } g' \in S \text{ i } g'' = g' \cdot g\}$. Similarment, donats subconjunts $S, T \subseteq G$, denotarem per $S \cdot T$ el conjunt format pels productes $g \cdot g'$, per a $g \in S$, $g' \in T$. I posarem S^{-1} per a denotar el conjunt dels inversos dels elements de S.

Convé donar una caracterització més operativa a nivell elemental dels subgrups normals. Ho fem en el resultat següent.

Proposició 2.5.3. *Siguin G un grup i $N \subseteq G$ un subgrup. Les propietats següents són equivalents.*

(a) *N és subgrup normal de G.*

(b) *Per a tot element $g \in G$ és $g \cdot N \subseteq N \cdot g$.*

(c) *Per a tot element $g \in G$ és $g \cdot N = N \cdot g$.*

(d) *Per a tot element $g \in G$ és $g \cdot N \cdot g^{-1} = N$.*

(e) *Per a tot element $g \in G$ és $g \cdot N \cdot g^{-1} \subseteq N$.*

(f) *Per a tot element $g \in G$ i tot element $g' \in N$ és $g \cdot g' \cdot g^{-1} \in N$.*

Demostració: Comencem per veure la implicació (b) $\Longrightarrow$ (c). Donat $g \in G$, tenim que $g, g^{-1} \in G$ i llavors, per hipòtesi, $g \cdot N \subseteq N \cdot g$ i $g^{-1} \cdot N \subseteq N \cdot g^{-1}$. En multiplicar la segona inclusió a l'esquerra i a la dreta per g, obtenim la inclusió $N \cdot g \subseteq g \cdot N$, contrària a $g \cdot N \subseteq N \cdot g$; per tant, la igualtat $g \cdot N = N \cdot g$. Per a veure la implicació (c) $\Longrightarrow$ (d), només cal multiplicar per g^{-1} a la dreta. La implicació (d) $\Longrightarrow$ (e) és immediata. I també ho és l'equivalència (e) $\Longleftrightarrow$ (f), perquè (f) només és escriure amb elements la inclusió de (e). I per a veure la implicació (e) $\Longrightarrow$ (b), només cal multiplicar per g a la dreta. Doncs, només resta veure l'equivalència de (a) amb qualsevol de les altres propietats. Veiem que (a) $\Longrightarrow$ (e). Per hipòtesi, existeixen un grup G' i un morfisme de grups $\varphi : G \longrightarrow G'$ tals que $N = \ker\varphi$. Llavors, per a tot $g \in G$ i tot $g' \in N$, tenim que

$$\varphi(g \cdot g' \cdot g^{-1}) = \varphi(g) \cdot \varphi(g') \cdot \varphi(g^{-1}) = \varphi(g) \cdot 1 \cdot \varphi(g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) = \varphi(g) \cdot \varphi(g)^{-1} = 1;$$

o sigui, que $g \cdot g' \cdot g^{-1} \in \ker\varphi = N$, com calia veure.

Finalment, veiem que (c) $\Longrightarrow$ (a). Comencem per veure que per a $g, g' \in G$, és $g \cdot N \cap g' \cdot N = \varnothing$ o bé $g \cdot N = g' \cdot N$. En efecte, si $g \cdot N \cap g' \cdot N \neq \varnothing$, existeixen elements

$n, n' \in N$ tals que $g \cdot n = g' \cdot n'$; llavors, $g = g' \cdot n' \cdot n^{-1} \in g' \cdot N$, de manera que $g \cdot N \subseteq g' \cdot N$, i anàlogament, $g' \in g \cdot N$, d'on $g' \cdot N \subseteq g \cdot N$; és a dir, $g' \cdot N = g \cdot N$.

Així, com que cada element $g \in G$ pertany a algun dels conjunts $g \cdot N$, resulta que podem escriure G com a reunió disjunta de conjunts no buits de la forma $g \cdot N$. Designem per G/N el conjunt format per aquests subconjunts $g \cdot N$. Notem que, per hipòtesi, per a $g, g' \in G$, és $g' \cdot N = N \cdot g'$ de manera que

$$(g \cdot N) \cdot (g' \cdot N) = (g \cdot N) \cdot (N \cdot g') = g \cdot N \cdot g' = g \cdot (N \cdot g') = g \cdot (g' \cdot N) = (g \cdot g') \cdot N;$$

així, en G/N, podem definir una operació binària per $(g \cdot N) \cdot (g' \cdot N) := (g \cdot g') \cdot N$; i aquesta operació és associativa, perquè ho és la de G. A més a més, $1 \cdot N = N$ és element neutre per a aquest producte, i com que $(g \cdot N) \cdot (g^{-1} \cdot N) = N = (g^{-1} \cdot N) \cdot (g \cdot N)$, resulta que $g^{-1} \cdot N$ és l'invers de $g \cdot N$. Per tant, G/N, amb aquestes operacions, és un grup. I, per definició de les operacions, l'aplicació $\pi : G \longrightarrow G/N$ donada per $\pi(g) := g \cdot N$ és un morfisme de grups. I el càlcul del seu nucli és senzill, perquè els elements $g \in G$ tals que $g \cdot N = N$ són exactament els de N.

Així, doncs, hem demostrat que existeixen un grup, G/N, i un morfisme de grups, $\pi : G \longrightarrow G/N$, tals que $N = \ker \pi$; o sigui, que N és un subgrup normal de G. □

Observació 2.5.4. Notem que la propietat (e) és equivalent a dir que N és invariant per tots els automorfismes interns de G (cf. **2.2.3**).

Definició 2.5.5. Donats un grup G i un subgrup normal $N \subseteq G$, el grup G/N que hem construït a la demostració de **2.5.3** s'anomena el grup quocient de G per N, i el morfisme de grups $\pi : G \longrightarrow G/N$ s'anomena la projecció canònica de G en G/N.

Observació 2.5.6. Notem que els elements $g \cdot N$ de G/N, pensats com a subconjunts de G, són exactament les fibres del morfisme $\pi : G \longrightarrow G/N$; per tant, el grup G/N és el grup que abans hem denotat, com a conjunt, per G/π. Com a conseqüència, tenim la interpretació següent del teorema d'isomorfia.

Corol·lari 2.5.7 (Primer teorema d'isomorfia de grups)**.** *Siguin G, G' grups i $\varphi : G \to G'$ un morfisme de grups. Llavors, es té un isomorfisme de grups $\overline{\varphi} : G/\ker\varphi \longrightarrow \operatorname{im}\varphi$.* □

Corol·lari 2.5.8. *Siguin G, G' grups i $\varphi : G \longrightarrow G'$ un morfisme de grups. Si φ és exhaustiu, llavors G' és isomorf a $G/\ker\varphi$.* □

Exemples 2.5.9. (a) Sigui G un grup qualsevol; llavors, G i $\{1\}$ són subgrups normals de G. En efecte, tots els automorfismes i, en particular, els automorfismes interns, deixen invariants G i $\{1\}$.

(b) Tot subgrup d'un grup commutatiu és normal. En efecte; si G és commutatiu, l'únic automorfisme intern de G és la identitat, de manera que tot subgrup és invariant.

(c) Si $N \subseteq H \subseteq G$ són subgrups d'un grup G i $N \subseteq G$ és normal, llavors N és subgrup normal de H. En efecte, si N és el nucli d'un morfisme de grups $\varphi : G \longrightarrow G'$, també ho és de la restricció de φ a H, $H \xrightarrow{incl} G \xrightarrow{\varphi} G'$, que és $H \cap N = N$, perquè $N \subseteq H$.

(d) Com a exemple d'un grup G i un subgrup $H \subseteq G$ tal que H no sigui subgrup normal de G, podem posar el grup $G := S_3$ de les permutacions de tres elements (cf. **1.6.4**), i $H := \{1, (1,2)\}$; els conjugats de H són els subgrups $\{1, (0,1)\}$, $\{1, (0,2)\}$ i $\{1, (1,2)\}$.

(e) La intersecció d'una família no buida de subgrups normals és un subgrup normal. En efecte, si $\{N_i\}_{i\in I}$ és una família no buida ($I \neq \varnothing$) de subgrups normals de G, llavors cada N_i és invariant per tots els automorfismes interns de G, de manera que la seva intersecció, $\bigcap_{i\in I} N_i$, també és invariant per tots els automorfismes interns de G.

Proposició 2.5.10. *Siguin G, G' grups i $\varphi : G \longrightarrow G'$ un morfisme de grups. Llavors,*

(a) *Si $N \subseteq G'$ és un subgrup normal de G', la seva antiimatge, $\varphi^{-1}(N) \subseteq G$, és un subgrup normal de G.*

(b) *Si $N \subseteq G$ és un subgrup normal de G, la seva imatge, $\varphi(N)$, és un subgrup normal de $\operatorname{im}\varphi$, però no necessàriament subgrup normal de G'.*

Demostració:

(a) Donats elements $g \in G$ i $n \in \varphi^{-1}(N)$, tenim que $\varphi(g) \in G'$ i que $\varphi(n) \in N$; com que $N \subseteq G'$ és normal, resulta que $\varphi(g \cdot n \cdot g^{-1}) = \varphi(g) \cdot \varphi(n) \cdot \varphi(g)^{-1} \in N$; o sigui, $g \cdot n \cdot g^{-1} \in \varphi^{-1}(N)$, com calia provar.

(b) Anàlogament, donats $g' \in \operatorname{im}\varphi$ i $n' \in \varphi(N)$, existeixen $g \in G$ i $n \in N$ tals que $g' = \varphi(g)$ i $n' = \varphi(n)$; llavors, $g \cdot n \cdot g^{-1} \in N$, perquè N és normal en G, i, per tant, $g' \cdot n' \cdot g'^{-1} = \varphi(g) \cdot \varphi(n) \cdot \varphi(g)^{-1} = \varphi(g \cdot n \cdot g^{-1}) \in \varphi(N)$.

D'altra banda, notem que el subgrup $H := \{1, (0,1)\}$ de $G := S_3$ no és normal, de manera que $H \subseteq H$ és normal, però si $\varphi : H \longrightarrow G$ és la inclusió, llavors $\varphi(H)$ no és normal en G (cf. **2.5.9**, (d)). □

Proposició 2.5.11. *Siguin G i G' grups, N un subgrup normal de G, $\pi : G \longrightarrow G/N$ el morfisme projecció canònica, i $\varphi : G \longrightarrow G'$ un morfisme qualsevol de grups. Una condició necessària i suficient per a l'existència d'un morfisme de grups $\overline{\varphi} : G/N \longrightarrow G'$ que factoritzi φ a través de π, o sigui, tal que el diagrama*

Diagrama 2.4: Factorització d'un morfisme de grups

sigui commutatiu, és que $N \subseteq \ker\varphi$.

Demostració: La condició és, clarament, necessària, perquè si existeix el morfisme $\overline{\varphi}$ i $g \in N$, llavors, $\varphi(g) = \overline{\varphi}(\pi(g)) = \overline{\varphi}(N) = 1$, perquè $N \in G/N$ és l'element neutre de G/N. Recíprocament, si $g, g' \in G$ són tals que $g \cdot N = g' \cdot N$, llavors $g^{-1} \cdot g' \in N$, de manera que, per hipòtesi, $g^{-1} \cdot g' \in \ker\varphi$; així, $\varphi(g^{-1} \cdot g') = 1$ i $\varphi(g') = \varphi(g)$. Per tant, podem definir una aplicació $\overline{\varphi} : G/N \longrightarrow G'$ per l'assignació $g \cdot N \mapsto \varphi(g)$; i per a aquesta aplicació és $\varphi = \overline{\varphi} \circ \pi$. Finalment, com que φ és morfisme de grups, de la definició del grup quocient G/N resulta que $\overline{\varphi}$ és morfisme de grups. □

Definició 2.5.12. Aquesta propietat es pot interpretar d'una manera més precisa com una propietat universal del grup quocient. En efecte, donats un grup G i un subgrup normal $N \subseteq G$, podem definir un grup quocient de G mòdul N com un grup G' i un morfisme de grups $\pi : G \longrightarrow G'$ per al qual és $N \subseteq \ker \pi$ i tals que per a tot grup H i tot morfisme de grups $\varphi : G \longrightarrow H$ per al qual és $N \subseteq \ker \varphi$ existeix un únic morfisme de grups $\varphi' : G' \longrightarrow H$ tal que

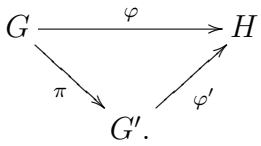
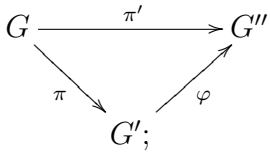


Diagrama 2.5: Propietat universal d'un grup quocient

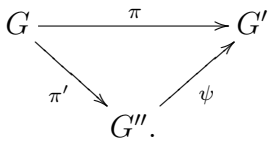
Es diu que φ' s'obté de φ per pas al quocient.

Acabem de provar-ne l'existència (cf. **2.5.5** i **2.5.11**). Per a la unicitat, tenim el resultat següent.

Proposició 2.5.13 (Unicitat del grup quocient)**.** *Siguin G un grup i N un subgrup normal de G. Si $\pi : G \longrightarrow G'$ i $\pi' : G \longrightarrow G''$ són grups quocient de G mòdul N, llavors existeix un únic morfisme de grups $\varphi : G' \longrightarrow G''$ tal que*



a més a més, aquest morfisme és un isomorfisme, amb invers l'únic morfisme de grups $\psi : G'' \longrightarrow G'$ tal que



Demostració: Per ser π i π' grups quocient de G mòdul N, tenim que $N \subseteq \ker \pi$ i que $N \subseteq \ker \pi'$; d'aquí obtenim l'existència dels morfismes φ i ψ. Ara, per composició, i de manera anàloga a la prova de la unicitat del producte de conjunts (cf. **1.2.4**), tenim que $\psi \circ \varphi = \mathrm{id}_{G'}$ i que $\varphi \circ \psi = \mathrm{id}_{G''}$; per tant, φ i ψ són isomorfismes, l'un invers de l'altre. □

Exercici 2.5.14. Siguin G i G', grups, $\varphi : G \longrightarrow G'$ un morfisme de grups, i $N \subseteq G$ un subgrup normal de G tal que $\ker \varphi \subseteq N$. Llavors, $\varphi(N) \subseteq \varphi(G)$ és un subgrup normal i $G/N \cong \varphi(G)/\varphi(N)$.

Acabarem la secció amb un resultat que posa de manifest la relació profunda de l'estructura del reticle (conjunt ordenat) dels subgrups d'un grup amb el de qualsevol dels seus quocients. Recordem, primerament, la definició de reticle.

Definició 2.5.15. Un reticle és un conjunt no buit, $\mathcal{S}$, amb un ordre parcial $\leq$, tal que per a tota parella d'elements $a, b \in \mathcal{S}$ existeixen suprem (o sigui, mínima fita superior), $a \vee b$, i ínfim (o sigui, màxima fita inferior), $a \wedge b \in \mathcal{S}$ del subconjunt $\{a, b\}$.

Exemple 2.5.16. Sigui G un grup. El conjunt $\mathcal{S}$ dels subgrups de G, amb l'ordre donat per la inclusió de conjunts, és un reticle. L'ínfim de dos subgrups H_1, $H_2 \subseteq G$, és el subgrup intersecció dels subgrups, $H_1 \cap H_2$; el suprem de dos subgrups H_1, $H_2 \subseteq G$, és el subgrup generat per la seva reunió, $\langle H_1 \cup H_2 \rangle$. Notem que el reticle té mínim, $\{1\}$, i màxim, G.

Exercici 2.5.17. Siguin G un grup, $N \subseteq G$ un subgrup normal de G, i $\pi : G \longrightarrow G/N$ el morfisme projecció canònica. Denotem per $\mathcal{S}(G, N)$ el conjunt dels subgrups de G que contenen N i per $\mathcal{S}(G/N)$ el conjunt dels subgrups de G/N. Llavors, l'aplicació $f : \mathcal{S}(G/N) \longrightarrow \mathcal{S}(G, N)$ donada per $H \mapsto \pi^{-1}(H)$ està bén definida, és bijectiva, respecta l'ordre donat per inclusió en cadascun dels dos reticles $\mathcal{S}(G/N)$ i $\mathcal{S}(G, N)$, i transforma subgrups normals en subgrups normals, en els dos sentits.

Aquest resultat s'acostuma a llegir en la forma "existeix una bijecció que respecta l'ordre i el caràcter de normalitat entre el conjunt dels subgrups de G que contenen N i el conjunt dels subgrups del grup quocient G/N".

Observació 2.5.18. Per a la definició de grup quocient cal tenir molt present la condició que el subgrup $N \subseteq G$ sigui normal. En efecte, si a la definició no s'exigís aquesta propietat i N no fos normal, l'existència de quocient i la seva unicitat també tindríen lloc, però el grup quocient seria G/N', amb la projecció canònica $\pi : G \longrightarrow G/N'$, on N' és el subgrup normal generat per N; és a dir, la intersecció de tots els subgrups normals de G que contenen N. Això faria que per a subgrups diferents N_1 i N_2 el quocient fos el mateix.

Per exemple, el subgrup normal generat per cadascun dels subgrups $N_0 := \{1, (1, 2)\}$, $N_1 := \{1, (0, 2)\}$, i $N_2 := \{1, (0, 1)\}$ del grup simètric S_3, és el propi grup S_3, i els quocients serien tots tres el grup trivial, d'un sol element.

2.6 Teoremes d'isomorfia de grups

Els teoremes d'isomorfia que tractarem en aquesta secció es troben a la majoria dels tractats d'àlgebra; però no tots els seus autors fan servir de la mateixa manera el qualificatiu que els acompanya: primer, segon o tercer (cf., per exemple, [Artin 1991], [Jacobson 1974], o [Lang 1984]). Aquí els hem anomenat d'acord amb l'ordre en què els demostrem, sense cap més pretensió ni motivació.

Observació 2.6.1. Notem que si $\varphi : G \longrightarrow G'$ és un morfisme exhaustiu de grups, el primer teorema d'isomorfia de grups (cf. **2.5.7**) ens permet dir que G' és (isomorf a) un quocient de G, de manera que el resultat següent es pot llegir, efectivament, en la forma "un quocient d'un quocient és un quocient".

Proposició 2.6.2 (Un quocient d'un quocient és un quocient)**.** *Considerem G, G' grups, $\varphi : G \longrightarrow G'$ un morfisme exhaustiu de grups, i $N' \subseteq G'$ un subgrup normal de G'. Llavors, $\varphi^{-1}(N') \subseteq G$ és un subgrup normal i φ defineix, per pas al quocient, un isomorfisme de grups $G/\varphi^{-1}(N') \cong G'/N'$.*

Demostració: Considerem la projecció canònica $\rho : G' \longrightarrow G'/N'$, donada per l'assignació $g' \mapsto g' \cdot N'$, i el morfisme composició $\rho \circ \varphi : G \longrightarrow G' \longrightarrow G'/N'$. Com que φ i ρ són morfismes exhaustius de grups, també aquesta composició és un morfisme exhaustiu de

grups, de manera que, pel primer teorema d'isomorfia de grups (cf. **2.5.7**), $\rho\circ\varphi$ factoritza en un isomorfisme $G/\ker(\rho\circ\varphi)\cong \operatorname{im}(\rho\circ\varphi)=G'/N'$; finalment, només cal adonar-se que $\ker(\rho\circ\varphi)=\varphi^{-1}(\ker\rho)=\varphi^{-1}(N')$. El diagrama següent resumeix la situació. □

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & G' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\rho} \\ G/\varphi^{-1}(N') & \xrightarrow[\ \overline{\varphi}\ ]{} & G'/N'. \end{array}$$

Diagrama 2.6: Un quocient d'un quocient és un quocient

Teorema 2.6.3 (Segon teorema d'isomorfia de grups)**.** *Siguin G un grup i $N\subseteq H\subseteq G$ subgrups normals de G. Llavors, N és un subgrup normal de H, $H/N\subseteq G/N$ és un subgrup normal de G/N i es té un isomorfisme canònic $(G/N)/(H/N)\cong G/H$.*

Demostració: Considerem la projecció canònica $\rho: G\longrightarrow G/H$; com que $N\subseteq H=\ker\rho$, la proposició **2.5.11** ens diu que ρ factoritza a través del quocient G/N; és a dir, que existeix un morfisme $\overline{\rho}: G/N\longrightarrow G/H$ tal que

$$\begin{array}{ccc} G & \xrightarrow{\ \rho\ } & G/H \\ {\scriptstyle\pi}\downarrow & \nearrow{\scriptstyle\overline{\rho}} & \\ G/N. & & \end{array}$$

Com que ρ és exhaustiu, també $\overline{\rho}$ és exhaustiu. El nucli d'aquest morfisme és format per les classes $g\cdot N$, $g\in G$, per a les quals és $g\cdot H=H$; és a dir, per a les quals és $g\in H$; és a dir, el nucli és H/N (en particular, H/N és un subgrup normal de G/N). El primer teorema d'isomorfia (cf. **2.5.7**) ens ensenya que $\overline{\rho}$ factoritza a través del quocient i que així s'obté un isomorfisme $\overline{\overline{\rho}}$ d'acord amb el diagrama següent, on $\overline{\pi}$ és la projecció canònica de G/N en el quocient per H/N:

$$\begin{array}{ccc} G & & \\ {\scriptstyle\pi}\downarrow & \searrow^{\rho} & \\ G/N & \xrightarrow{\ \overline{\rho}\ } & G/H.\ \square \\ {\scriptstyle\overline{\pi}}\downarrow & \nearrow_{\overline{\overline{\rho}},\cong} & \\ (G/N)/(H/N) & & \end{array}$$

Diagrama 2.7: Segon teorema d'isomorfia de grups

Teorema 2.6.4 (Tercer teorema d'isomorfia de grups)**.** *Siguin G un grup, $H,N\subseteq G$ subgrups de G, i suposem que N és un subgrup normal de G. Llavors, $H\cdot N=N\cdot H$, $H\cdot N\subseteq G$ és un subgrup, $N\subseteq H\cdot N$ és un subgrup normal, $N\cap H\subseteq H$ és un subgrup normal, i es té un isomorfisme canònic $H\cdot N/N\cong H/(N\cap H)$.*

Demostració: Per a tot $g\in N$ i tot $h\in H$, com que N és normal en G, tenim que $h\cdot g\cdot h^{-1}\in N$; per tant, $h\cdot g=(h\cdot g\cdot h^{-1})\cdot h\in N\cdot H$; això ens diu que $H\cdot N\subseteq N\cdot H$. La

inclusió contrària, $N \cdot H \subseteq H \cdot N$ es prova anàlogament. Aquesta propietat ens permet veure fàcilment que $N \cdot H$ és un subgrup de G. En efecte, l'operació producte del grup G es pot restringir a $N \cdot H$, ja que donats $g, g' \in N$, $h, h' \in H$, tenim que

$$(g \cdot h) \cdot (g' \cdot h') = g \cdot (h \cdot g') \cdot h' \in g \cdot (H \cdot N) \cdot h' = g \cdot (N \cdot H) \cdot h' = N \cdot H.$$

A més a més, l'element neutre $1 = 1 \cdot 1 \in N \cdot H$, i $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1} \in H \cdot N = N \cdot H$; per tant, podem restringir a $N \cdot H$ les tres operacions de grup de G, com calia veure.

D'altra banda, com que N és un subgrup normal de G i també és $N \subseteq H \cdot N$, tenim que N és un subgrup normal de $H \cdot N$. En particular, té sentit considerar el grup quocient $(H \cdot N)/N$ i la projecció canònica $\pi : H \cdot N \longrightarrow (H \cdot N)/N$. La composició amb la inclusió $incl : H \longrightarrow (H \cdot N)$ proporciona un morfisme de grups $\varphi := \pi \circ incl : H \longrightarrow (H \cdot N)/N$; aquest morfisme és exhaustiu, perquè per a $h \in H$ i $g \in N$, hi ha igualtat de classes $(h \cdot g) \cdot N = h \cdot N$, de manera que tota classe en $(H \cdot N)/N$ admet un representant en H. Finalment, el càlcul del nucli d'aquest morfisme és immediat, i proporciona que $\ker \varphi = H \cap \ker \pi = H \cap N$. El primer teorema d'isomorfia de grups (cf. **2.5.7**) permet concloure que $H \cap N$ és un subgrup normal de H i que es té l'isomorfisme que es volia $H/(H \cap N) \cong (H \cdot N)/N$. La situació es pot resumir en el diagrama següent,

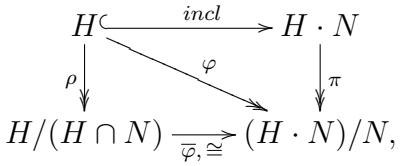
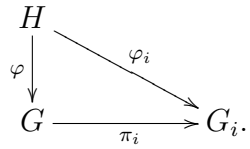


Diagrama 2.8: Tercer teorema d'isomorfia

on $\rho : H \longrightarrow H/(H \cap N)$ és la projecció canònica. □

2.7 Producte de grups

Recordem que, donada una família no buida de conjunts, $\{G_i\}_{i \in I}$, hem definit un producte d'aquesta família (cf. **1.2.1**) com un conjunt G i una família $\{\pi_i : G \longrightarrow G_i\}_{i \in I}$ d'aplicacions de manera que per a tot conjunt H i tota família d'aplicacions $\{\varphi_i : H \longrightarrow G_i\}_{i \in I}$ existeix una única aplicació $\varphi : H \longrightarrow G$ que fa commutar tots els diagrames



Ara es tracta de definir una estructura similar per al cas de grups.

Definició 2.7.1. Sigui $\{G_i\}_{i \in I}$ una família no buida de grups i considerem el producte, $G := \prod_{i \in I} G_i$, dels conjunts G_i. En G, podem definir una única estructura de grup de manera que totes les projeccions $\pi_i : \prod_{j \in I} G_j \longrightarrow G_i$, $i \in I$, donades per $\pi_i(\{g_j\}_{j \in I}) := g_i$, siguin morfismes de grups.

En efecte, donats elements $\{g_i\}_{i\in I}, \{g'_i\}_{i\in I} \in G$, amb $g_i, g'_i \in G_i$, per a tot $i \in I$, podem definir

$$\{g_i\}_{i\in I} \cdot \{g'_i\}_{i\in I} := \{g_i \cdot g'_i\}_{i\in I} \in G.$$

Aquest producte, juntament amb la família $1 := \{g_i = 1\}_{i\in I} \in G$, com a element neutre, i $\{g_i^{-1}\}_{i\in I} \in G$ com a invers de l'element $\{g_i\}_{i\in I} \in G$, determina una estructura de grup en G de manera que les projeccions π_i, $i \in I$, siguin morfismes de grups. I, clarament, és única, perquè si volem que π_i sigui un morfisme de grups, el component i-èsim del producte ha de ser el producte dels components i-èsims dels factors. El grup G, juntament amb les projeccions π_i, $i \in I$, s'anomena el grup producte de la família $\{G_i\}_{i\in I}$. Notem que si tots els grups G_i, $i \in I$, són commutatius, llavors G també és commutatiu.

Proposició 2.7.2 (Propietat universal del producte)**.** *Siguin $\{G_i\}_{i\in I}$ una família no buida de grups i $G := \prod_{i\in I} G_i$, amb les projeccions canòniques $\pi_i : G \longrightarrow G_i$, el seu producte, tal com l'acabem de definir. Aleshores, per a tot grup H i tota família de morfismes de grups $\{\psi_i : H \longrightarrow G_i\}_{i\in I}$, existeix un únic morfisme de grups $\psi : H \longrightarrow G$ tal que per a tot índex $i \in I$ és $\psi_i = \pi_i \circ \psi$; és a dir, tal que per a tot índex $i \in I$ el diagrama següent és commutatiu:*

$$\forall \{\psi_i\}_{i\in I}\, \exists! \psi\, \forall i \in I$$

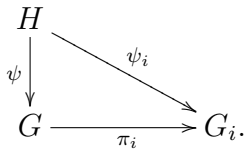
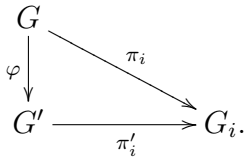


Diagrama 2.9: Propietat universal del producte de grups

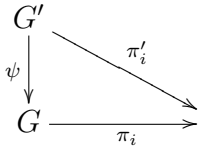
Demostració: L'única aplicació del conjunt H en el conjunt G, $\psi : H \longrightarrow G$, per a la qual és $\psi_i = \pi_i \circ \psi$, per a tot $i \in I$, és l'aplicació donada per $\psi(h) := \{\psi_i(h)\}_{i\in I}$; i aquesta aplicació és un morfisme de grups. □

Corol·lari 2.7.3 (Unicitat del producte)**.** *Sigui $\{G_i\}_{i\in I}$ una família no buida de grups, i suposem que existeixen grups G, G', i famílies de morfismes de grups $\{\pi_i : G \longrightarrow G_i\}_{i\in I}$, $\{\pi'_i : G' \longrightarrow G_i\}_{i\in I}$, tals que se satisfà la propietat universal del producte per a cadascuna de les dues famílies; és a dir, que per a tot grup H i tota família de morfismes de grups $\{\psi_i : H \longrightarrow G_i\}_{i\in I}$, existeix un únic morfisme de grups $\psi : H \longrightarrow G$ tal que per a tot $i \in I$ és $\psi_i = \pi_i \circ \psi$; i existeix un únic morfisme de grups $\psi' : H \longrightarrow G'$ tal que per a tot $i \in I$ és $\psi_i = \pi'_i \circ \psi'$. Llavors, existeix un únic isomorfisme de grups $\varphi : G \longrightarrow G'$ tal que per a tot $i \in I$ és $\pi_i = \pi'_i \circ \varphi$.*

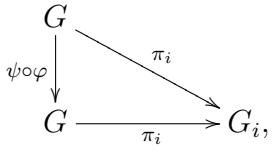
Demostració: Com que per a G' i $\{\pi'_i\}_{i\in I}$ se satisfà la propietat universal del producte, si prenem $H := G$ i $\psi'_i := \pi_i$, obtenim l'existència d'un morfisme de grups $\varphi : G \longrightarrow G'$, que és l'únic tal que, per a tot $i \in I$ és

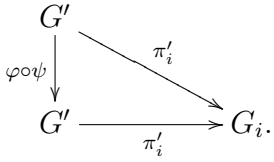


Anàlogament, com que per a G i $\{\pi_i\}_{i\in I}$ se satisfà la propietat universal del producte, si prenem $H := G'$ i $\psi_i := \pi'_i$, obtenim l'existència d'un morfisme de grups $\psi : G' \longrightarrow G$ tal que, per a tot $i \in I$ és

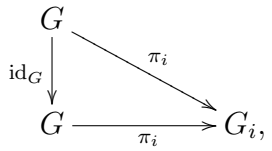


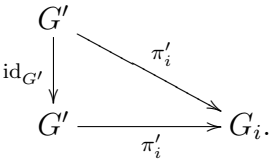
Per composició, obtenim morfismes de grups $\psi \circ \varphi : G \longrightarrow G$ i $\varphi \circ \psi : G' \longrightarrow G'$ tals que per a tot $i \in I$ és





Ara bé, per a les identitats $\mathrm{id}_G : G \longrightarrow G$ i $\mathrm{id}_{G'} : G' \longrightarrow G'$ també se satisfà que





Per les unicitats de les hipòtesis, aplicades a les famílies $H = G$ i $\{\psi_i\}_{i\in I} = \{\pi_i\}_{i\in I}$, i $H = G'$ i $\{\psi_i\}_{i\in I} = \{\pi'_i\}_{i\in I}$, respectivament, obtenim que $\psi \circ \varphi = \mathrm{id}_G$ i que $\varphi \circ \psi = \mathrm{id}_{G'}$; és a dir, que l'únic morfisme de grups $\varphi : G \longrightarrow G'$ per al qual se satisfà la propietat demanada és un isomorfisme. Això demostra l'existència i la unicitat de l'isomorfisme que volíem trobar. □

2.8 Grups cíclics

Hem definit el concepte de subgrup generat per un subconjunt S d'un grup G (cf. la definició **2.3.13**). En particular, té sentit pensar en quins subconjunts $S \subseteq G$ generen tot G. Pot ser que G pugui ésser generat per subconjunts finits o no.

Definició 2.8.1. Sigui G un grup. Es diu que G és finitament generat si existeix un subconjunt finit $S \subseteq G$ tal que G és el subgrup de G generat per S.

Exemples 2.8.2. • Qualsevol grup finit és, òbviament, finitament generat.

• El grup additiu $\mathbb{Z}$ dels nombres enters és finitament generat; els conjunts $\{1\}$ i $\{-1\}$ en són conjunts de generadors. En particular, $(\mathbb{Z}, +, 0, -)$ és infinit i generat per un sol element (cf., més avall, **2.8.5**).

• Hem vist en **2.3.16** que el grup multiplicatiu $(\mathbb{Q}_{>0}, \cdot, 1, (\ )^{-1})$ dels nombres racionals positius admet com a conjunt de generadors el subconjunt (infinit) format per tots els nombres naturals primers; però no admet cap subconjunt finit de generadors.

En efecte, sigui $S \subseteq \mathbb{Q}_{>0}$ un subconjunt finit qualsevol, i posem $S = \left\{\dfrac{a_1}{b_1}, \ldots, \dfrac{a_r}{b_r}\right\}$, amb $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbb{Z}_{>0}$, i $\mathrm{mcd}(a_i, b_i) = 1$, per a $1 \leq i \leq r$. Llavors, el conjunt

P_S format pels nombres naturals primers p tals que existeix i, $1 \leq i \leq r$, i p divideix a_i o b_i, també és finit. I el subgrup de $\mathbb{Q}_{>0}$ generat per S no conté cap nombre racional de numerador o denominador divisible per un nombre primer que no pertanyi a P_S. □

• Tampoc no és finitament generat el grup additiu dels nombres racionals, $(\mathbb{Q}, +, 0, -)$. En efecte, si $S \subseteq \mathbb{Q}$ és un subconjunt finit i $d \in \mathbb{Z}_{>0}$ és un denominador comú dels elements de S, el subgrup generat per S no conté cap nombre racional de denominador múltiple estricte de d; per tant, no pot ser tot $\mathbb{Q}$. □

2.8.3. Donat un grup G, cada element $g \in G$ genera un subgrup de G. Així, tot grup G conté subgrups generats per un sol element. És convenient, doncs, començar per l'estudi dels grups generats per un sol element.

Definició 2.8.4. Sigui G un grup. Es diu que G és cíclic si G admet un conjunt de generadors format per un sol element. Això és dir que existeix un element $g \in G$ de manera que G és el subgrup de G generat per g.

Exemples 2.8.5. • El grup $\mathbb{Z}$, dels nombres enters amb la suma, és un grup cíclic, generat per $\{1\}$, i també per $\{-1\}$. En efecte, si un subgrup de $\mathbb{Z}$ conté 1, llavors conté 0, conté 1, conté $2 = 1 + 1$ i, per inducció, conté tots els nombres naturals; i com que és un grup, conté els seus inversos; així, conté $\mathbb{N} \cup -\mathbb{N} = \mathbb{Z}$. D'altra banda, si un subgrup de $\mathbb{Z}$ conté -1, llavors conté el seu invers, 1, de manera que el subgrup és tot $\mathbb{Z}$. □

• Per a tot nombre enter $n \geq 1$, el grup quocient de $\mathbb{Z}$ pel subgrup $n\mathbb{Z}$, dels nombres enters múltiples de n, $\mathbb{Z}/n\mathbb{Z}$, és un grup cíclic (cf., més avall, **2.8.8**). La classe d'un nombre enter a genera $\mathbb{Z}/n\mathbb{Z}$ si, i només si, $\mathrm{mcd}(a, n) = 1$ (cf., més avall, **2.8.12**).

• Sigui $n \geq 1$ un nombre enter. El grup de les arrels n-èsimes de la unitat en el conjunt $\mathbb{C}$ dels nombres complexos és cíclic, generat per qualsevol arrel primitiva n-èsima de la unitat; és a dir, per $e^{2\pi ik/n} = \cos(2k\pi/n) + i\sin(2k\pi/n)$, amb $1 \leq k \leq n$, $\mathrm{mcd}(k, n) = 1$ (cf., més avall, **2.8.12**).

• En general, els subgrups finits del grup dels elements invertibles d'un cos són cíclics. Més endavant (cf. **6.4.18**) en veurem una demostració.

Comencem per estudiar el grup additiu dels nombres enters, $(\mathbb{Z}, +, 0, -)$; en particular, els seus subgrups i els seus quocients.

Proposició 2.8.6 (Subgrups de $(\mathbb{Z}, +, 0, -)$)**.** *Els subgrups del grup additiu dels nombres enters són, exactament, els* $n\mathbb{Z} := \{n \cdot a : a \in \mathbb{Z}\}$*, per a* $n \in \mathbb{Z}$*. A més a més, per a* $m, n \in \mathbb{Z}$*, tenim que* $m\mathbb{Z} = n\mathbb{Z}$ *si, i només si,* $m = \pm n$*, i* $m\mathbb{Z} \subseteq n\mathbb{Z}$ *si, i només si,* n *divideix* m*.*

Demostració: Sigui $n \in \mathbb{Z}$, $n \neq 0$, i considerem l'aplicació $\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z}$ donada per l'assignació $a \mapsto n \cdot a$, per a $a \in \mathbb{Z}$. Llavors, φ_n és un morfisme de grups. Entre altres coses, això ens diu que la seva imatge, que és exactament $n\mathbb{Z}$, és un subgrup de $\mathbb{Z}$, i que és un grup cíclic generat per n, que és la imatge del generador 1 de $\mathbb{Z}$. A més a més, el nucli del morfisme φ_n és $\{0\}$, perquè per a $n, a \in \mathbb{Z}$, si és $n \cdot a = 0$ i $n \neq 0$, llavors ha de ser $a = 0$. El teorema d'isomorfia ens diu que $\mathbb{Z} \cong n\mathbb{Z}$, per a $n \neq 0$.

Ara, si $m\mathbb{Z} = n\mathbb{Z}$, del fet que $n \in m\mathbb{Z}$ obtenim l'existència d'un nombre enter $a \in \mathbb{Z}$ tal que $n = m \cdot a$; i, anàlogament, del fet que $m \in n\mathbb{Z}$ obtenim l'existència d'un nombre enter $b \in \mathbb{Z}$ tal que $m = n \cdot b$; així, $n = n \cdot (b \cdot a)$, de manera que, com que $n \neq 0$, és

$b \cdot a = 1$, d'on $b = a = \pm 1$, i $m = \pm n$, com volíem veure. En particular, hem vist que $m\mathbb{Z} \subseteq n\mathbb{Z}$ si, i només si, n divideix m.

Resta veure que no hi ha cap més subgrup que els que acabem de descriure. Però això també és senzill. Si $G \subseteq \mathbb{Z}$ és el subgrup $\{0\}$, tenim que és $G = 0\mathbb{Z}$. Suposem, doncs, que $G \neq \{0\}$. Com que existeix algun nombre enter $n \in G$, $n \neq 0$, i com que si $m \in G$ llavors $-m \in G$, tenim que existeix $n \in G$, $n > 0$ i, en conseqüència, existeix el menor nombre enter positiu n tal que $n \in G$. Afirmem que $G = n\mathbb{Z}$. Com que $n \in G$, la inclusió $n\mathbb{Z} \subseteq G$ és immediata. Recíprocament, si $b \in G$, en fer la divisió entera de b entre n, obtenim l'existència d'un quocient $q \in \mathbb{Z}$ i un residu $m \in \mathbb{Z}$, $0 \leq m < n$, tals que $b = n \cdot q + m$. Llavors, $m = b - n \cdot q \in G$, i si fos $m > 0$, això contradiria l'elecció de n com el nombre positiu no nul més petit de G; per tant, ha de ser $m = 0$, de manera que $b = n \cdot q \in n\mathbb{Z}$, con restava veure. □

Corol·lari 2.8.7. *En particular, tots els subgrups diferents de* $\{0\}$ *del grup additiu dels nombres enters són grups cíclics, i isomorfs a* $(\mathbb{Z}, +, 0, -)$. □

Observació 2.8.8. De **2.3.17** es dedueix immediatament que la imatge d'un grup cíclic per un morfisme de grups és un grup cíclic. En particular, per a tot $n \in \mathbb{Z}$, el grup quocient $\mathbb{Z}/n\mathbb{Z}$ és cíclic. I, llevat d'isomorfismes de grups, no n'hi ha més. Vegem-ho.

Proposició 2.8.9. *Sigui G un grup cíclic. Llavors, existeix un morfisme exhaustiu de grups $\varphi : \mathbb{Z} \longrightarrow G$; en conseqüència, existeix $n \in \mathbb{N}$ i $G \cong \mathbb{Z}/n\mathbb{Z}$.* (Notem que per a $n = 0$ és $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.)

Demostració: Sigui g un generador de G; llavors, existeix un únic morfisme de grups $\varphi : \mathbb{Z} \longrightarrow G$ tal que $\varphi(1) = g$; en efecte, φ és l'aplicació donada per l'assignació $n \mapsto g^n$. Com que el generador de G pertany a la imatge de φ, resulta que φ és un morfisme exhaustiu i el teorema d'isomorfia ens permet assegurar que $G = \operatorname{im}\varphi \cong \mathbb{Z}/\ker\varphi$. Ara, com que $\ker\varphi \subseteq \mathbb{Z}$ és un subgrup, tenim que existeix $n \in \mathbb{N}$ tal que $\ker\varphi = n\mathbb{Z}$. Això acaba la prova. □

Definició 2.8.10. Siguin G un grup i $g \in G$ un element qualsevol. Llavors, $\langle g \rangle \subseteq G$ és un subgrup cíclic de G; per tant, existeix un únic nombre natural $n \in \mathbb{N}$ tal que $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Si $n = 0$, es diu que g és d'ordre infinit; si $n \neq 0$, es diu que g és d'ordre n.

Així, doncs, l'ordre d'un element g d'un grup G és el generador no negatiu del nucli de l'únic morfisme de grups $\varphi : \mathbb{Z} \longrightarrow G$ que envia 1 a g, si aquest nucli és no nul, i l'ordre es infinit si el nucli és $\{0\}$.

Exercici 2.8.11. Siguin G un grup i $g \in G$ un element qualsevol. L'ordre de g és el menor nombre natural, $n \geq 1$, si existeix, tal que $g^n = 1$; si no existeix, g és d'ordre infinit.

Proposició 2.8.12. *Sigui G un grup i suposem que $g \in G$ és un element d'ordre finit, n. Llavors, per a tot nombre enter k, l'ordre de g^k és* $\dfrac{n}{\operatorname{mcd}(k,n)}$.

Demostració: Posem $d := \operatorname{mcd}(k,n)$, i escrivim $n = d \cdot n'$, $k = d \cdot k'$, amb $n', k' \in \mathbb{Z}$; tindrem que $\operatorname{mcd}(n', k') = 1$ i que $\dfrac{n}{\operatorname{mcd}(k,n)} = n'$. Notem que $(g^k)^{n'} = g^{k \cdot n'} = g^{n \cdot k'} = 1$; per tant, g^k és d'ordre finit, $m \geq 1$, del qual acabem de veure que és $m \leq n'$. Es tracta de veure que $m = n'$. Però si fos $m < n'$, llavors seria $k \cdot m < k \cdot n' = n$, i, alhora, tindríem que $g^{k \cdot m} = (g^k)^m = 1$, fet que contradiria que g és d'ordre n. □

Exercici 2.8.13. Siguin G un grup i $g \in G$ un element d'ordre finit, n. Si per a algun nombre enter $m \geq 1$ és $g^m = 1$, llavors n és un divisor de m.

Exercici 2.8.14. Siguin G un grup cíclic i $g \in G$ un generador de G.

(a) Si g és d'ordre infinit, per a tot grup H i tot element $h \in H$ existeix un únic morfisme de grups $\varphi : G \longrightarrow H$ tal que $\varphi(g) = h$.

(b) Si g és d'ordre finit, n, donats un grup H i un element $h \in H$, existeix un morfisme de grups $\varphi : G \longrightarrow H$ tal que $\varphi(g) = h$ si, i només si, l'ordre de h és un divisor de n. En aquest cas, φ és necessàriament únic.

Observació 2.8.15. Per a tot nombre enter $n \geq 2$, podem considerar el grup multiplicatiu $(\mathbb{Z}/n\mathbb{Z})^*$, format pels elements invertibles de l'anell $\mathbb{Z}/n\mathbb{Z}$; això és, format per les classes que admeten un representant $a \in \mathbb{Z}$ tal que $\text{mcd}(a, n) = 1$. A l'assignatura d'Aritmètica es treballa amb el concepte d'arrel primitiva mòdul un nombre enter $n \geq 2$. En particular, l'existència d'arrels primitives mòdul n és equivalent al fet que el grup $(\mathbb{Z}/n\mathbb{Z})^*$ sigui cíclic.

Exercici 2.8.16. Sigui G un grup cíclic finit de cardinal n. Llavors, el grup dels automorfismes de G és isomorf a $(\mathbb{Z}/n\mathbb{Z})^*$.

Exercici 2.8.17. Sigui G un grup cíclic finit de cardinal n.

(a) L'aplicació f que assigna a cada subgrup $H \subseteq G$ el seu cardinal, $H \mapsto f(H) := \#H$, és una bijecció del reticle dels subgrups de G en el reticle dels divisors naturals de n; és a dir, aquesta bijecció transforma l'ordre d'inclusió entre subgrups en l'ordre dels divisors de n donat per la divisibilitat; és a dir, f és tal que $H \subseteq H'$ si, i només si, $f(H)|f(H')$.

(b) Existeix una bijecció, g, del reticle dels subgrups de G en el reticle dels divisors naturals de n tal que $H \subseteq H'$ si, i només si, $g(H')|g(H)$.

Capítol 3

Accions de grups

Molts exemples de grups apareixen com a grups d'automorfismes d'algun conjunt amb alguna estructura algebraica. Es tracta de veure que aquest fet no és casual i que, de fet, una manera molt natural de pensar els grups és com a (sub)grups d'automorfismes.

3.1 Accions d'un grup en un conjunt

L'eina bàsica que permet interpretar els grups com a grups d'automorfismes és el concepte d'acció d'un grup en un conjunt.

Definició 3.1.1. Siguin G un grup i X un conjunt no buit. Es diu que el grup G opera per l'esquerra en X, o que el grup G actua per l'esquerra en X, o que X és un G-conjunt per l'esquerra, si existeix una acció $G \times X \longrightarrow X$, que escriurem $(g, x) \mapsto g \cdot x$, per a la qual se satisfan les dues propietats següents:

(a) per a tots els elements $g, g' \in G$ i tot element $x \in X$ és $(g \cdot g') \cdot x = g \cdot (g' \cdot x)$; i

(b) per a tot element $x \in X$ és $1 \cdot x = x$.

Notem que per a l'acció per l'esquerra hem fet servir notació multiplicativa.

Observació 3.1.2. Notem també que la primera propietat expressa una certa compatibilitat del producte del grup amb l'acció; i la segona, una certa compatibilitat del neutre del grup amb l'acció; i que aquestes dues propietats impliquen la compatibilitat següent dels inversos amb l'acció: per a tot $g \in G$ i tot $x \in X$, és $g^{-1} \cdot (g \cdot x) = x = g \cdot (g^{-1} \cdot x)$.

Definició 3.1.3. Siguin G un grup i X un conjunt no buit. Es diu que el grup G opera per la dreta en X, o que el grup G actua per la dreta en X, o que X és un G-conjunt per la dreta, si existeix una acció $G \times X \longrightarrow X$, que escriurem $(g, x) \mapsto x^g$, per a la qual se satisfan les dues propietats següents:

(a) per a tots els elements $g, g' \in G$ i tot element $x \in X$ és $x^{g \cdot g'} = (x^g)^{g'}$; i

(b) per a tot element $x \in X$ és $x^1 = x$.

Notem que per a una acció per la dreta és més còmoda la notació exponencial.

Observació 3.1.4. Notem la diferència essencial entre una acció per l'esquerra i una acció per la dreta. En una acció per l'esquerra, donats elements $g, g' \in G$ i un element $x \in X$, l'acció del producte $g \cdot g'$ sobre un element $x \in X$ es produeix primerament per l'acció de g' sobre x, i després per l'acció de g sobre el resultat anterior. En canvi, si l'acció és per la dreta, l'acció del mateix producte $g \cdot g'$ sobre x es produeix primerament per l'acció de g sobre x, i després per l'acció de g' sobre el resultat anterior. Òbviament, si el grup és commutatiu, tota acció per l'esquerra ho és per la dreta i recíprocament. Es parla d'una acció bilateral o bé, simplement, d'una acció.

Exemples 3.1.5. (a) Donat un conjunt qualsevol, X, qualsevol subgrup G del grup de les aplicacions bijectives de X en X actua per l'esquerra de manera natural en el conjunt X: l'acció $G \times X \longrightarrow X$ és donada per l'assignació òbvia $(\sigma, x) \mapsto \sigma(x)$.

(b) En particular, donat un conjunt G amb una família d'operacions $\{*_i : G^{n_i} \longrightarrow G\}_{i \in I}$ i una família d'accions de conjunts $\{\circ_j : K_j \times G \longrightarrow G\}_{j \in J}$, el grup dels automorfismes de G per a aquestes operacions i accions, $\mathrm{Aut}(G, \{*_i\}_{i \in I}, \{\circ_j\}_{j \in J})$, opera per l'esquerra de manera natural en el conjunt G.

(c) Així, doncs, donat un grup G, el grup d'automorfismes de G actua per l'esquerra de manera natural en el conjunt dels elements de G: l'acció $\mathrm{Aut}(G) \times G \longrightarrow G$ és donada per l'assignació òbvia $(\sigma, g) \mapsto \sigma(g)$.

(d) Sigui G un grup. L'aplicació $G \times G \longrightarrow G$ donada per l'assignació $(\sigma, g) \mapsto \sigma \cdot g$, per a $\sigma \in G$, i $g \in G$, on pensem σ com a operador i g com objecte sobre el qual s'opera, és una acció per l'esquerra del grup G en el conjunt G; s'anomena la translació per l'esquerra.

(e) Sigui G un grup. El grup G també opera per la dreta en el conjunt G per tanslació. L'acció és donada per l'assignació $(\sigma, g) \mapsto g \cdot \sigma$, per a $\sigma \in G$, i $g \in G$ (pensem σ com a operador i g com objecte sobre el qual s'opera). L'acció s'anomena la translació per la dreta.

(f) Sigui G un grup. L'acció per conjugació per l'esquerra de(l grup) G en (el conjunt) G és donada per l'assignació $(\sigma, g) \mapsto \sigma \cdot g \cdot \sigma^{-1}$. L'acció per conjugació per la dreta de(l grup) G en (el conjunt) G és donada per l'assignació $(\sigma, g) \mapsto g^\sigma := \sigma^{-1} \cdot g \cdot \sigma$. Notem la definició de g^σ, per a $\sigma, g \in G$.

(g) Sigui G un grup. L'acció per conjugació per l'esquerra de(l grup) G en el conjunt $\mathcal{P}(G)$ de tots els subconjunts de G és donada per l'assignació $(\sigma, H) \mapsto \sigma \cdot H \cdot \sigma^{-1}$. L'acció per conjugació per la dreta de(l grup) G en el conjunt $\mathcal{P}(G)$ de tots els subconjunts de G és donada per l'assignació $(\sigma, H) \mapsto H^\sigma := \sigma^{-1} \cdot H \cdot \sigma$. Notem la definició de H^σ, per a $\sigma \in G$ i $H \subseteq G$, subconjunt.

(h) Sigui G un grup. Podem restringir les accions anteriors per conjugació al conjunt dels subgrups (i no només subconjunts) de G. L'acció per conjugació per l'esquerra de(l grup) G en el conjunt $\mathcal{S}(G)$ de tots els subgrups de G és donada per l'assignació $(\sigma, H) \mapsto \sigma \cdot H \cdot \sigma^{-1}$. L'acció per conjugació per la dreta de(l grup) G en el conjunt $\mathcal{S}(G)$ de tots els subgrups de G és donada per l'assignació $(\sigma, H) \mapsto H^\sigma := \sigma^{-1} \cdot H \cdot \sigma$. Notem la definició de H^σ, per a $\sigma \in G$ i $H \subseteq G$, subgrup.

(i) Siguin K un cos i E un K-espai vectorial. Llavors, la restricció a K^* de l'acció de K en E donada pel producte per escalars, $(\lambda, x) \mapsto \lambda \cdot x$, és una acció (bilateral, perquè el grup és commutatiu) del grup multiplicatiu K^* de K en el conjunt E.

3.1.6. Donada una acció per l'esquerra d'un grup G en un conjunt X, $G \times X \longrightarrow X$, podem considerar una aplicació $\varphi : G \longrightarrow \mathrm{Bij}(X)$, de G en el conjunt de les aplicacions bijectives del conjunt X en si mateix, definida per $g \mapsto \varphi_g$, on $\varphi_g : X \longrightarrow X$ és l'aplicació definida per l'assignació $x \mapsto g \cdot x$. Llavors, φ és un morfisme de grups. I recíprocament, donat un morfisme de grups $\varphi : G \longrightarrow \mathrm{Bij}(X)$, podem definir una acció per l'esquerra de G en X per l'assignació $(g, x) \mapsto \varphi(g)(x)$. Així, és equivalent considerar accions per l'esquerra del grup G en el conjunt X o bé considerar morfismes del grup G en el grup $\mathrm{Bij}(X)$.

Observació 3.1.7. Notem que, per a una acció per la dreta, l'assignació equivalent $g \mapsto \psi_g$, on $\psi_g(x) := x^g$, no és pas un morfisme de grups de G en $\mathrm{Bij}(X)$. En aquest cas, l'assignació que proporciona un morfisme de grups és l'assignació donada per $g \mapsto \psi_g$, on $\psi_g(x) := x^{g^{-1}}$, per a tot $x \in X$. De nou això fa equivalent considerar accions per la dreta de G en X o bé morfismes de grups de G en $\mathrm{Bij}(X)$.

Corol·lari 3.1.8. *Siguin G un grup i X un conjunt. Donar una acció per l'esquerra de G en X, $(g, x) \mapsto g \cdot x$, és equivalent a donar l'acció per la dreta, $(g, x) \mapsto x^g := g^{-1} \cdot x$, de G en X.* □

D'acord amb la definició general de morfisme per a accions d'un conjunt (cf. **1.9.2**), podem definir el concepte de morfisme per a accions d'un grup G; o sigui, de morfisme de G-conjunts per l'esquerra, i també de morfisme de G-conjunts per la dreta.

Definició 3.1.9. Siguin G un grup, X, Y conjunts, i $\rho_X : G \times X \longrightarrow X$ i $\rho_Y : G \times Y \longrightarrow Y$ accions per l'esquerra del grup G en els conjunts X, Y. Un morfisme d'accions, o morfisme de G-conjunts, o aplicació equivariant, o aplicació G-equivariant, de ρ_X en ρ_Y, és una aplicació $\varphi : X \longrightarrow Y$ tal que per a tot $g \in G$ i tot $x \in X$ és $\varphi(g \cdot x) = g \cdot \varphi(x)$; és a dir, $\varphi\big(\rho_X(g, x)\big) = \rho_Y\big(g, \varphi(x)\big)$. Si les dues accions del grup G ho són per la dreta, enlloc de per l'esquerra, obtenim el concepte de morfisme d'accions per la dreta del grup G; la propietat és la mateixa: que $\varphi\big(\rho_X(g, x)\big) = \rho_Y\big(g, \varphi(x)\big)$; o sigui, que $\varphi(x^g) = \big(\varphi(x)\big)^g$.

La definició s'expressa, en tots dos casos, per la commutativitat del diagrama següent.

$$\begin{array}{ccc} G \times X & \xrightarrow{\rho_X} & X \\ {\scriptstyle \mathrm{id}\times\varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ G \times Y & \xrightarrow[\rho_Y]{} & Y \end{array}$$

Diagrama 3.1: Morfisme d'accions d'un grup en un conjunt

Notem que les accions són sempre pel mateix costat; així, si es vol considerar un morfisme d'una acció per l'esquera en una per la dreta, o recíprocament, cal canviar una de les accions de costat via l'aplicació $g \mapsto g^{-1}$ de G en G, com en **3.1.8**.

La demostració de les propietats següents és immediata a partir de les definicions i es deixa com a exercici.

Proposició 3.1.10. *Se satisfan les propietats següents.*

(a) *La identitat és un morfisme d'accions de G.*

(b) *La composició de morfismes d'accions per l'esquerra de G és un morfisme d'accions per l'esquerra de G.*

(c) *La composició de morfismes d'accions per la dreta de G és un morfisme d'accions per la dreta de G.*

(d) *Un isomorfisme d'accions de G és un morfisme que admet un morfisme invers.*

(e) *Un morfisme d'accions de G és isomorfisme si, i només si, el morfisme, com a aplicació entre conjunts, és una bijecció.* □

3.2 Índex d'un subgrup. Teorema de Lagrange

Un context molt adequat per a la definició d'índex d'un subgrup d'un grup i per a establir el teorema de Lagrange és el context de les accions per translació d'un grup en el conjunt dels seus elements; ho fem a continuació.

Definició 3.2.1. Siguin G un grup, X un conjunt i $(g,x) \mapsto g\cdot x$ una acció per l'esquerra de G en X. Per a tot element $x \in X$, el conjunt $G\cdot x := \{g\cdot x : g \in G\} \subseteq X$ s'anomena l'òrbita de x, o també la trajectòria de x. Anàlogament, per a una acció per la dreta, $(g,x) \mapsto x^g$, de G en X, l'òrbita d'un element qualsevol $x \in X$ és el conjunt $x^G := \{x^g : g \in G\} \subseteq X$.

Observació 3.2.2. Per a tot element $x \in X$ i tot element $g \in G$, l'òrbita de x coincideix amb la de $g\cdot x$ (la de x^g, si l'acció és per la dreta); d'aquí es dedueix que l'acció de G produeix una partició de X en òrbites:

$$X = \biguplus_{x\in L} G\cdot x \qquad \text{(respectivament, } X = \biguplus_{x\in R} x^G\text{)},$$

on $L \subseteq X$ (respectivament, $R \subseteq X$) és un conjunt de representants de les òrbites (cf. **A.1.4**). Una acció s'anomena transitiva (també es diu que el grup opera transitivament o que el grup actua transitivament) si només hi ha una òrbita.

3.2.3. Siguin G un grup i $H \subseteq G$ un subgrup qualssevol. Podem considerar l'acció per l'esquerra de H en el conjunt G, $H\times G \longrightarrow G$, donada per la multiplicació per l'esquerra $(h,g) \mapsto h\cdot g$. Això produeix una partició de G com a reunió d'òrbites,

$$G = \biguplus_{g\in L_H} H\cdot g,$$

on L_H és un conjunt de representants de les òrbites per l'esquerra.

3.2.4. Anàlogament, podem considerar l'acció per la dreta de H en G, $H\times G \longrightarrow G$, donada per la multiplicació per la dreta $(h,g) \mapsto g\cdot h$, i obtenim una partició de G com a reunió d'òrbites,

$$G = \biguplus_{g\in R_H} g\cdot H,$$

on R_H és un conjunt de representants de les òrbites per la dreta.

Proposició 3.2.5. *Amb les notacions anteriors, se satisfan les propietats següents.*

(a) *Totes les òrbites de les dues accions anteriors són equipotents; és a dir, per a tot $g \in G$ hi ha bijeccions entre els conjunts H, $H \cdot g$, i $g \cdot H$.*

(b) *Hi ha una bijecció entre els conjunts L_H i R_H.*

(c) *Hi ha bijeccions entre els conjunts G, $L_H \times H$, i $R_H \times H$.*

Demostració:

(a) Per a cada element $g \in G$, les aplicacions $H \longrightarrow H \cdot g$ i $H \longrightarrow g \cdot H$ donades, respectivament, per $h \mapsto h \cdot g$ i per $h \mapsto g \cdot h$ són bijectives.

(b) Sigui L_H un conjunt qualsevol de representants de les òrbites $H \cdot g$, $g \in G$; aleshores, el conjunt $R'_H := \{g \in G : g^{-1} \in L_H\}$ és un conjunt de representants de les òrbites $g \cdot H$, $g \in G$. En efecte, l'aplicació $G \longrightarrow G$ donada per $g \mapsto g^{-1}$ és bijectiva i coincideix amb la seva pròpia inversa; per tant, la partició $G = \biguplus_{g \in L_H} H \cdot g$ dóna lloc a la partició $G = \biguplus_{g \in L_H} (H \cdot g)^{-1} = \biguplus_{g \in L_H} g^{-1} \cdot H$. Com a conseqüència, el conjunt $R'_H = \{g^{-1} : g \in L_H\}$ és un conjunt de representants de les òrbites $g \cdot H$ i l'aplicació $g \mapsto g^{-1}$ proporciona una bijecció entre L_H i R'_H. Finalment, com que tots els conjunts de representants de les òrbites $g \cdot H$ són equipotents, R'_H i R_H són equipotents i, per composició, L_H i R_H són equipotents.

(c) L'aplicació $L_H \times H \longrightarrow G$ donada per la multiplicació, $(g, h) \mapsto h \cdot g$, és bijectiva, perquè $G = \biguplus_{g \in L_H} H \cdot g$; l'exhaustivitat és pel fet que G és reunió d'òrbites, i la injectivitat, perquè la reunió és disjunta. Anàlogament, la multiplicació $(g, h) \mapsto g \cdot h$ proporciona una bijecció $R_H \times H \longrightarrow G$. □

Observació 3.2.6. Siguin G un grup i $H \subseteq G$ un subgrup. La partició de G en classes per l'esquerra mòdul H, $G = \biguplus_{g \in L_H} H \cdot g$ es correspon amb la relació d'equivalència $g \equiv_L g' \pmod{H}$ si, i només si, $g' \cdot g^{-1} \in H$. I anàlogament, la partició $G = \biguplus_{g \in R_H} g \cdot H$ es correspon amb la relació d'equivalència $g \equiv_R g' \pmod{H}$ si, i només si, $g^{-1} \cdot g' \in H$.

Sovint es fan servir aquestes relacions d'equivalència per a la definició de l'índex d'un subgrup d'un grup; això evita parlar prèviament d'accions de grups en conjunts, però llavors cal provar els resultats equivalents dues vegades: per a les relacions d'equivalència, i per a les òrbites.

Definició 3.2.7. Siguin G un grup i $H \subseteq G$ un subgrup qualssevol.

• Les classes de G mòdul H per l'esquerra són les òrbites $H \cdot g$, per a $g \in G$. El conjunt de classes per l'esquerra es representa per $H\backslash G$.

• Les classes de G mòdul H per la dreta són les òrbites $g \cdot H$, per a $g \in G$. El conjunt de classes per la dreta es representa per G/H.

• L'índex de H en G és el cardinal de qualsevol conjunt de representants de les classes per l'esquerra (o per la dreta, ja que tenen el mateix cardinal). L'índex de H en G es denota per $[G : H]$ o, algunes vegades, per $(G : H)$.

• L'ordre de G és el cardinal del conjunt G. De manera equivalent, com que si $H = \{1\}$, llavors $L_H = R_H = G$, tenim que l'ordre de G coincideix amb l'índex de $\{1\}$ en G. L'ordre de G es denota per $\#G$, encara que també es fa servir la notació $|G|$. Un grup finit és un grup d'ordre finit.

Corol·lari 3.2.8 (Teorema de Lagrange)**.** *Siguin G un grup i H un subgrup. Llavors, se satisfà la igualtat entre cardinals $\#G = [G : H] \cdot \#H$.*

Demostració: Acabem de veure que hi ha una bijecció entre G i el producte cartesià de conjunts $L_H \times H$; per tant, hem obtingut la igualtat de cardinals desitjada. □

Observació 3.2.9. Notem que també podem escriure el teorema de Lagrange en la forma $[G : \{1\}] = [G : H] \cdot [H : \{1\}]$. Més generalment, es té el resultat següent.

Exercici 3.2.10. Siguin G un grup i $K \subseteq H \subseteq G$ subgrups. Llavors, se satisfà la fórmula de multiplicativitat dels índexs, $[G : K] = [G : H] \cdot [H : K]$.

Corol·lari 3.2.11. *Si G és un grup finit i $H \subseteq G$ és un subgrup qualsevol, llavors l'ordre de H i l'índex de H en G són finits i divideixen l'ordre de G.* □

Corol·lari 3.2.12. *Si G és un grup finit i $g \in G$ és un element qualsevol, llavors l'ordre de g divideix l'ordre de G.*

Demostració: Si $g \in G$ és d'ordre finit, posem n, el subgrup generat per g és el conjunt $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$, de cardinal n; o sigui, d'ordre n. Apliquem el resultat anterior al subgrup $H := \langle g \rangle$. □

Exercici 3.2.13. Tot grup finit d'ordre un nombre primer és cíclic, i qualsevol element diferent del neutre de G genera G.

3.3 La fórmula d'òrbites

Donada una acció (per l'esquerra) d'un grup G en un conjunt X, podem considerar la partició de X en òrbites $X = \biguplus_{x \in L} G \cdot x$ (cf. l'observació **3.2.2**), on L és un conjunt de representants de les òrbites. Per tant, si X és finit, obtenim que L és finit, totes les òrbites $G \cdot x$ són finites, i $\#X = \sum_{x \in L} \#(G \cdot x)$. En aquesta secció, es tracta d'obtenir una altra descripció d'aquesta fórmula.

Definició 3.3.1. Sigui $(g, x) \mapsto g \cdot x$ una acció per l'esquerra d'un grup G en un conjunt X. Per a tot element $x \in X$, el subconjunt $G_x := \{g \in G : \ g \cdot x = x\}$ és un subgrup de G; s'anomena el grup d'isotropia de x, o també l'estabilitzador de x. També se'l denota com $\mathrm{Stab}(x)$. A fi d'evitar confusions entre l'òrbita $G \cdot x$ i el grup d'isotropia G_x, utilitzarem majoritàriament la notació $\mathrm{Stab}(x)$.

Proposició 3.3.2. *Sigui $(g, x) \mapsto g \cdot x$ una acció per l'esquerra d'un grup G en un conjunt X. Per a tot $x \in X$ i tot $g \in G$, es té que* $\mathrm{Stab}(g \cdot x) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$. *És a dir, els estabilitzadors d'elements de la mateixa òrbita són subgrups conjugats.* □

3.3.3. Siguin G un grup, X un conjunt, i $G \times X \longrightarrow X$ una acció per l'esquerra de G en X. Per a tot element $x \in X$, podem considerar la restricció de l'acció a l'òrbita $G \cdot x$, $G \times (G \cdot x) \longrightarrow (G \cdot x)$. L'aplicació $G \longrightarrow (G \cdot x)$ donada per $g \mapsto g \cdot x$ és exhaustiva (per definició de $G \cdot x$) i dos elements $g, g' \in G$ pertanyen a la mateixa fibra si, i només si, $g^{-1} \cdot g' \in \mathrm{Stab}(x)$; és a dir, cada fibra és una classe lateral $g \cdot \mathrm{Stab}(x)$. Això ens diu que tenim una bijecció entre el conjunt de classes $G/\mathrm{Stab}(x)$ i l'òrbita $G \cdot x$. Per tant, tenim que $\#(G \cdot x) = [G : \mathrm{Stab}(x)]$; és a dir, el cardinal de l'òrbita de x coincideix amb l'índex de l'estabilitzador de x. Per tant, hem obtingut una demostració del teorema següent.

Teorema 3.3.4 (La fórmula d'òrbites)**.** *Siguin G un grup, X un conjunt i $G \times X \longrightarrow X$ una acció per l'esquerra de G en X. Llavors,*

$$\#X = \sum_{x \in L} [G : \mathrm{Stab}(x)],$$

on L és un conjunt de representants de les òrbites. □

3.4 Aplicacions de la fórmula d'òrbites

La fórmula d'òrbites es pot aplicar, en particular, a les accions per conjugació d'un grup en diferents conjunts. En aquesta secció n'estudiem algunes que proporcionen eines molt útils per a l'estudi dels grups; especialment, dels grups finits.

Definició 3.4.1. Sigui G un grup. Si considerem l'acció per conjugació de G en el conjunt $\mathcal{P}(G)$ dels subconjunts de G, resulta que, per a tot $S \in \mathcal{P}(G)$, és

$$\mathrm{Stab}(S) = N_G(S) := \{g \in G : \ g \cdot S \cdot g^{-1} = S\}.$$

Per tant, $N_G(S)$ és un subgrup de G; s'anomena el normalitzador de S. L'òrbita d'un subconjunt $S \subseteq G$ s'anomena la classe de conjugació de S.

Corol·lari 3.4.2. *Siguin G un grup i $H \subseteq G$ un subgrup. Llavors, el cardinal de la classe de conjugació de H és l'índex $[G : N_G(H)]$. És a dir, el nombre de subgrups de G conjugats de H és donat per l'índex $[G : N_G(H)]$.* □

Observació 3.4.3. Notem que un conjugat d'un subgrup és un subgrup, de manera que és el mateix parlar de la classe de conjugació d'un subgrup per a l'acció en el conjunt dels subgrups de G que per a l'acció en el conjunt de tots els subconjunts de G.

Definició 3.4.4. Anàlogament, si considerem l'acció per conjugació d'un grup G en el conjunt G dels seus elements, tenim que per a tot $g \in G$ és

$$\mathrm{Stab}(g) = Z_G(g) := \{h \in G : \ h \cdot g \cdot h^{-1} = g\}.$$

Per tant, $Z_G(g)$ és un subgrup de G; s'anomena el centralitzador de g. Notem que coincideix amb el normalitzador del subconjunt $\{g\}$.

Corol·lari 3.4.5. *Siguin G un grup i $g \in G$ un element. Llavors, el cardinal de la classe de conjugació de g és l'índex $[G : Z_G(g)]$.* □

Definició 3.4.6. Siguin G un grup i $S \subseteq G$ un subconjunt qualsevol. S'anomena centralitzador de S el subgrup $Z_G(S) := \bigcap_{g \in S} Z_G(g) = \{h \in G : \text{ per a tot } g \in S \text{ és } h \cdot g \cdot h^{-1} = g\}$.

Observacions 3.4.7. • En particular, tenim que $Z(G) := Z_G(G)$ és un subgrup normal de G; s'anomena el centre de G. Notem que $Z(G)$ és un subgrup commutatiu de G, i que $Z(G) = G$ si, i només si, G és commutatiu.

• D'altra banda, si $H \subseteq G$ és un subgrup qualsevol, llavors H és un subgrup normal de $N_G(H)$.

Corol·lari 3.4.8 (Fórmula de les classes)**.** *Sigui G un grup. Llavors, se satisfà la igualtat*

$$\#G = \sum_{g \in L} [G : Z_G(g)],$$

on L és un conjunt de representants de les classes de conjugació d'elements de G. □

Exercici 3.4.9. Sigui G un grup.

(a) Si $K \subseteq H \subseteq G$ són subgrups tals que K és normal en H, llavors $H \subseteq N_G(K)$.

(b) Si $K \subseteq G$ és un subgrup qualsevol, llavors $N_G(K)$ és el més gran dels subgrups $H \subseteq G$ tals que $K \subseteq H$ i K és normal en H.

(c) Si $K \subseteq G$ és un subgrup qualsevol i $H \subseteq N_G(K)$, llavors $K \cdot H$ és un subgrup de G i K és normal en $K \cdot H$.

La fórmula de les òrbites i, en conseqüència, la fórmula de les classes admeten una formulació que té en compte els punts fixos.

Definició 3.4.10. Siguin G un grup, X un conjunt, i $G \times X \longrightarrow X$ una acció de G en X. Un element $x \in X$ s'anomena un punt fix per a l'acció si, i només si, $Stab(x) = G$; és a dir, si per a tot $g \in G$ és $g \cdot x = x$.

Corol·lari 3.4.11. *Siguin G un grup, X un conjunt i $G \times X \longrightarrow X$ una acció per l'esquerra de G en X. Llavors,*

$$\#X = \#X_0 + \sum_{x \in L'} [G : \mathrm{Stab}(x)],$$

on X_0 és el conjunt dels punts fixos per a l'acció i L' és un conjunt de representants de les òrbites amb més d'un element. □

Corol·lari 3.4.12. *Sigui G un grup. Llavors, se satisfà la igualtat*

$$\#G = \#Z(G) + \sum_{g \in L'} [G : Z_G(g)],$$

on $Z(G)$ és el centre de G i L' és un conjunt de representants de les classes de conjugació d'elements de G que contenen més d'un element. □

Aquestes fórmules tenen una rellevància especial si el conjunt X és finit; o si el grup G és finit. I encara més si el grup és un p-grup.

Definició 3.4.13. Siguin G un grup finit i p un nombre (natural) primer. Es diu que G és un p-grup si l'ordre de G és una potència de p; és a dir, si existeix un nombre natural $r \geq 0$ tal que $\#G = p^r$. En particular, el grup trivial és un p-grup per a tot nombre primer p, perquè $\#G = p^0$. I, pel teorema de Lagrange (cf. **3.2.8**), tot subgrup d'un p-grup és un p-grup.

Corol·lari 3.4.14 (Congruencia dels punts fixos)**.** *Siguin p un nombre primer i G un p-grup no trivial. Si G actua sobre un conjunt finit, X, llavors, per al conjunt de punts fixos de l'acció, X_0, se satisfà la congruència*

$$\#X_0 \equiv \#X \pmod{p}.$$

En particular, si $\#X$ no és múltiple de p, llavors hi ha algun punt fix.

Demostració: Com que G és un p-grup, per a tot subgrup propi $H \subsetneq G$ es té que p divideix l'índex $[G : H]$. Per tant, si $x \in X$ però $x \notin X_0$, llavors $\mathrm{Stab}(x) \subseteq G$ és un subgrup de G diferent del total; per tant, $[G : \mathrm{Stab}(x)] \equiv 0 \pmod{p}$ i, en conseqüència,

$$\#X = \#X_0 + \sum_{x \in L'} [G : \mathrm{Stab}(x)] \equiv \#X_0 \pmod{p}.$$

Notem que si $\#X$ no és múltiple de p, tampoc no ho és $\#X_0$, de manera que $\#X_0 \neq 0$. □

Corol·lari 3.4.15. *Siguin p un nombre primer i G un p-grup no trivial. Llavors, el centre de G no és trivial; és a dir, $Z(G) \neq \{1\}$.* □

Corol·lari 3.4.16. *Siguin p un nombre primer, G un grup finit, i $H \subseteq G$ un p-subgrup de G; és a dir, un subgrup de G que és un p-grup. Llavors,*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Demostració: Considerem el conjunt de classes G/H i l'aplicació de $H \times G/H \longrightarrow G/H$ donada per translació per l'esquerra: $(h, g \cdot H) \mapsto (h \cdot g) \cdot H$, per a tot $g \in G$. Aquesta aplicació és una acció per l'esquerra, i podem descriure el conjunt de punts fixos de la manera següent: donada una classe $g \cdot H$, $g \in G$, la classe és fixa per l'acció de H si, i només si, per a tot element $h \in H$ és $h \cdot g \cdot H = g \cdot H$; o sigui, si, i només si, $g^{-1} \cdot h \cdot g \in H$; és a dir, si, i només si, $g \in N_G(H)$. Per tant, la classe $g \cdot H$ és fixa si, i només si, $g \in N_G(H)$, de manera que el subconjunt de punts fixos per l'acció és el conjunt de classes $N_G(H)/H$. Com que $\#(G/H) = [G : H]$ i $\#(N_G(H)/H) = [N_G(H) : H]$, el corol·lari **3.4.14** proporciona la congruència volguda. □

3.5 Grups simètrics

Tot i que ja han aparegut en alguna ocasió, ara és un bon moment per a tractar els grups de permutacions amb més profunditat.

Definició 3.5.1. Si X és un conjunt qualsevol, una aplicació bijectiva de X en X també s'anomena una permutació de X. En particular, el conjunt de les aplicacions bijectives de X en X, $\mathrm{Bij}(X)$, és un grup amb la composició d'aplicacions i l'aplicació identitat de X com a element neutre; se'l sol anomenar el grup de les permutacions de X, o bé el grup simètric sobre X; si no hi ha risc de confusió, el denotarem per S_X.

Observació 3.5.2. Siguin X, Y conjunts del mateix cardinal i $\varphi : X \longrightarrow Y$ una aplicació bijectiva. Llavors, l'assignació $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ defineix un isomorfisme $S_X \longrightarrow S_Y$. En particular, per a tot conjunt finit X de cardinal n, el grup S_X s'identifica amb el grup de les permutacions del conjunt $\{0, 1, \ldots, n-1\}$.

Observació 3.5.3. Tot i que podem pensar n com $n = \{0, 1, \ldots, n-1\}$, i, per tant, la notació natural per al grup de les permutacions de n és S_n, de vegades s'escriu S_n per al grup de les permutacions del conjunt $\{1, 2, \ldots, n\}$. Cal estar alerta amb el context.

El fet que l'ordre del grup simètric S_n sigui $n!$ pot fer pensar que "el grup S_n és molt gran". Aquesta frase es pot interpretar de manera més precisa.

Proposició 3.5.4 (Teorema de Cayley)**.** *Siguin G un grup finit i n el seu ordre. Llavors, existeix un morfisme injectiu de grups $\varphi : G \longrightarrow S_n$. Per tant, S_n conté una còpia isomorfa de qualsevol grup d'ordre n.*

Demostració: Considerem l'acció per translació de G en G; cada element $g \in G$ produeix una permutació $h \mapsto g \cdot h$ del conjunt G; és a dir, un element $\sigma_g \in S_G$, que identifiquem amb S_n. Les propietats d'acció ens permeten dir, d'una banda, que aquesta aplicació $\sigma : G \longrightarrow S_n$, $g \mapsto \sigma_g$, és un morfisme de grups; i de l'altra, que σ_g només pot ser la identitat si $g = 1 \in G$; és a dir, σ és un morfisme injectiu de G en S_n. □

Proposició 3.5.5. *Siguin G un grup finit i n el seu ordre. Llavors, existeix un morfisme injectiu de grups $\mathrm{Aut}(G) \longrightarrow S_{n-1}$. Així, el grup simètric S_{n-1} conté una còpia isomorfa del grup d'automorfismes de qualsevol grup d'ordre n.*

Demostració: Efectivament, poden identificar $\mathrm{Aut}(G)$ amb un subgrup del grup de les permutacions dels elements del conjunt $G' := G - \{1\}$, que és de cardinal $n-1$. En efecte, si $\sigma \in \mathrm{Aut}(G)$, llavors $\sigma(1) = 1$, de manera que l'aplicació bijectiva σ restringeix a una bijecció de G'. I és clar que la composició restringeix a la composició, de manera que obtenim un morfisme de grups, i que si la restricció de σ a G' és la identitat, com que $\sigma(1) = 1$, també σ és la identitat; és a dir, que el morfisme és injectiu. □

3.5.6. Donada una permutació $\sigma \in S_n$, $n \geq 1$, en alguns contextos s'acostuma a escriure σ com la matriu de dues files

$$\begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ \sigma(0) & \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) \end{pmatrix},$$

o també, si, com a conjunts, és $\{a_0, a_1, \ldots, a_{n-1}\} = \{0, 1, \ldots, n-1\}$, com la matriu de dues files

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ \sigma(a_0) & \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_{n-1}) \end{pmatrix};$$

és a dir, amb els elements $\{0, 1, \ldots, n-1\}$ escrits en qualsevol ordre a la primera fila i les seves imatges corresponents a la segona fila.

Definició 3.5.7. En general, donat un subconjunt $\{a_1, \ldots, a_m\} \subseteq \{0, 1, \ldots, n-1\}$ de cardinal m, la permutació σ donada per $\sigma(a_i) := a_{i+1}$, per a $1 \leq i \leq m-1$, $\sigma(a_m) := a_1$, i $\sigma(k) := k$, si $k \neq a_i$, per a tot a_i, s'anomena un cicle de longitud m o, també, un m-cicle, i es denota habitualment per $(a_1, a_2, \ldots, a_m)$. Els 2-cicles s'anomenen transposicions.

3.5.8. Notem que per a tot r, $1 \leq r \leq m-1$, és $(a_1, \ldots, a_m) = (a_{r+1}, \ldots, a_m, a_1, \ldots, a_r)$, que $(a_1, \ldots, a_m)^{-1} = (a_m, a_{m-1}, \ldots, a_2, a_1)$, i que $(a_1, \ldots, a_m)$ és un element d'ordre m del grup S_n. Per a $n = 2$ i per a $n = 3$, és cert que tota permutació d'ordre m de S_n és un m-cicle, per a tots els valors possibles de m. Però per a $n \geq 4$, no és cert que tot element de S_n d'ordre m sigui un m-cicle per a tot m possible; per exemple, per a $n \geq 4$, la permutació $(0,1) \circ (2,3)$ és d'ordre $m = 2$ però no és una transposició (2-cicle). I per a $n \geq 5$, l'element $(0,1) \circ (2,3,4)$ és d'ordre 6, però no és un 6-cicle; en particular, pot ser que per a alguns valors de n, S_n contingui elements d'ordre $> n$.

3.5.9. S'ha comentat més amunt que l'ordre del grup simètric és donat per $\#S_n = n!$; en particular, S_0 i S_1 són (isomorfs a) el grup trivial, d'un sol element. Això fa que sovint s'acostumi a treballar amb els grups simètrics S_n per a $n \geq 2$. Fins i tot, com que S_2 és un grup de dos elements, i, per tant, cíclic d'ordre 2, en parlar de grups simètrics sovint es restringeix l'atenció als grups simètrics S_n per a $n \geq 3$.

3.5.10. Per a $n \geq 3$, el grup S_n no és commutatiu. En efecte, s'hi satisfà que

$$(0,1) \circ (1,2) = (0,1,2) \neq (0,2,1) = (1,2) \circ (0,1).$$

Proposició 3.5.11. *En el grup simètric S_n se satisfan les propietats següents.*

(a) (Dos cicles disjunts commuten.) *Si $(a_1, \ldots, a_r)$, $(b_1, \ldots, b_s) \in S_n$ són cicles de longituds r, s, respectivament, i se satisfà que $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \varnothing$, és a dir, els dos cicles són disjunts, llavors $(a_1, \ldots, a_r) \circ (b_1, \ldots, b_s) = (b_1, \ldots, b_s) \circ (a_1, \ldots, a_r)$.*

(b) *Tota permutació és producte de cicles disjunts dos a dos.*

(c) *Si $a_1, \ldots, a_k \in \{0, 1, \ldots, n-1\}$ són diferents dos a dos, llavors*

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2) \circ (a_2, a_3) \circ \cdots \circ (a_{k-1}, a_k);$$

en conseqüencia, tot cicle és producte de transposicions.

(d) *I, en conseqüència, tota permutació és producte de transposicions.* □

Exercici 3.5.12 (Càlcul de les classes de conjugació del grup simètric S_n)**.**

(a) Siguin $n \geq 2$, $\sigma \in S_n$ una permutació, i $(a_1, \cdots, a_r) \in S_n$ un cicle, qualssevol. Llavors,

$$\sigma \circ (a_1, \cdots, a_r) \circ \sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_r)).$$

(b) Donats dos cicles de la mateixa longitud, σ_1, $\sigma_2 \in S_n$, existeix una permutació $\sigma \in S_n$ tal que $\sigma \circ \sigma_1 \circ \sigma^{-1} = \sigma_2$.

(c) Siguin $\sigma_1, \ldots, \sigma_k \in S_n$ cicles disjunts dos a dos, i també $\tau_1, \ldots, \tau_k \in S_n$, cicles disjunts dos a dos. Posem $\sigma := \sigma_1 \circ \cdots \circ \sigma_k$ i $\tau := \tau_1 \circ \cdots \circ \tau_k$. Si, per a $1 \leq i \leq k$, la longitud del cicle σ_i coincideix amb la del cicle τ_i, aleshores existeix una permutació $\rho \in S_n$ tal que $\rho \circ \sigma \circ \rho^{-1} = \tau$.

Corol·lari 3.5.13. *Sigui $n \geq 2$. Hi na una correspondència bijectiva entre el conjunt de les classes de conjugació d'elements del grup S_n i el conjunt de les particions de n. És a dir, el nombre de classes de conjugació d'elements del grup S_n és el nombre de particions de n.*

Recordem que s'anomena partició d'un nombre natural $n \neq 0$ una successió de nombres naturals no nuls $m_1 \geq m_2 \geq \cdots \geq m_r$ tal que $n = m_1 + \cdots + m_r$. Per exemple, les particions de 5 són:

$$(5), \quad (4,1), \quad (3,2), \quad (3,1,1), \quad (2,2,1), \quad (2,1,1,1), \quad (1,1,1,1,1).$$

Demostració: Donada una permutació qualsevol $\sigma \in S_n$, considerem-ne una descomposició com a producte de cicles disjunts, ordenats per longituds decreixents, i completem-la amb els cicles de longitud 1 que manquen a fi que la suma de les longituds sigui exactament n. D'aquesta manera, les longituds dels cicles determinen una partició de n.

I, en virtut de l'exercici anterior, dues permutacions determinen la mateixa partició si, i només si, són elements conjugats de S_n; és a dir, si, i només si, pertanyen a la mateixa classe de conjugació. □

3.5.14. Si $m \leq n$, podem considerar un morfisme injectiu de grups $S_m \longrightarrow S_n$ donat per la identificació d'una permutació de $\{0, 1, \ldots, m-1\}$ com la permutació de $\{0, 1, \ldots, n-1\}$ que té el mateix efecte en els elements $0, 1, \ldots, m-1$ i deixa fixos els $m, \ldots, n-1$. Per tant, podem pensar S_m com el subgrup de S_n de les permutacions que deixen fixos els elements $m, \ldots, n-1$. Proposem com a exercici demostrar el resultat següent, més general.

Proposició 3.5.15. *Considerem qualsevol subconjunt $X \subseteq \{0, 1, \ldots, n-1\}$ de m elements, el seu complementari, Y, i una bijecció qualsevol $\sigma : X \longrightarrow \{0, 1, \ldots, m-1\}$. Podem identificar S_m amb el subgrup de S_n de les permutacions que deixen fixos els elements de Y (és a dir, que restringides a Y són la identitat) de la manera següent. Donada una permutació qualsevol $\tau \in S_m$, sigui $\varphi_\sigma(\tau) : \{0, 1, \ldots, n-1\} \longrightarrow \{0, 1, \ldots, n-1\}$ l'aplicació donada per*

$$\varphi_\sigma(\tau)(k) := \begin{cases} k, & \text{si } k \in Y, \\ (\sigma^{-1} \circ \tau \circ \sigma)(k), & \text{si } k \in X. \end{cases}$$

Llavors, $\varphi_\sigma(\tau) \in S_n$ i l'aplicació $\varphi_\sigma : S_m \longrightarrow S_n$ donada per $\tau \mapsto \varphi_\sigma(\tau)$ és un morfisme injectiu de grups, amb imatge el subgrup de les permutacions de $\{0, 1, \ldots, n-1\}$ que restringides a Y són la identitat. □

Observació 3.5.16. Notem que si estenem σ a una bijecció de tot $\{0, 1, \ldots, n-1\}$, que també anomenarem σ, mitjançant una bijecció qualsevol $\sigma' : Y \longrightarrow \{m, \ldots, n-1\}$, llavors $\varphi_\sigma(S_m) = \sigma^{-1} S_m \sigma \subseteq S_n$; és a dir, els dos subgrups S_m i $\varphi_\sigma(S_m)$ no només són isomorfs, sinó que són conjugats dins S_n.

Observació 3.5.17. No és cert que sots els subgrups de S_n isomorfs a S_m siguin conjugats. Per exemple, per a $n \geq 4$, els subgrups $\{1, (0,1) \circ (2,3)\}$ i $S_2 = \{1, (0,1)\}$ són isomorfs, però no són conjugats (cf. **3.5.8**).

En l'exercici següent posem de manifest alguns conjunts de generadors per al grup simètric S_n. En particular, veiem que S_n es pot generar amb només dos elements. I, per a acabar la secció, plantegem com a exercici la prova que el centre dels grups simètrics S_n, $n \geq 3$, és trivial.

Exercici 3.5.18. Per a tot $n \geq 2$, el grup simètric S_n admet els conjunts següents de generadors.

(a) $\{(0,1), (0,2), \cdots, (0,n-1)\}$.

(b) $\{(0,1), (1,2), \cdots, (n-2,n-1)\}$.

(c) $\{(0,1,\cdots,n-1), (0,1)\}$.

Exercici 3.5.19. Per a $n \geq 3$, el centre de S_n és el subgrup trivial.

3.6 Grups alternats

Així com la família $\{S_n\}_{n\geq 1}$, dels grups simètrics, és important, també ho és la dels grups alternats, $\{A_n\}_{n\geq 2}$, que són subgrups dels grups simètrics. Dediquem aquesta secció a un primer estudi dels grups alternats, que continuarem a la secció **4.6**.

Lema 3.6.1. *Si $a, b, c \in \{0, 1, \ldots, n-1\}$ són diferents dos a dos, llavors $n \geq 3$ i en el grup simètric S_n se satisfà que $(a,b) \circ (b,c) = (a,c) \circ (a,b)$.* □

D'aquesta propietat i del fet que dues transposicions disjuntes commuten es dedueix immediatament el resultat següent.

Corol·lari 3.6.2. *Siguin $n \geq 2$ i $a, b \in \{0, 1, \ldots, n-1\}$, diferents. Donades transposicions $\tau_1, \ldots, \tau_k \in S_n$, existeixen transposicions $\tau'_1, \ldots, \tau'_k \in S_n$ tals que*

$$(a,b) \circ \tau_1 \circ \cdots \circ \tau_k = \tau'_1 \circ \cdots \circ \tau'_k \circ (a,b).$$ □

Proposició 3.6.3. *Sigui $n \geq 2$, L'element neutre de S_n no és producte d'una quantitat senar de transposicions.*

Demostració: El resultat és obvi per a S_2. Suposem, doncs, que $n \geq 3$. Ara, és clar que la permutació identitat no és una transposició en S_n; és a dir, que no és el producte d'una sola transposició. Per inducció, sigui $r \geq 1$ un nombre natural, suposem que la identitat no és producte de $2s+1$ transposicions, per a $0 \leq s < r$, i veiem que no és producte de $2r+1$ transposicions. Per reducció a l'absurd, suposem que la identitat és un producte de $2r+1$ transposicions, posem $\tau_1, \ldots, \tau_{2r+1} \in S_n$, $\mathrm{id} = \tau_1 \circ \cdots \circ \tau_{2r} \circ \tau_{2r+1}$; hem d'obtenir una contradicció.

Escrivim $\tau_{2r+1} = (a, x_{2r+1})$, amb $x_{2r+1} \neq a$. En alguna de les transposicions $\tau_1, \ldots, \tau_{2r}$ ha d'aparèixer a, perquè, en cas contrari, x_{2r+1} no seria fix pel producte $\tau_1 \circ \cdots \circ \tau_{2r} \circ \tau_{2r+1}$ i aquest producte no seria la identitat. Alguna de les transposicions $\tau_1, \ldots, \tau_{2r}$ és, doncs, de la forma (a, x_{2r}), amb $x_{2r} \neq a$. En virtut del corol·lari anterior, i canviant si convé algunes de les transposicions τ_i per altres transposicions però sense variar-ne la quantitat, podem suposar que $\tau_{2r} = (a, x_{2r})$. I si fos $x_{2r} = x_{2r+1}$, podríem simplificar les dues transposicions, de manera que la identitat seria producte de $2r-1 = 2(r-1)+1$ transposicions, fet contrari a la hipòtesi d'inducció. Per tant, $x_{2r} \neq x_{2r+1}$. De nou, com que x_{2r} és fix per la identitat, però el producte $(a, x_{2r}) \circ (a, x_{2r+1})$ transforma x_{2r} en a, hi ha d'haver alguna transposició de les (noves) $\tau_1, \ldots, \tau_{2r-1}$ que sigui de la forma (a, x_{2r-1}), amb $x_{2r-1} \neq a$. I de nou la podem dur cap a la dreta, al costat de qualsevol de les $(a, x_{2r}) \circ (a, x_{2r+1})$. Si

x_{2r-1} coincidís amb x_{2r} o amb x_{2r+1}, podríem simplificar una parella de transposicions, contràriament a la hipòtesi d'inducció. Per tant, els tres elements x_{2r-1}, x_{2r}, i x_{2r+1} són diferents dos a dos. I podem procedir per inducció, fins a expressar la identitat en la forma $(a, x_1) \circ (a, x_2) \circ \cdots \circ (a, x_{2r}) \circ (a, x_{2r+1})$, amb els elements $x_1, \ldots, x_{2r+1}$ diferents dos a dos i diferents de a. Però això és, de nou, contradictori, perquè x_1 no seria fix per la identitat. □

Corol·lari 3.6.4. *Sigui S_n, $n \geq 2$, el grup simètric. Donada una permutació qualsevol $\sigma \in S_n$, la paritat del nombre de transposicions en què σ pot descompondre com a producte està ben definida; és a dir, si $\tau_1, \ldots, \tau_r, \tau'_1, \ldots, \tau'_s \in S_n$ són transposicions tals que $\sigma = \tau_1 \circ \cdots \circ \tau_r = \tau'_1 \circ \cdots \circ \tau'_s$, llavors $r \equiv s \pmod 2$.*

Demostració: En efecte, com que tota transposició coincideix amb la seva permutació inversa, podem escriure $\sigma^{-1} = \tau'_s \circ \cdots \circ \tau'_1$, de manera que $\mathrm{id} = \tau_1 \circ \cdots \circ \tau_r \circ \tau'_s \circ \cdots \circ \tau'_1$ és producte de $r + s$ transposicions i, per tant, $r + s$ és parell. □

Definició 3.6.5. Considerem el grup simètric S_n amb $n \geq 2$. Donada una permutació $\sigma \in S_n$, anomenarem signe de σ o, també, signatura de σ, i escriurem $\mathrm{sig}(\sigma)$, el nombre $(-1)^r \in \mathbb{Z}$, on r és la paritat del nombre de transposicions en què σ pot descompondre com a producte. Direm que una permutació σ és parella si $\mathrm{sig}(\sigma) = 1$, i que és senar si $\mathrm{sig}(\sigma) = -1$. L'aplicació $\mathrm{sig} : S_n \longrightarrow \{\pm 1\}$ definida per $\sigma \mapsto \mathrm{sig}(\sigma)$ és un morfisme exhaustiu de grups; el seu nucli $A_n := \ker \mathrm{sig} \subseteq S_n$ s'anomena el n-èsim grup alternat. Per definició, $A_n \subseteq S_n$ és un subgrup normal; i és d'índex 2.

Observació 3.6.6. Per a $n = 1$, tenim que $S_n = \{1\}$, de manera que també podem definir $A_1 = \{1\}$ i també és el subgrup normal format per les permutacions parelles, perquè totes ho són (no hi ha transposicions). Només en aquest cas l'índex no és 2.

Exercici 3.6.7. Per a tot $n \geq 3$, el grup alternat A_n admet els conjunts següents de generadors.

(a) El conjunt de tots els 3-cicles, $\{(a, b, c) : a, b, c \in \{0, 1, \ldots, n-1\}, \#\{a, b, c\} = 3\}$.

(b) El conjunt dels 3-cicles de la forma $(0, a, b)$, amb $1 \leq a < b \leq n - 1$.

(c) El conjunt dels 3-cicles de la forma $(0, 1, k)$, amb $2 \leq k \leq n - 1$.

3.6.8. Notem que en el grup alternat A_3 només hi ha dos 3-cicles, que no són conjugats, perquè A_3 és commutatiu. D'altra banda, per a $n = 4$, A_4 conté vuit 3-cicles, que no poden formar una sola classe de conjugació, per exemple, perquè 8 no divideix l'ordre, 12, de A_4, mentre que el nombre de conjugats és l'índex del normalitzador i, per tant, un divisor de l'ordre del grup. Però per a $n \geq 5$, els 3-cicles formen una classe de conjugació. En efecte, se satisfà el resultat següent.

Proposició 3.6.9. *Per a tot $n \geq 5$, el conjunt dels 3-cicles del grup alternat A_n constitueix una classe de conjugació; és a dir, dos 3-cicles de A_n són conjugats per un element de A_n.*

Demostració: Suposem que $a, b, c, d, e, f \in \{0, 1, \ldots, n-1\}$, amb $\#\{a, b, c, d, e, f\} = 6$ (és a dir, que a, b, c, d, e, f són diferents dos a dos); llavors,

$$(a, b) \circ (c, f) \circ (b, e) \circ (a, d) \circ (a, b, c) \circ (a, d) \circ (b, e) \circ (c, f) \circ (a, b) = (d, e, f);$$

per tant, dos 3-cicles disjunts (només n'hi pot haver si $n \geq 6$) són conjugats per un element de A_n. Anàlogament, si $\#\{a,b,c,d,e\} = 5$, llavors

$$(c,e) \circ (b,d) \circ (a,b,c) \circ (b,d) \circ (c,e) = (a,d,e);$$

per tant, dos 3-cicles amb un sol element comú (i només n'hi pot haver si $n \geq 5$) també són conjugats per un element de A_n. Ara (notem que $(b,c) \notin A_n$, però $(b,c) \circ (d,e) \in A_n$),

$$(d,e) \circ (b,c) \circ (a,b,c) \circ (b,c) \circ (d,e) = (a,c,b),$$

de manera que un 3-cicle i el seu invers també són conjugats per un element de A_n. I, finalment (com aans, $(c,d) \notin A_n$, però $(c,d) \circ (e,f) \in A_n$),

$$(e,f) \circ (c,d) \circ (a,b,c) \circ (c,d) \circ (e,f) = (a,b,d),$$

de manera que dos 3-cicles amb exactament dos elements comuns també són conjugats per un element de A_n, perquè (a,d,b) és l'invers de (a,b,d) i, per tant, també és conjugat de (a,b,c) per un element de A_n. □

3.7 Teoremes de Sylow

Una eina molt útil per al treball amb grups finits consisteix en els anomenats teoremes de Sylow. Abans, però, de la seva formulació, comencem amb un resultat previ.

Siguin G un grup, X un conjunt, i $G \times X \longrightarrow X$ una acció per l'esquerra del grup G en el conjunt X. Podem considerar una acció de G en el conjunt de parts de X, $\mathcal{P}(X)$, donada per l'assignació $(g,Y) \mapsto g \cdot Y := \{g \cdot y : y \in Y\}$. En particular, té sentit parlar del subgrup estabilitzador de cada subconjunt $Y \subseteq X$. Se satisfà el resultat següent.

Proposició 3.7.1. *Siguin G un grup, X un conjunt, i $G \times X \longrightarrow X$ una acció per l'esquerra del grup G en el conjunt X. Els subconjunts $Y \subseteq X$ tals que, per a l'acció de G en $\mathcal{P}(X)$, és $G = \mathrm{Stab}(Y)$, són exactament les reunions d'òrbites, per a l'acció de G en X, $Y = \bigcup_{y \in Y} G \cdot y$. És a dir, per a un subconjunt $Y \subseteq X$ és $G \cdot Y = Y$ si, i només si, $Y = \bigcup_{y \in Y} G \cdot y$.*

Demostració: Si $G \cdot Y = Y$, llavors per a tot $y \in Y$ i tot $g \in G$ és $g \cdot y \in Y$; això diu que per a tot $y \in Y$ és $G \cdot y \subseteq Y$, i $Y = \bigcup_{y \in Y} G \cdot y$. Recíprocament, si $Y = \bigcup_{y \in Y} G \cdot y$, llavors $G \cdot Y = \bigcup_{y \in Y} G \cdot G \cdot y = \bigcup_{y \in Y} G \cdot y = Y$. □

Corol·lari 3.7.2. *Sigui G un grup i considerem l'acció de G en $\mathcal{P}(G)$ donada per translació per l'esquerra, $(g,S) \mapsto g \cdot S$. Per a tot subconjunt no buit $S \subseteq G$, $S \neq \varnothing$, l'ordre del subgrup $\mathrm{Stab}(S)$ és un divisor del cardinal de S.*

Demostració: Sigui $H := \mathrm{Stab}(S)$ i considerem l'acció per translació de H en G i, en conseqüencia, l'acció per translació de H en $\mathcal{P}(G)$. Tenim que $H \cdot S = S$, i l'aplicació de

la proposició anterior a aquesta situació ens diu que $S = \bigcup_{s\in S} H\cdot s$. Si prenem un conjunt de representants de les òrbites, aquest conjunt és no buit (perquè $S \neq \varnothing$) i la reunió és disjunta; per tant, el cardinal de S és una suma no nul·la dels cardinals de les òrbites $H\cdot s$, que són tots iguals a l'ordre de H; per tant, $\#H$ divideix $\#S$, com calia veure. □

Definició 3.7.3. Siguin G un grup finit, $n := \#G$, el seu ordre, i p un nombre primer que divideix n. Escrivim n en la forma $n = p^r\cdot m$, amb $r \geq 1$ i $p \nmid m$. Un subgrup $H \subseteq G$ s'anomena un p-subgrup de Sylow de G si $\#H = p^r$; és a dir, si és un p-subgrup de G d'índex no divisible per p. El primer teorema de Sylow afirma l'existència de tals subgrups.

Teorema 3.7.4 (Primer teorema de Sylow)**.** *Siguin G un grup finit i p un nombre primer que divideix $\#G$. Llavors, existeix almenys un p-subgrup de Sylow de G.*

Comencem amb un resultat previ de natura purament aritmètica. Recordem que per a un nombre natural primer p i un nombre enter no nul n, s'anomena valoració p-àdica de n l'exponent de p en la descomposició en factors primers de n.

Lema 3.7.5. *Siguin p un nombre primer i X un conjunt finit de cardinal $p^r\cdot m$, amb $r\geq 1$ i $p\nmid m$. El nombre de subconjunts de X de cardinal p^r és el nombre combinatori $\binom{p^r\cdot m}{p^r}$, i no és divisible per p.*

Demostració: És clar que el nombre de subconjunts de cardinal p^r d'un conjunt de cardinal $p^r\cdot m$ és el nombre combinatori $\binom{p^r\cdot m}{p^r}$, que és un nombre natural que podem escriure, en $\mathbb{Q}$, en la forma

$$\binom{p^r\cdot m}{p^r} = \frac{\prod_{k=0}^{p^r-1}(p^r\cdot m-k)}{\prod_{k=0}^{p^r-1}(p^r-k)} = \prod_{k=0}^{p^r-1}\frac{p^r\cdot m-k}{p^r-k}.$$

Com que $r\geq 1$ i p no divideix m, els únics factors dels productes que són divisibles per p són els factors que corresponen als valors de k múltiples de p; i la valoració p-àdica dels numeradors i els denominadors corresponents és la mateixa, i coincideix amb la valoració p-àdica de k (excepte per a $k=0$, en què les dues valoracions p-àdiques són exactament r). Per tant, la valoració p-àdica del numerador coincideix amb la del denominador; és a dir, el nombre combinatori no és divisible per p. □

Demostració (del primer teorema de Sylow): Escrivim $\#G = p^r\cdot m$, amb $r\geq 1$ i $p\nmid m$, i sigui $\mathcal{S}$ el subconjunt de $\mathcal{P}(G)$ format pels subconjunts de cardinal p^r que, clarament, és no buit perquè $\#G \geq p^r$.

Si fem actuar G en $\mathcal{S}$ per translació per l'esquerra i apliquem la fórmula d'òrbites, obtenim que $\#\mathcal{S} = \sum_{X\in\mathcal{L}} \#(G\cdot X)$, on $\mathcal{L}$ és un conjunt de representants de les òrbites $(G\cdot X)$. Com que, en virtut del lema **3.7.5**, p no divideix $\#\mathcal{S}$, obtenim que hi ha alguna òrbita de cardinal no divisible per p; és a dir, hi ha algun conjunt $X\in\mathcal{S}$ tal que p no

divideix $\#(G \cdot X) = [G : \mathrm{Stab}(X)]$. I com que, en virtut del corol·lari **3.7.2**, $\#\mathrm{Stab}(X)$ divideix $\#X = p^r$, el subgrup $\mathrm{Stab}(X)$ és un p-subgrup de G d'índex no divisible per p; és a dir, $\mathrm{Stab}(X)$ és un p-subgrup de Sylow de G. □

Corol·lari 3.7.6 (Teorema de Cauchy)**.** *Siguin G un grup finit i p un nombre primer que divideix l'ordre de G. Llavors, existeix algun element de G d'ordre p; equivalentment, G conté algun subgrup cíclic d'ordre p.*

Demostració: Podem considerar un p-subgrup de Sylow $S \subseteq G$ i un element $g \in S$, $g \neq 1$. Com que l'ordre de g divideix l'ordre de S, tenim que g és d'ordre p^s, amb $1 \leq s \leq r$; i, aleshores, l'element $g^{p^{s-1}}$ és d'ordre p (cf. **2.8.12**). □

Observació 3.7.7. Hi ha alguna altra demostració habitual del primer teorema de Sylow que utilitza el teorema de Cauchy; òbviament, cal demostrar prèviament i de manera independent aquest teorema.

Teorema 3.7.8 (Segon teorema de Sylow)**.** *Siguin p un nombre primer, G un grup finit, $H \subseteq G$ un subgrup d'ordre divisible per p, i $S \subseteq G$ un p-subgrup de Sylow de G, l'existència del qual és garantida pel primer teorema de Sylow. Llavors, existeix $g \in G$ tal que el subgrup intersecció $H \cap (g \cdot S \cdot g^{-1})$ és un p-subgrup de Sylow de H.*

Demostració: Considerem el conjunt G/S, de les classes laterals $g \cdot S$, $g \in G$. Clarament, l'acció de G en G/S per translació només té una òrbita, i el subgrup $S \subseteq G$ és l'estabilitzador de l'element $S = 1 \cdot S \in G/S$. Per tant, per a tot element $g \cdot S \in G/S$, $g \in G$, l'estabilitzador de $g \cdot S$ és el subgrup conjugat $g \cdot S \cdot g^{-1}$ (cf. **3.3.2**).

Restringim a H l'operació de G en G/S i considerem la descomposició en òrbites de G/S per a aquesta acció de H. Com que S és un p-subgrup de Sylow de G, tenim que $\#(G/S) = [G : S]$ no és divisible per p, de manera que alguna H-òrbita és de cardinal no divisible per p; sigui $g \cdot S \in G/S$, $g \in G$, un representant d'aquesta H-òrbita. Com que l'estabilitzador de l'element $g \cdot S$ per a l'acció de G és $g \cdot S \cdot g^{-1}$, resulta que l'estabilitzador de $g \cdot S$ per a l'acció de H és la intersecció $H \cap (g \cdot S \cdot g^{-1})$, i l'índex $[H : H \cap (g \cdot S \cdot g^{-1})]$ és el cardinal de la H-òrbita de $g \cdot S$, que no és divisible per p. Això implica que el p-grup $H \cap (g \cdot S \cdot g^{-1})$ és un p-subgrup de Sylow de H, l'existència del qual calia veure. □

Corol·lari 3.7.9. *Siguin G un grup finit i p un nombre natural primer.*

(a) *Per a tot p-subgrup $H \subseteq G$ existeix un p-subgrup de Sylow $S \subseteq G$ tal que $H \subseteq S$.*

(b) *Tots els p-subgrups de Sylow de G són conjugats.*

Demostració:

(a) Fixem un p-subgrup de Sylow $S' \subseteq G$ i sigui $H \subseteq G$ un p-subgrup de G. Si $H = \{1\}$, el resultat és clar. Si $H \neq \{1\}$, llavors H és d'ordre divisible per p i podem aplicar el segon teorema de Sylow (**3.7.8**). Existeix $g \in G$ tal que $H \cap g \cdot S' \cdot g^{-1}$ és un p-subgrup de Sylow de H; i com que H és un p-grup, ha de ser $H \cap g \cdot S' \cdot g^{-1} = H$. Això ens diu que $H \subseteq g \cdot S' \cdot g^{-1} =: S$, que és un p-subgrup de Sylow de G.

(b) Ara, donats dos p-subgrups de Sylow S, $S' \subseteq G$, de nou tenim que existeix $g \in G$ tal que $S \cap g \cdot S' \cdot g^{-1} = S$, perquè S és un p-grup. Això diu que $S \subseteq g \cdot S' \cdot g^{-1}$ i, com que tots dos subgrups són p-subgrups de Sylow, que $S = g \cdot S' \cdot g^{-1}$. □

Teorema 3.7.10 (Tercer teorema de Sylow)**.** *Sigui G un grup finit i escrivim el seu ordre en la forma $n := \#G = p^r \cdot m$, on p és un nombre primer, $r \geq 1$, i m és un nombre natural no divisible per p. Llavors, per al nombre de p-subgrups de Sylow de G, posem n_p, se satisfan les propietats següents.*

(a) $n_p = [G : N_G(S)]$, *l'índex del subgrup normalitzador de qualsevol p-subgrup de Sylow $S \subseteq G$.*

(b) n_p *divideix m, que és l'índex $[G : S]$ de qualsevol p-subgrup de Sylow $S \subseteq G$.*

(c) $n_p \equiv 1 \pmod{p}$.

Demostració: Pel segon teorema de Sylow (**3.7.8**), tots els p-subgrups de Sylow de G són conjugats; això és dir que formen una òrbita per a l'acció per conjugació de G en el conjunt dels subgrups de G. I l'estabilitzador d'un qualsevol dels elements de l'òrbita, posem S, és el normalitzador, $N_G(S)$. Només cal tenir en compte que el cardinal de l'òrbita, n_p, és l'índex de l'estabilitzador de qualsevol dels seus elements. Això demostra la primera propietat; i també la segona, perquè $S \subseteq N_G(S)$ i, per tant, $[G : N_G(S)]$ divideix $[G : S] = m$.

Per a veure la congruència $n_p \equiv 1 \pmod{p}$, considerem l'acció per conjugació de S en el conjunt dels p-subgrups de Sylow de G, conjunt que és de cardinal n_p. Per a qualsevol p-subgrup de Sylow $S' \subseteq G$, l'òrbita que determina S' conté només l'element S' si, i només si, $S \subseteq N_G(S')$. Si aquest és el cas, resulta que els subgrups S i S' de $N_G(S')$ en són p-subgrups de Sylow i, per tant, conjugats en $N_G(S')$; però com que $S' \subseteq N_G(S')$ és normal, resulta que $S' = S$. Així, l'única òrbita que només conté un element és l'òrbita de S. El cardinal de qualsevol altra òrbita és divisible per p, perquè l'acció ho és d'un p-grup. La fórmula d'òrbites (**3.3.4**) proporciona la congruència. □

Capítol 4

Grups lliures, diedrals, resolubles, de simetries

L'estudi de la teoria de grups té dues motivacions especialment importants. D'una banda, les representacions lineals dels grups, que permeten tractar-los en forma matricial; de l'altra, l'estudi de les simetries. De fet, la primera vegada que es van introduir els grups de manera abstracta, després que Gauss ho havia fet del grup de classes de formes quadràtiques binàries, va ser com a grups de simetries de les arrels de polinomis, i això va donar lloc als grups que després s'anomenarien grups de Galois de les equacions algebraiques. En aquest capítol introduirem les eines més bàsiques que permeten parlar de manera elemental de grups de simetries.

4.1 Grups lliures

A fi de proporcionar la primera de les eines que ens seran útils per a l'estudi dels grups de simetries, l'exemple següent pot ser il·luminador. Es tracta de recordar el concepte de base d'un espai vectorial i de fer-ne palesa la propietat universal que les caracteritza.

Siguin, doncs, K un cos i E un K-espai vectorial, i suposem que $B \subseteq E$ és una K-base de E. Llavors, per a tot K-espai vectorial F i tota aplicació $f : B \longrightarrow F$, només com a conjunts, existeix una única aplicació K-lineal $\varphi : E \longrightarrow F$, o sigui, morfisme d'espais vectorials, tal que el diagrama següent és commutatiu.

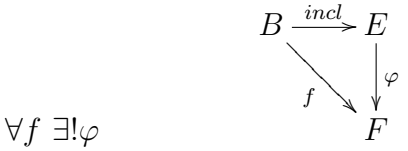


Diagrama 4.1: Propietat universal d'una base d'un espai vectorial

És a dir, per a definir una aplicació K-lineal des d'un espai vectorial qualsevol E, és suficient triar arbitràriament les imatges dels elements d'una base qualsevol de E. Aquesta situació té un paral·lelisme en el context d'altres estrucuctures; en aquest capítol ho veurem en el cas de l'estructura de grups i en el cas de l'estructura de grups abelians;

més endavant (cf. **6.2.8**), ho veurem per a l'estructura de K-àlgebra (associativa, unitària i commutativa).

Definició 4.1.1. Siguin G un grup i B un conjunt qualssevol. Es diu que G és un grup lliure de base B si existeix una aplicació $\psi : B \longrightarrow G$, com a conjunts, tal que per a tot grup H i tota aplicació $f : B \longrightarrow H$, com a conjunts, existeix un únic morfisme de grups $\varphi : G \longrightarrow H$ tal que

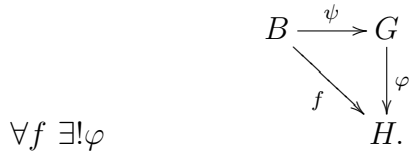


Diagrama 4.2: Definició de grup lliure

Definició 4.1.2. Siguin G un grup abelià i B un conjunt qualssevol. Es diu que G és un grup abelià lliure de base B si existeix una aplicació $\psi : B \longrightarrow G$, com a conjunts, tal que per a tot grup abelià H i tota aplicació $f : B \longrightarrow H$, com a conjunts, existeix un únic morfisme de grups (abelians) $\varphi : G \longrightarrow H$ tal que

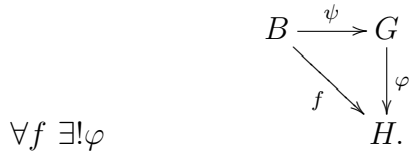


Diagrama 4.3: Definició de grup abelià lliure

Observació 4.1.3. Notem la diferència de les dues definicions, que és importantíssima. En el cas de grup lliure, la propietat universal es predica per a tots els grups H, mentre que en el cas de grup abelià lliure, només es predica per a grups abelians. Però, per contra, en el cas de grups lliures només es demana que l'objecte sigui un grup, mentre que en l'altre cas es demana que el grup sigui abelià; per tant, un grup lliure no té per què ser un grup abelià lliure (caldria que fos abelià); i un grup abelià lliure no té per què ser un grup lliure (hauria de satisfer la propietat universal per a tots els grups, i no només per als abelians).

Exemples 4.1.4. • El grup trivial és un grup lliure, i també un grup abelià lliure, de base el conjunt buit.

• El grup additiu dels nombres enters, $\mathbb{Z}$, és un grup lliure, i també és un grup abelià lliure, de base qualsevol conjunt d'un sol element, conjunt que podem identificar amb $B = \{1\} \subseteq \mathbb{Z}$, si ψ és l'aplicació que envia aquest element a $1 \in \mathbb{Z}$.

• De fet, tot grup cíclic infinit, amb generador g, és un grup lliure, i també un grup abelià lliure, de base $B = \{g\}$ (i l'aplicació d'inclusió del conjunt $\{g\}$ en G).

• El grup abelià additiu $\mathbb{Z}^n$ és un grup abelià lliure de base $B = \{e_0, \ldots, e_{n-1}\}$, on $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, amb 1 en el component i-èsim i 0 en els altres, per a $0 \leq i \leq n-1$. Però, si $n \geq 2$, no és un grup lliure. Per exemple, si en H hi ha dos elements que no commuten, posem h_0, h_1, no hi pot haver cap morfisme de grups de $\varphi : \mathbb{Z}^n \longrightarrow H$ tal que

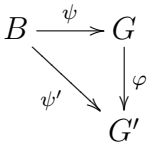
$\varphi(e_0) = h_0$ i $\varphi(e_1) = h_1$, perquè $\operatorname{im}\varphi \subseteq H$ hauria de ser, d'una banda, un subgrup abelià de H, i, de l'altra, un subgrup de H que contingués h_0 i h_1, i que, per tant, no podria ser commutatiu. Es deixa com a exercici la comprovació que $\mathbb{Z}^n$ és un grup abelià lliure de base $B = \{e_0, \ldots, e_{n-1}\}$.

Corol·lari 4.1.5. *Sigui B un conjunt qualsevol. Si existeix una aplicació $\psi : B \longrightarrow G$ de manera que, amb aquesta aplicació, G és un grup lliure de base B (o un grup abelià lliure de base B), llavors ψ és injectiva.*

Demostració: Suposem que ψ no és injectiva; llavors, existeixen elements $g_1, g_2 \in B$, $g_1 \neq g_2$ tals que $\psi(g_1) = \psi(g_2)$. Sigui ara $H \neq \{1\}$ un grup qualsevol, i siguin $h_1, h_2 \in H$, $h_1 \neq h_2$. Si considerem qualsevol aplicació $f : B \longrightarrow H$ tal que $f(g_1) = h_1$ i $f(g_2) = h_2$, no pot existir cap morfisme de grups (ni, de fet, cap aplicació entre conjunts) $\varphi : G \longrightarrow H$ tal que $\varphi \circ \psi = f$, perquè ψ identifica dos elements que no identifica f. □

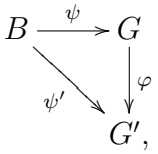
Observació 4.1.6. Aquest resultat fa que puguem pensar que B és un subconjunt de G i ψ és la inclusió de B en G. En general, però, això no és necessari i podem considerar qualsevol conjunt equipotent a B com a base, a canvi de modificar ψ amb una bijecció adequada d'aquest conjunt en B.

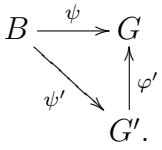
Proposició 4.1.7. *Suposem que B és un conjunt qualsevol i G, G' són grups lliures de base B, o bé grups abelians lliures de base B. Llavors, existeix un únic morfisme de grups $\varphi : G \longrightarrow G'$ tal que el diagrama*



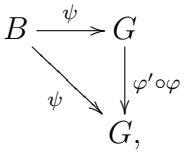
és commutatiu, on ψ, ψ' són les inclusions de B en el grup corresponent, i aquest morfisme és un isomorfisme.

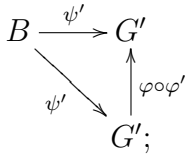
Demostració: Per ser G i G' grups lliures de base B (o bé grups abelians lliures de base B), existeixen morfismes de grups φ, φ', únics tals que



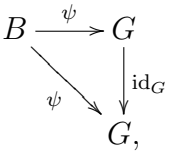


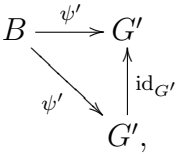
Per tant, per a les composicions se satisfà que





però, com que





les unicitats de la propietat universal ens diuen que $\varphi' \circ \varphi = \mathrm{id}_G$ i que $\varphi \circ \varphi' = \mathrm{id}_{G'}$, de manera que φ i φ' són isomorfismes, l'un invers de l'altre. □

4.1.8. Així, doncs, si per a un conjunt B existeix un grup lliure de base B, aquest grup lliure és únic llevat d'un únic isomorfisme. I anàlogament per a grups abelians; si existeix un grup abelià lliure de base B, aquest grup abelià lliure és únic llevat d'un únic isomorfisme. La resta de la secció està dedicada, gairebé íntegrament, a la demostració de l'existència del grup lliure de base qualsevol conjunt B. El cas de grups abelians lliures es tractarà posteriorment (cf. **4.2.4**).

Teorema 4.1.9 (Existència de grups lliures)**.** *Sigui B un conjunt qualsevol. Llavors, existeix un grup lliure de base B.*

Demostració: En aquesta demostració farem la construcció, amb tot detall, d'un model de grup lliure. Notem que si el conjunt B és el conjunt buit (o bé conté un sol element) ja hem vist en els exemples de més amunt (cf. **4.1.4**) l'existència dels corresponents grup lliure i grup abelià lliure de base B. A partir d'ara, doncs, suposarem que $B \neq \varnothing$.

Considerem dos objectes diferents $+, - \notin B$, i siguin $B^+ := B \times \{+\}$, $B^- := B \times \{-\}$, i $A := B^+ \cup B^-$; notem que la unió és disjunta. Escriurem els elements de A en la forma b^+, o b^-, per a $b \in B$; i identificarem B amb B^+ via l'aplicació $b \mapsto b^+$. Anomenarem alfabet el conjunt A, i lletres (o símbols) els seus elements.

A continuació, considerarem totes les paraules que es poden formar amb les lletres de A; és a dir, considerarem el conjunt $G^*(B) := \bigcup_{n \geq 0} A^n$. Anomenarem paraules els elements de $G^*(B)$; amb més precisió, anomenarem paraules de n lletres (o de n símbols, o de longitud n) els elements de A^n, i escriuren $1 \in A^0$ per a la paraula buida. En general, escriurem els elements de $G^*(B)$ per juxtaposició, sense parèntesis ni comes: $a_0 a_1 \cdots a_{n-1} \in A^n$, per a $a_i \in A$, $0 \leq i \leq n-1$. I direm que la paraula $a_0 a_1 \cdots a_{n-1}$ conté les paraules $a_i a_{i+1} \cdots a_j$ per a $0 \leq i \leq j \leq n-1$, i també que conté la paraula 1.

Definició 4.1.10. Anomenarem dígrafs muts les paraules bb^- i b^-b, amb $b \in B$. I direm que una paraula $a_0 a_1 \cdots a_{n-1}$, $n \geq 2$, és escurçable si existeix k, $0 \leq k \leq n-2$, tal que la paraula $a_k a_{k+1}$ és un dígraf mut; és a dir, si la paraula conté algun dígraf mut. Anomenarem reduïdes les paraules no escurçables.

Definició 4.1.11. Sigui $G(B)$ el subconjunt de $G^*(B)$ format per les paraules reduïdes. Com que la paraula 1 i les paraules d'una sola lletra són reduïdes, tenim que $1 \in G(B)$ i que $A \subseteq G(B)$.

Es tracta de definir una estructura de grup en $G(B)$ i de demostrar que $G(B)$ és un grup lliure de base B. Per a això, comencem per definir un procés de reducció de paraules.

Siguin $r_0 : A^0 \longrightarrow G(B)$ i $r_1 : A \longrightarrow G(B)$ les aplicacions donades per $1 \mapsto 1$, i $a \mapsto a$, respectivament. Suposem que $n \geq 2$ i que per a tot $k < n$ hem definit una aplicació de reducció $r_k : A^k \longrightarrow G(B)$; es tracta de definir l'aplicació de reducció $r_n : A^n \longrightarrow G(B)$. Donada una paraula $a_0 \cdots a_{n-1} \in A_n$, posem $r_n(a_0 \cdots a_{n-1}) :=$

$$\begin{cases} a_0 \cdots a_{n-1}, & \text{si } a_0 \cdots a_{n-1} \text{ és reduïda,} \\ r_{n-2}(a_0 \cdots a_{i-1} a_{i+2} \cdots a_{n-1}), & \text{si } a_i a_{i+1} \text{ és el primer dígraf mut de } a_0 \cdots a_{n-1}. \end{cases}$$

En particular, per a tot $b \in B$, és $r_2(bb^-) = r_2(b^-b) = 1$.

Així, per a tot $n \geq 0$, tenim una aplicació de reducció $r_n : A^n \longrightarrow G(B)$ i podem definir $r : G^*(B) \longrightarrow G(B)$ a partir de les seves restriccions: $r|_{A^n} := r_n$; és a dir, donada una paraula $x \in G^*(B)$, existeix un únic $n \geq 0$ tal que $x \in A^n$, i llavors $r(x) := r_n(x)$. Se satisfà la propietat següent.

Proposició 4.1.12. *Siguin $x \in G(B)$ una paraula reduïda i $y \in G^*(B)$ una paraula qualsevol. Aleshores,*

$$r(xy) = r(xr(y)), \qquad i \qquad r(yx) = r(r(y)x).$$

Demostració (de la proposició): Anem a provar la primera igualtat, $r(xy) = r(xr(y))$. Posem $x = a_0 \cdots a_{n-1}$, $y = a_n \cdots a_{n+m-1}$, amb $a_i \in A$ lletres, $0 \leq i \leq n+m-1$, i raonem per inducció sobre la longitud, m, de y.

Clarament, per a $m = 0$ i per a $m = 1$ és $r(y) = y$, de manera que la propietat és tautològica, per a tota paraula reduïda x:

$$r(xy) = r(xr(y)).$$

Suposem, doncs, que per a tota paraula reduïda $x' \in G(B)$ i tota paraula $y' \in G^*(B)$ de menys de m lletres se satisfà que

$$r(x'y') = r(x'r(y')).$$

Distingim casos. Suposem, en primer lloc, que $a_{n-1}a_n$ no és un dígraf mut. Si la paraula y és reduïda, llavors $r(y) = y$ i també xy és reduïda, de manera que $r(xy) = xy = xr(y) = r(xr(y))$. I si la paraula y no és reduïda, com que $a_{n-1}a_n$ no és un dígraf mut, el primer dígraf mut de xy coincideix amb el primer dígraf mut de y; sigui $a_{n+k}a_{n+k+1}$, amb $0 \leq k \leq m-2$, aquest primer dígraf mut, i posem $y' := a_n \cdots a_{n+k-1}a_{n+k+2} \cdots a_{n+m-1}$. Llavors, per definició de r, és $r(y) = r(y')$, i $r(xy) = r(xy')$. I, per hipòtesi d'inducció, com que y' és de $m-2 < m$ lletres, tenim que $r(xy') = r(xr(y'))$; per tant,

$$r(xy) = r(xy') = r(xr(y')) = r(xr(y)),$$

com calia veure.

Mirem-nos ara l'altre cas i suposem, doncs, que $a_{n-1}a_n$ és un dígraf mut. Posem $x' := a_0 \cdots a_{n-2}$, $y' := a_{n+1} \cdots a_{n+m-1}$, de manera que $x = x'a_{n-1}$ i $y = a_n y'$. Llavors, $r(xy) = r(x'a_{n-1}a_n y') = r(x'y')$, perquè el primer dígraf mut de xy és $a_{n-1}a_n$, i $r(x'y') = r(x'r(y'))$, perquè podem utilitzar la hipòtesi d'inducció, ja que la paraula y' és més curta que y i la paraula x' és reduïda. Doncs, tenim, d'una banda, que $r(xy) = r(x'r(y'))$. Posem $y'' := r(y')$; en particular, y'' és reduïda i, per tant, $r(y'') = y''$. Això ens diu que $r(xy) = r(x'y'')$.

Calculem, ara, $r(xr(y))$; per a acabar la prova, cal veure que $r(xr(y)) = r(x'y'')$. Tenim que $r(xr(y)) = r(x'a_{n-1}r(a_n y'))$; però, per hipòtesi d'inducció, com que la paraula y' és més curta que la paraula y i la paraula a_n és reduïda, tenim que $r(a_n y') = r(a_n r(y'))$; o sigui, que $r(xr(y)) = r(x'a_{n-1}r(a_n r(y'))) = r(x'a_{n-1}r(a_n y''))$. I, a més a més, les paraules x' i y'' són reduïdes. Si la primera lletra de y'' no és a_{n-1}, llavors $a_n y''$ és reduïda i $r(a_n y'') = a_n y''$, de manera que $r(x'a_{n-1}r(a_n y'')) = r(x'a_{n-1}a_n y'') = r(x'y'')$, com calia veure. I si la primera lletra de y'' és a_{n-1}, posem $y'' = a_{n-1}y'''$ i calculem $r(a_n y'') = r(a_n a_{n-1} y''') = r(y''') = y'''$, perquè y''' és reduïda, de manera que $r(x'a_{n-1}r(a_n y'')) =$

$r(x'a_{n-1}r(a_na_{n-1}y'''))=r(x'a_{n-1}r(y'''))=r(x'a_{n-1}y''')=r(x'y'')$, i això acaba la prova de la primera propietat.

La segona propietat es pot demostrar de manera similar. Deixem els detalls com a exercici. □

Corol·lari 4.1.13. *Siguin $x,y\in G^*(B)$ paraules qualssevol. Llavors,*

$$r(r(x)y)=r(r(x)r(y))=r(xr(y)).\ \square$$

Observació 4.1.14. Es pot provar, per exemple, per inducció, que per a $x,y\in G^*(B)$ és $r(xy)=r(r(x)r(y))$. També deixem els detalls com a exercici.

Continuem amb la demostració de l'existència del grup lliure. Aquest resultat ens permet definir una operació binària en $G(B)$ de la manera següent.

Definició 4.1.15. Donades paraules reduïdes $x,y\in G(B)$, posem $x*y:=r(xy)$. Notem que $x*y=r(r(x)r(y))=r(r(xy))=r(xr(y))=r(r(x)y)$.

Proposició 4.1.16. *$G(B)$, amb l'operació binària $*$ que acabem de definir, admet una única estructura de grup. A més a més, B és un conjunt generador de $G(B)$.*

Demostració: La paraula buida, 1, és clarament un element neutre per a aquesta operació $*$. D'altra banda, donada una paraula reduïda $x=a_0\cdots a_{n-1}$, $a_0,\ldots,a_{n-1}\in A$, posem $a_i^-:=b^-$, si $a_i=b^+$, amb $b\in B$, i $a_i^-:=b^+$, si $a_i=b^-$, amb $b\in B$. Llavors, la paraula $a_{n-1}^-\cdots a_0^-$ és reduïda i és inversa de x respecte de $*$ i 1 (càlcul immediat). Veiem, finalment, que $*$ és associativa. Per a això, considerem paraules reduïdes x,y,z, i calculem: $(x*y)*z=r((x*y)z)=r(r(xy)z)=r(xyz)=r(xr(yz))=r(x(y*z))=x*(y*z)$, com calia veure.

Per a veure que B és un conjunt generador de $G(B)$, ho podem fer per inducció sobre la longitud de la paraula reduïda $x:=a_0\cdots a_{n-1}\in G(B)$. Si $n=0$, la paraula és l'element neutre i, evidentment, pertany al subgrup generat per B. Si $n=1$, llavors $x\in B\uplus B^-$; o sigui, $x\in B$ o bé $x^{-1}\in B$, de manera que x pertany al subgrup generat per B. I si $a_1\cdots a_{n-1}$ pertany al subgrup generat per B, com que $a_0\cdots a_{n-1}=r(a_0a_1\cdots a_{n-1})=r(r(a_0)r(a_1\cdots a_{n-1}))=a_0*(a_1\cdots a_{n-1})$, també $a_0\cdots a_{n-1}$ hi pertany. □

Finalment, veiem que aquest grup $G(B)$ és un grup lliure de base B. És a dir, veiem el resultat següent.

Proposició 4.1.17. *Donats un grup G i una aplicació $f:B\longrightarrow G$ de conjunts, qualssevol, existeix un únic morfisme de grups $\varphi:G(B)\longrightarrow G$ tal que $\varphi(b)=f(b)$, per a tot $b\in B$.*

Demostració: En efecte, comencem per definir una aplicació $\varphi_n:A^n\longrightarrow G$ de la manera següent: per a $n=0$, posem $\varphi_0:A^0\longrightarrow G$ l'aplicació donada per $1\mapsto 1$; per a $n=1$, posem $\varphi_1:A\longrightarrow G$ l'aplicació donada per l'assignació $b\mapsto f(b)$, i $b^-\mapsto f(b)^{-1}$, per a tot $b\in B$; com que $A=B\uplus B^-$, φ_1 està ben definida. Ara, per a tot $n\geq 2$, podem definir una aplicació $\varphi_n:A^n\longrightarrow G$ per l'assignació $a_0\cdots a_{n-1}\mapsto\varphi_1(a_0)\cdots\varphi_1(a_{n-1})$. I com que $G^*(B)=\biguplus_{n\geq 0}A^n$, podem definir $\varphi^*:G^*(B)\longrightarrow G$ a partir de les restriccions: $\varphi^*(a_0\cdots a_{n-1}):=\varphi_n(a_0\cdots a_{n-1})=\varphi_1(a_0)\cdots\varphi_1(a_{n-1})$.

És clar, de la definició de φ^*, que per a $x, y \in G^*(B)$, és $\varphi^*(xy) = \varphi^*(x) \cdot \varphi^*(y)$. En particular, per a un dígraf mut $a_k a_{k+1}$, es té que $\varphi^*(a_k a_{k+1}) = 1$, de manera que si una paraula $a_0 \cdots a_{n-1} \in A^n$ conté un dígraf mut, $a_k a_{k+1}$, amb $0 \leq k \leq n-2$, llavors $\varphi_n(a_0 \cdots a_{n-1}) = \varphi_{n-2}(a_0 \cdots a_{k-1} a_{k+2} \cdots a_{n-1})$. D'aquí es dedueix que per a tota paraula $x \in G^*(B)$ és $\varphi^*(r(x)) = \varphi(x)$.

Sigui $\varphi : G(B) \longrightarrow G$ la restricció de φ^* al subconjunt $G(B)$. Llavors, φ és un morfisme de grups, perquè per a $x, y \in G(B)$ és $\varphi(x * y) = \varphi^*(x * y) = \varphi^*(r(r(x)r(y))) = \varphi^*(r(x)r(y)) = \varphi^*(r(x)) \cdot \varphi^*(r(y)) = \varphi^*(x) \cdot \varphi^*(y) = \varphi(x) \cdot \varphi(y)$. Finalment, és clar que per a tot $b \in B$ és $\varphi(b) = \varphi_1(b) = f(b)$ i, com que B genera $G(B)$, el morfisme φ és determinat unívocament per les imatges dels elements $b \in B$. □

Amb això s'acaba la demostració de l'existència de grup lliure. □

Corol·lari 4.1.18. *Sigui G un grup qualsevol. Llavors, existeixen un conjunt B, un grup lliure de base B, $G(B)$, i un morfisme exhaustiu de grups $\varphi : G(B) \longrightarrow G$.*

Demostració: Siguin B un conjunt de generadors de G (per exemple, podríem prendre $B = G$), $G(B)$ el grup lliure de base B, i $f : B \longrightarrow G$ l'aplicació d'inclusió del conjunt B en el grup G. El morfisme que proporciona la propietat universal de grup lliure és un morfisme de grups tal que $B \subseteq \operatorname{im} \varphi$; per tant, $G = \langle B \rangle \subseteq \operatorname{im} \varphi$ i $\operatorname{im} \varphi = G$. □

Observació 4.1.19. En virtut del teorema d'isomorfia, tenim que $G \cong G(B)/\ker \varphi$; és a dir, tot grup és quocient d'un grup lliure. Notem que, a més a més, podem prendre qualsevol B de cardinal més gran o igual que el cardinal de qualsevol conjunt de generadors de G; en particular, si G admet un conjunt de generadors de cardinal c; també podem prendre B de cardinal c.

4.2 Suma directa i grups abelians lliures

Per a la construcció del grup abelià lliure de base donada, és convenient disposar del concepte de suma directa de grups abelians. Aquest concepte de suma directa, restringit al cas d'espais vectorials, se sol treballar en un curs d'àlgebra lineal; però és molt més general i, de fet, és semblant al concepte de producte, del qual només es diferencia formalment en el sentit dels morfismes involucrats.

Definició 4.2.1. Sigui $\{G_i\}_{i \in I}$ una família de grups abelians. S'anomena suma directa de la família $\{G_i\}_{i \in I}$ un grup abelià G i una família $\{\psi_i : G_i \longrightarrow G\}_{i \in I}$ de morfismes de grups abelians, tals que per a tota família de morfismes de grups abelians $\{\varphi_i : G_i \longrightarrow H\}_{i \in I}$ existeix un únic morfisme de grups abelians $\varphi : G \longrightarrow H$ tal que per a tot $i \in I$ és

$$\forall \{\varphi_i\}_{i \in I} \ \exists! \varphi \ \forall i \in I$$

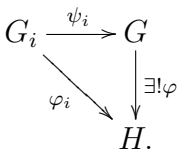


Diagrama 4.4: Propietat universal de la suma directa

Aquest grup suma directa, G, es representa per $\bigoplus_{i \in I} G_i$, i els morfismes $\psi_j : G_j \longrightarrow \bigoplus_{i \in I} G_i$ s'anomenen els morfismes canònics o inclusions canòniques.

Notem que, si comparem aquesta definició amb la definició de grup abelià producte, només s'ha donat la volta a tots els morfismes que hi apareixen. De manera semblant a aquell cas, n'obtenim la unicitat, cas que existeixi.

Corol·lari 4.2.2. *Sigui $\{G_i\}_{i\in I}$ una família no buida de grups abelians. Si existeix una suma directa $\{G_i \xrightarrow{\psi_i} G\}_{i\in I}$, és única llevat d'un únic isomorfisme. Amb més precisió, si*

$$\left\{G_i \xrightarrow{\psi_i} G\right\}_{i\in I}, \qquad \left\{G_i \xrightarrow{\psi'_i} G'\right\}_{i\in I},$$

són sumes directes de la família $\{G_i\}_{i\in I}$, llavors existeix un únic morfisme $\varphi : G \longrightarrow G'$ tal que per a tot $i \in I$ és

$$\begin{array}{ccc} G_i & \xrightarrow{\psi_i} & G \\ & \searrow^{\psi'_i} & \downarrow \varphi \\ & & G'. \end{array}$$

Aquest morfisme φ és un isomorfisme. □

Teorema 4.2.3 (Existència de sumes directes)**.** *Sigui $\{G_i\}_{i\in I}$ una família no buida de grups abelians. Llavors, existeix una suma directa*

$$\left\{G_j \xrightarrow{\psi_j} \bigoplus_{i\in I} G_i\right\}_{j\in I}.$$

Demostració: És suficient posar-ne de manifest un model. Per exemple, notem additivament els grups i, dins el grup producte cartesià $\prod_{i\in I} G_i$, considerem el subgrup

$$\bigoplus_{i\in I} G_i := \left\{\{g_i\}_{i\in I} \in \prod_{i\in I} G_i : \text{ existeix } J \subseteq I \text{ finit, i } g_i = 0 \text{ per a tot } i \in I,\, i \notin J\right\}.$$

I prenem com a morfismes canònics els donats per les aplicacions $\psi_j : G_j \longrightarrow \bigoplus_{i\in I} G_i$, definides com segueix:

$$\text{per a } g \in G_j, \qquad \psi_j(g) := \{g_i\}_{i\in I}, \qquad \text{on } g_i := \begin{cases} 0, & \text{si } i \neq j, \\ g, & \text{si } i = j. \end{cases}$$

Notem que, per a tot element $x = \{g_i\}_{i\in I} \in \bigoplus_{i\in I} G_i$, el conjunt $J_x := \{j \in I : g_j \neq 0\} \subseteq I$ és finit (i de fet, buit, si, i només si, $x = 0$) i $x = \sum_{j\in J_x} \psi_j(g_j)$, de manera única.

Així, donats un grup abelià H i una família $\{\varphi_i : G_i \longrightarrow H\}_{i\in I}$ de morfismes de grups abelians, podem definir $\varphi : \bigoplus_{i\in I} G_i \longrightarrow H$ per l'assignació $\varphi(x) := \sum_{j\in J_x} \varphi_j(g_j)$. La comprovació que φ és un morfisme de grups abelians, l'únic per al qual se satisfà la propietat universal de la suma directa és senzilla i es deixa com a exercici. □

L'existència de la suma directa d'una família qualsevol de grups abelians ens permet demostrar molt fàcilment l'existència del grup abelià lliure de base donada, un conjunt qualsevol B.

Teorema 4.2.4 (Existència de grups abelians lliures)**.** *Sigui B un conjunt qualsevol. Llavors, existeix un grup abelià lliure de base B.*

DEMOSTRACIÓ: Ja hem vist que si $B = \varnothing$, el grup trivial és un grup abelià lliure de base $\varnothing$, i que el grup additiu $\mathbb{Z}$ és un grup abelià lliure de base $\{1\}$. En general, per a un conjunt qualsevol $B \neq \varnothing$, i per a tot element $b \in B$, posem $G_b := \mathbb{Z}$, el grup additiu; i considerem la família $\{G_b\}_{b\in B}$. Llavors, el grup abelià suma directa, $\bigoplus_{b\in B} G_b$, amb l'aplicació $B \longrightarrow \bigoplus_{b\in B} G_b$ donada per les assignacions $b \mapsto 1 \in G_b \mapsto \psi_b(1) \in \bigoplus_{b\in B} G_b$, on ψ_b són els morfismes canònics en la suma directa, és un grup abelià lliure de base B. La comprovació és, de nou, un exercici senzill. □

Com en el cas de grups, allà sense la restricció de commutativitat, tenim el resultat següent (cf. **4.1.18**, **4.1.19**).

Corol·lari 4.2.5. *Sigui G un grup abelià qualsevol. Llavors, existeixen un conjunt B, un grup abelià lliure de base B, $A(B)$, i un morfisme exhaustiu de grups $\varphi : A(B) \longrightarrow G$. Si G admet un conjunt de generadors de cardinal c, el grup abelià lliure $A(B)$ es pot prendre de base B de cardinal c.* □

4.3 Subgrup derivat. Abelianitzat d'un grup

El fet de disposar de commutativitat de l'operació binària de grup fa que el treball amb grups abelians sigui més senzill que el treball amb grups arbitraris. En aquesta secció, estudiarem una manera d'associar a cada grup, i de manera natural, un grup abelià, de manera que algunes propietats del grup es reflecteixin en aquest grup abelià. Així, obtindrem una eina còmoda per al tractament d'alguns grups. El procés s'anomena d'abelianització d'un grup i el grup abelià associat a un grup G s'anomena l'abelianitzat del grup G.

Definició 4.3.1. Siguin G un grup i $g, h \in G$. S'anomena commutador de g i h, en aquest ordre, l'element $[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1} \in G$. Donats subgrups (o més generalment, subconjunts no buits) $H, K \subseteq G$, s'anomena commutador de H i K el subgrup $[H, K] \subseteq G$ generat pels commutadors $[h, k]$, per a $h \in H$ i $k \in K$. És a dir,

$$[H, K] := \langle h \cdot k \cdot h^{-1} \cdot k^{-1} : \ h \in H, \ k \in K \rangle.$$

S'anomena derivat de G el commutador $D(G) := [G, G]$.

Proposició 4.3.2. *Sigui G un grup. Se satisfan les propietats següents.*

(a) *Per a elements $g, h \in G$ qualssevol, és $[h, g] = [g, h]^{-1}$.*

(b) *$D(G) \subseteq G$ és un subgrup normal de G.*

(c) *El grup quocient $G/D(G)$ és abelià.*

(d) *Si $K \subseteq G$ és un subgrup normal de G i G/K és un grup abelià, llavors $D(G) \subseteq K$. O sigui, $D(G)$ és el subgrup normal de G més petit per al qual el grup quocient és commutatiu.*

Demostració:

(a) La propietat és immediata a partir de la definició.

(b) Com que, per definició, $D(G) = [G, G]$ és un subgrup de G, és suficient veure que per a tot $g \in G$ i tot generador $[h, k]$, $h, k \in G$, de $D(G)$, és $g \cdot [h, k] \cdot g^{-1} \in D(G)$. Però se satisfà que

$$\begin{aligned} g \cdot [h,k] \cdot g^{-1} &= g \cdot h \cdot k \cdot h^{-1} \cdot k^{-1} \cdot g^{-1} \\ &= (g \cdot h \cdot g^{-1} \cdot h^{-1}) \cdot (h \cdot (g \cdot k) \cdot h^{-1} \cdot (g \cdot k)^{-1}) \\ &= [g,h] \cdot [h,(g \cdot k)] \in D(G). \end{aligned}$$

(c) Un grup qualsevol G' és abelià si, i només si, per a tota parella d'elements $g, h \in G'$ és $g \cdot h \cdot g^{-1} \cdot h^{-1} = 1$; o sigui, si tots els commutadors $[g, h]$ són trivials. I aquesta propietat se satisfà, per definició de $D(G)$, en el grup quocient $G/D(G)$.

(d) Per a tota parella d'elements $g, h \in G$ la classe del commutador $[g, h]$ en el grup quocient G/K és la trivial, perquè aquest grup és abelià; per tant, el representant $[g, h]$ pertany a K, com calia veure. □

Definició 4.3.3. Sigui G un grup. El grup abelià $G^{ab} := G/D(G)$ s'anomena el grup abelianitzat de G. Clarament, si G és abelià, llavors $G^{ab} = G$, perquè $D(G) = \{1\}$.

Definició 4.3.4. Siguin G, H, grups i $\varphi : G \longrightarrow H$ un morfisme de grups. Llavors, existeix un únic morfisme de grups $\widetilde{\varphi} : G^{ab} \longrightarrow H^{ab}$ tal que

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ G^{ab} & \xrightarrow[\widetilde{\varphi}]{} & H^{ab}. \end{array}$$

En efecte, com que H^{ab} és commutatiu, resulta que $D(G) \subseteq \ker(\pi \circ \varphi)$; per tant, el morfisme $\pi \circ \varphi$ factoritza a través del quocient G^{ab}. Aquest morfisme $\widetilde{\varphi}$ s'anomena l'abelianitzat del morfisme φ.

Exercici 4.3.5. Siguin G, H, K grups i $\varphi : G \longrightarrow H$, $\psi : H \longrightarrow K$ morfismes de grups. Llavors, $\widetilde{\psi \circ \varphi} = \widetilde{\psi} \circ \widetilde{\varphi}$. I per a la identitat de G, és $\widetilde{\mathrm{id}_G} = \mathrm{id}_{G^{ab}}$.

Observació 4.3.6. Només a tall d'informació, i sense entrar en cap detall, podem dir que en llenguatge de teoria de categories el pas dels grups als seus abelianitzats i dels morfismes de grups als morfismes corresponents entre els seus abelianitzats és un functor covariant de la categoria de grups a la categoria de grups abelians. Un primer fet remarcable, però, és que, per a tot conjunt B, el grup abelià lliure de base B és exactament l'abelianitzat del grup lliure de base B.

Proposició 4.3.7. *Siguin B un conjunt qualsevol i $G(B)$ el grup lliure de base B. Llavors, $G(B)^{ab}$ és un model del grup abelià lliure de base B. És a dir, si $A(B)$ és un grup abelià lliure de base B, llavors existeix un únic isomorfisme $\psi : A(B) \longrightarrow G(B)^{ab}$ tal que per a tot $b \in B$, $\psi(b)$ és la classe en $G(B)^{ab}$ de l'element $b \in G(B)$; és a dir, $\psi(b) = b \cdot D(G(B)) \in G^{ab}$.*

DEMOSTRACIÓ: Recordem que $G(B)^{ab} = G(B)/D(G(B))$, on $D(G(B))$ és el derivat del grup $G(B)$. Considerem el diagrama següent d'aplicacions de conjunts i morfismes de grups. En aquest diagrama, π és la projecció canònica de $G(B)$ en $G(B)^{ab}$; φ és el morfisme exhaustiu determinat per la inclusió $B \hookrightarrow A(B)$, perquè $B \hookrightarrow G(B)$ és el grup lliure de base B i B genera $A(B)$; ψ és el morfisme determinat per l'aplicació $B \hookrightarrow G(B) \xrightarrow{\pi} G(B)^{ab}$, perquè $B \hookrightarrow A(B)$ és el grup abelià lliure de base B, i que és exhaustiu perquè la imatge de B genera $G(B)^{ab}$; i, finalment, $\widetilde{\varphi}$ és el morfisme determinat per φ, ja que per ser $A(B)$ un grup abelià, tenim que $D(G(B)) \subseteq \ker\varphi$, i, per tant, el morfisme φ factoritza a través de la projecció π.

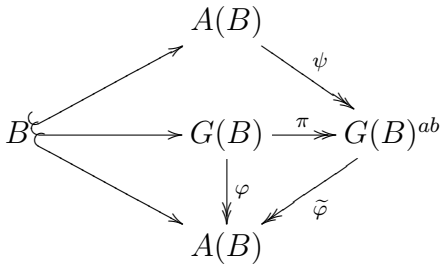


Diagrama 4.5: Grup lliure i grup abelià lliure

Ara, notem que les dues composicions $\widetilde{\varphi}\circ\psi$ i $\psi\circ\widetilde{\varphi}$ són les identitats corresponents. La primera, perquè $B \hookrightarrow A(B)$ és el grup abelià lliure de base B, per als dos morfismes $\widetilde{\varphi}\circ\psi$ i $\mathrm{id}_{A(B)}$ se satisfà que $b \mapsto b$, per a tot $b \in B$, i perquè B genera $A(B)$. I la segona, per una raó semblant: la imatge de qualsevol element $b \in B$ en $G(B)^{ab}$, per qualsevol dels dos morfismes $\psi\circ\widetilde{\varphi}$ i $\mathrm{id}_{G(B)^{ab}}$ és la classe $b\cdot D(G(B))$, perquè $\varphi(b) = b$, i les classes $b\cdot D(G(B))$, $b \in B$, generen $A(B)$. Això demostra que els dos morfismes ψ i $\widetilde{\varphi}$ són isomorfismes i acaba la demostració. □

4.4 Presentacions de grups. Grups diedrals

Sigui G un grup qualsevol. El fet que existeixi algun conjunt B de manera que G es pugui escriure com un grup quocient del grup lliure de base B, $G(B)$, justifica la definició següent.

Definició 4.4.1. Sigui G un grup qualsevol. Una presentació de G és una parella formada per un conjunt B, anomenat conjunt de generadors, i un conjunt R, anomenat conjunt de relacions, tal que R és un subconjunt del grup lliure $G(B)$, de base B, i el grup G és isomorf al grup quocient $G(B)/N(R)$, on $N(R)$ és el menor subgrup normal de $G(B)$ que conté R; és a dir, el subgrup normal generat per R. Es fa servir la notació $G = \langle B; R\rangle$. S'anomenen relacions tots els elements de $N(R)$, i no només els del conjunt R.

Observacions 4.4.2. • Notem que, donat un grup qualsevol, G, i un subconjunt qualsevol $R \subseteq G$, el conjunt de subgrups normals de G que contenen R és no buit (per exemple, perquè G hi pertany) i, per tant, té sentit la intersecció de tots aquests subgrups normals; i, clarament, aquesta intersecció és un subgrup normal i conté R.

• Si $B = \{b_0 1, \ldots b_{n-1}\}$ i $R = \{r_0, \ldots, r_{m-1}\}$ són finits, en lloc d'escriure $\langle B; R\rangle$, s'acostuma a escriure $\langle b_0, \ldots, b_{n-1}; r_0, \ldots, r_{m-1}\rangle$, sense escriure les claus de conjunt: $\{$, $\}$.

Exemples 4.4.3. • Si G és un grup lliure de base B, llavors $G = \langle B; \varnothing\rangle = \langle B; \{1\}\rangle$.

• Sigui G un grup cíclic d'ordre d. Llavors $G = \langle g; g^d\rangle$ és una presentació de G. En efecte, el grup lliure generat per un sol element g és cíclic infinit; per tant, és commutatiu i qualsevol subgrup és normal; en particular, el subgrup generat per g^d; i, clarament, $G \cong \langle g\rangle/\langle g^d\rangle$.

• Sigui G un grup cíclic d'ordre d. Per a tota parella de nombres enters, $m, n \in \mathbb{Z}$, tals que $\mathrm{mcd}(m, n) = d$, la presentació $\langle g; g^n, g^m\rangle$ ho és del grup cíclic d'ordre d.

Observacions 4.4.4. • Sigui $G = \langle B; R\rangle$ una presentació d'un grup G. Això és dir que $G \cong G(B)/N(R)$, on $G(B)$ és el grup lliure de base B i $N(R)$ és el subgrup normal de $G(B)$ generat per R. Com que les imatges en G dels elements de R són l'element neutre, sovint les relacions $x \in R$ s'escriuen en la forma $x = 1$. I relacions de la forma $x \cdot y^{-1}$, $x, y \in G(B)$, també s'escriuen en la forma $x = y$.

• A partir d'una relació $a \cdot b^{-1}$, s'obté la relació $a^2 \cdot b^{-2}$, ja que

$$a^2 \cdot b^{-2} = (a \cdot (a \cdot b^{-1}) \cdot a^{-1}) \cdot (a \cdot b^{-1}),$$

i el subgrup de les relacions és normal, per definició. Per inducció, s'obté que si es té una relació $a \cdot b^{-1}$, llavors també es té la relació $a^n \cdot b^{-n}$, per a tot nombre enter n (natural o no). D'altra banda, la presència d'una relació $a^2 \cdot b^{-2}$ en una presentació, no implica la presència de la relació $a \cdot b^{-1}$.

Definició 4.4.5. Per a tot nombre enter $n \geq 1$, S'anomena grup diedral $(2 \cdot n)$-èsim el grup determinat per la presentació $D_{2\cdot n} := \langle g, s; g^n, s^2, s \cdot g \cdot s \cdot g\rangle$.

Exemples 4.4.6. • $D_{2\cdot 1} = \{1, s\}$ és un grup cíclic d'ordre 2. En efecte, la presentació

$$D_{2\cdot 1} = \langle g, s; g, s^2, s \cdot g \cdot s \cdot g\rangle$$

prové del grup lliure $G(g, s)$, de base $\{g, s\}$. Considerem, també, el grup lliure $G(s)$, de base $\{s\}$, el morfisme de grups $\varphi : G(g, s) \longrightarrow G(s)$ determinat per les assignacions $g \mapsto 1$, $s \mapsto s$, i la projecció $\pi : G(s) \longrightarrow G(s)/\langle s^2\rangle$. És clar que el morfisme composició $\pi \circ \varphi$ és exhaustiu i que el seu nucli és $\varphi^{-1}(\langle s^2\rangle) = \langle g, s^2\rangle$, perquè el nucli de φ és $\langle g\rangle$. En virtut del teorema d'isomorfia, tenim que $G(g, s)/\langle g, s^2\rangle \cong G(s)/\langle s^2\rangle$, que és un grup cíclic d'ordre 2. Només cal adonar-nos, ara, que el menor subgrup normal que conté g, s^2 també conté $s \cdot g \cdot s \cdot g = (s \cdot g \cdot s^{-1}) \cdot s^2 \cdot g$; per tant, el nucli és, també, $\langle g, s^2, s \cdot g \cdot s \cdot g\rangle$, com calia veure.

• $D_{2\cdot 2} = \{1, g, s, s \cdot g\}$ és el grup producte de dos grups cíclics d'ordre 2. En efecte, és generat per dos elements d'ordre 2, g, s, per als quals se satisfà que el producte també és d'ordre 2 i que commuten. Deixem els detalls com a exercici.

Proposició 4.4.7 (Representació del grup diedral com a grup de matrius reals)**.** *Per a tot nombre enter $n \geq 1$, el grup diedral $D_{2\cdot n}$ és isomorf al subgrup de $\mathbf{GL}(2, \mathbb{R})$ generat per les matrius*

$$g := \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}, \qquad s := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Els seus elements són els productes g^k, i $s \cdot g^k$, per a $0 \leq k \leq n-1$, amb $g^n = 1$. I se satisfà que, per a tot k, $0 \leq k \leq n-1$, és $g^k \cdot s = s \cdot g^{n-k}$.

DEMOSTRACIÓ: El resultat és una simple comprovació. Les relacions $s^2 = 1$ i $g^n = 1$ ens diuen que, en el quocient, és $s^{-1} = s$ i $g^{-1} = g^{n-1}$. Això ens permet intercalar, a qualsevol paraula, una potència positiva adequada de g o de s sense canviar la seva classe. A més a més, la relació $s \cdot g \cdot s \cdot g$ ens diu que, en el quocient, és $s \cdot g = g^{n-1} \cdot s$; per tant, podem fer córrer les potències de s cap a l'esquerra i obtenim que tota paraula en les lletres g, s, té un representant de la forma g^k, o $s \cdot g^k$, per a $0 \leq k \leq n-1$. I totes aquestes són diferents. Per exemple, com que les matrius g^k són de determinant 1 i les altres de determinant -1, no pot haver-hi igualtats de la forma $g^k = s \cdot g^r$, amb $0 \leq k, r \leq n-1$; i una igualtat $s \cdot g^k = s \cdot g^r$ equivaldria a una igualtat $g^k = g^r$, de manera que hauria de ser $k = r$. □

Observació 4.4.8. Les matrius de la proposició anterior pertanyen, de fet, al grup ortogonal $\mathbf{O}(2, \mathbb{R}) \subseteq \mathbf{GL}(2, \mathbb{R})$ i representen exactament els desplaçaments del pla euclidià que deixen invariant un n-àgon regular centrat a l'origen de coordenades i amb un vèrtex al punt de coordenades $(1, 0)$.

Proposició 4.4.9 (Representació del grup diedral com a grup de permutacions)**.** *Per a tot nombre enter $n \geq 1$, el grup diedral $D_{2\cdot n}$ és isomorf al subgrup del grup simètric S_n generat pel n-cicle $g = (0, 1, \ldots, n-1)$ i la permutació*

$$s = \begin{cases} (1, n-1) \circ (2, n-2) \circ \cdots \circ (m-1, m+1), & \text{si } n = 2m, \text{ parell,} \\ (1, n-1) \circ (2, n-2) \circ \cdots \circ (m, m+1), & \text{si } n = 2m+1, \text{ senar.} \end{cases}$$

DEMOSTRACIÓ: Reprenem les notacions de la proposició anterior i considerem els vectors $P_k := (\cos \frac{2k\pi}{n}, \sin \frac{2k\pi}{n}) \in \mathbb{R}^2$, $0 \leq k \leq n-1$. Aquests vectors proporcionen els n vèrtexs d'un n-àgon regular sobre la circumferència unitat. I el grup $D_{2\cdot n}$, tal com l'hem descrit en la proposició anterior, actua en el conjunt $\{P_0, \ldots, P_{n-1}\}$; de fet, g^k actua com la rotació d'angle $\frac{2k\pi}{n}$ (transforma, doncs, P_r en P_{k+r}, amb els índexs pensats en $\mathbb{Z}/n\mathbb{Z}$), i s actua com la simetria axial d'eix l'eix d'abscises. La verificació de les fórmules de l'enunciat és una simple comprovació. □

Corol·lari 4.4.10. *Per a tot nombre enter $n \geq 1$, el grup diedral $D_{2\cdot n}$ és d'ordre $2 \cdot n$ i conté un subgrup cíclic d'índex 2 (i, per tant, d'ordre n).*

DEMOSTRACIÓ: En efecte, si $D_{2\cdot n} = \langle g, s; g^n, s^2, s \cdot g \cdot s \cdot g \rangle$, el subgrup que es demana és el subgrup $C_n := \langle g \rangle = \{1, g, \ldots, g^{n-1}\} \subseteq D_{2\cdot n}$. □

4.5 Grups resolubles

A la introducció d'aquest capítol hem comentat que una de les primeres aparicions dels grups es produí en l'estudi de la resolubilitat per radicals de les equacions algebraiques. De fet, la propietat dels grups de simetries de les arrels dels polinomis que permet decidir si una equació algebraica és o no és resoluble per radicals és la propietat que s'ha anomenat, justament per aquesta raó, resolubilitat del grup. En aquesta secció, estudiarem el concepte de grup resoluble de manera abstracta, sense referència al problema que el justifica que, de fet, s'estudia en un curs d'equacions algebraiques (cf. [Travesa 2020]).

Definició 4.5.1. Es diu que un grup G és resoluble si existeix una cadena finita de subgrups de G, $G =: G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$, tal que, per a $1 \leq i \leq n$, G_i és un subgrup normal de G_{i-1} i el grup quocient G_{i-1}/G_i és un grup abelià. Una cadena de subgrups d'aquesta forma s'anomena una resolució del grup G.

Exemples 4.5.2. (a) Tot grup commutatiu G és resoluble, perquè la cadena $G \supseteq \{1\}$ és una resolució de G.

(b) Siguin A un anell commutatiu, G el subgrup de $\mathbf{GL}(2, A)$ format per les matrius de la forma $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$, i $H \subseteq G$ el subgrup format per les matrius de la forma $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$. Llavors, G i H són grups resolubles.

Per a demostrar-ho, comencem per notar que les matrius de $\mathbf{GL}(2, A)$ de la forma $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ formen un subgrup normal K de H; en efecte, aquest conjunt és el nucli de la restricció a H del morfisme determinant, $\det : \mathbf{GL}(2, A) \longrightarrow \mathbf{GL}(1, A) = A^*$. Com que aquest morfisme $\det : H \longrightarrow \mathbf{GL}(1, A) = A^*$ és exhaustiu, el grup quocient H/K és isomorf a $\mathbf{GL}(1, A) = A^*$; en particular, commutatiu. D'altra banda, K és isomorf al grup additiu de A, perquè l'aplicació $f : A \longrightarrow K$ definida per $f(b) := \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ és un isomorfisme. Per tant, K és un subgrup commutatiu de H i, en conseqüència, la cadena de subgrups $H \supseteq K \supseteq \{1\}$ és una resolució de H.

Vegem ara que G és resoluble. El subgrup $H \subseteq G$ és normal i el grup quocient G/H és isomorf a $\mathbf{GL}(1, A)$, ja que l'aplicació $g : G \longrightarrow \mathbf{GL}(1, A)$ donada per $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto d$ és un morfisme exhaustiu de grups de nucli H. Per tant, la cadena $G \supseteq H \supseteq K \supseteq \{1\}$ és una resolució del grup G.

(c) Els grups diedrals $D_{2\cdot n}$ són resolubles. En efecte, si $D_{2\cdot n} = \langle g, s; g^n, s^2, s \cdot g \cdot s \cdot g \rangle$, llavors el subgrup $C_n := \langle g \rangle \subseteq D_{2\cdot n}$ és cíclic i d'index 2; per tant, abelià i normal, i el grup quocient $D_{2\cdot n}/C_n$ és abelià (cíclic d'ordre 2). Doncs, la cadena $D_{2\cdot n} \supseteq C_n \supseteq \{1\}$ és una resolució de $D_{2\cdot n}$. □

(d) Els grups simètrics S_3 i S_4 i el grup alternat A_4 són resolubles. En efecte, és immediat comprovar que la cadena $S_3 \supseteq A_3 \supseteq \{1\}$ és una resolució de S_3. D'altra banda, si $V_4 := \{1, (0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$ designa el grup de Klein, també és immediat comprovar que la cadena $S_4 \supseteq A_4 \supseteq V_4 \supseteq \{1\}$ proporciona una resolució de S_4 i de A_4.

(e) Notem que S_2 és cíclic d'ordre 2, que A_3 és cíclic d'ordre 3, i que A_2 és el grup trivial; per tant, aquests grups també són resolubles.

Proposició 4.5.3. *Siguin G un grup resoluble i H un subgrup qualsevol de G. Llavors, H és resoluble.*

Demostració: Sigui $G_0 := G \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ una resolució de G; es tracta de veure que la cadena $H_0 := H \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\}$, on $H_i := H \cap G_i$, és una resolució de H. En primer lloc, observem que $H_i = H \cap G_i \subseteq H \cap G_{i-1} = H_{i-1}$ i que H_i és normal en H_{i-1}; a més a més, el nucli del morfisme de grups $H_{i-1} = H \cap G_{i-1} \longrightarrow G_{i-1} \longrightarrow G_{i-1}/G_i$ és, evidentment, $H_i = H \cap G_i$; per tant, H_{i-1}/H_i s'identifica amb un subgrup de G_{i-1}/G_i i, per tant, és commutatiu. □

Proposició 4.5.4. *Siguin G un grup resoluble i N un subgrup normal de G. Llavors, G/N és un grup resoluble.*

DEMOSTRACIÓ: Sigui $G_0 := G \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ una resolució de G; es tracta de veure que la cadena $\overline{G}_0 := G/N = \overline{G} \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_n = \{1\}$ és una resolució de G/N, on posem $\overline{G}_i := G_iN/N$, que és el subgrup de G/N generat per la imatge de G_i en G/N.

Com que N és un subgrup normal de G, el normalitzador de N és tot G; per tant, per a $0 \leq i \leq n$, el subgrup de G generat per G_i i N és G_iN (cf. **3.4.9**). A més a més, com que G_i és un subgrup normal de G_{i-1}, també G_iN és un subgrup normal de $G_{i-1}N$, i $\overline{G}_i$ és un subgrup normal de $\overline{G}_{i-1}$. Ara, $\overline{G}_0 = G_0N/N = GN/N = G/N$ i $\overline{G}_n = G_nN/N = N/N = \{1\}$; doncs, només resta veure que els grups quocient $\overline{G}_{i-1}/\overline{G}_i$ són commutatius. El morfisme de grups $G_{i-1} \xrightarrow{\text{incl}} G_{i-1}N \xrightarrow{\text{proj}} G_{i-1}N/G_iN$ és exhaustiu i el seu nucli conté G_i; com a conseqüència, i per pas al quocient, obtenim un morfisme exhaustiu de grups $G_{i-1}/G_i \longrightarrow G_{i-1}N/G_iN$; com que G_{i-1}/G_i és commutatiu, també $G_{i-1}N/G_iN$ és commutatiu; i, com que $G_{i-1}N/G_iN$ és isomorf a $\overline{G}_{i-1}/\overline{G}_i$, aquest darrer grup és commutatiu, com volíem veure. □

Proposició 4.5.5. *Siguin G un grup i $N \subseteq G$ un subgrup normal de G. El grup G és resoluble si, i només si, ho són els grups N i G/N.*

DEMOSTRACIÓ: Les dues proposicions anteriors són una prova de la implicació directa. Recíprocament, suposem que N i G/N són resolubles i siguin

$$N_0 := N \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}, \quad \overline{G}_0 := G/N \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_s = \{1\},$$

resolucions de N i de G/N. Considerem la projecció canònica $\pi : G \longrightarrow G/N$, i siguin $G_i := \pi^{-1}(\overline{G}_i)$, per a $0 \leq i \leq s$, els grups antiimatge. Com que $\overline{G}_i$ és un subgrup normal de $\overline{G}_{i-1}$, per a $1 \leq i \leq s$, obtenim que G_i és un subgrup normal de G_{i-1}; i, a més a més, G_{i-1}/G_i és isomorf a $\overline{G}_{i-1}/\overline{G}_i$; en particular, els quocients G_{i-1}/G_i són commutatius. D'altra banda, com que $\overline{G}_s = \{1\}$, és $G_s = N = N_0$, de manera que la cadena de subgrups de G

$$G_0 := G \supseteq G_1 \supseteq \cdots \supseteq G_s = N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}$$

és una resolució de G. □

Corol·lari 4.5.6. *Siguin p un nombre primer i G un p-grup. Llavors, G és resoluble.*

DEMOSTRACIÓ: Sigui $\#G = p^r$, amb $r \geq 0$. Clarament, si $r = 0$, G és el grup trivial i, per tant, resoluble; i si $r = 1$, G és un grup cíclic d'ordre p; en particular, abelià i, per tant, resoluble. Suposem, doncs, que $r \geq 2$ i que tot p-grup d'ordre p^s amb $s < r$ és resoluble. Ara, el centre de G no és trivial (cf. **3.4.15**), i és un subgrup normal i abelià de G; per tant, $Z(G)$ és resoluble, i $G/Z(G)$ és un p-grup d'ordre p^s, amb $s < r$; per tant, resoluble, per hipòtesi d'inducció. Doncs, G és resoluble. □

Un objectiu important d'aquesta secció és la demostració del resultat següent.

Teorema 4.5.7. *Si $n \geq 5$, el grup simètric S_n no és resoluble.*

Lema 4.5.8. *Per a tot nombre natural $n \geq 2$, és $D(S_n) = A_n$. Per a tot nombre natural $n \geq 5$ és $D(A_n) = A_n$.*

DEMOSTRACIÓ: Clarament, tot commutador $\sigma\tau\sigma^{-1}\tau^{-1}$ descompon com a producte d'una quantitat parella de transposicions, ja que σ i σ^{-1} descomponen en el producte de la mateixa quantitat de transposicions, i τ i τ^{-1} també. És a dir, tots els commutadors pertanyen a

A_n; per tant, $D(A_n) \subseteq D(S_n) \subseteq A_n$. Recíprocament, per a $n \geq 3$, un 3-cicle (a,b,c) es pot escriure en la forma $(a,b,c) = (a,b)(a,c)(a,b)(a,c) = (a,b)(a,c)(a,b)^{-1}(a,c)^{-1}$, de manera que els 3-cicles pertanyen a $D(S_n)$; com que els 3-cicles generen A_n (cf. **3.6.7**), obtenim que, per a $n \geq 3$, és $D(S_n) = A_n$. I, per a $n = 2$, és immediat que $D(S_2) = A_2 = \{1\}$. Resta veure que, per a $n \geq 5$, és $A_n \subseteq D(A_n)$. Siguin a,b,c,d,e, diferents dos a dos; llavors, $(a,b,d)(a,c,e)(a,b,d)^{-1}(a,c,e)^{-1} = (a,b,c)$; així, tot 3-cicle (a,b,c) pertany a $D(A_n)$; això acaba la prova. □

Observació 4.5.9. Per a completar el resultat anterior, observem que $D(A_4) = V_4$, el grup de Klein, i que $D(A_3) = \{1\}$.

Corol·lari 4.5.10. *Per a $n \geq 5$, A_n no és resoluble.*

Demostració: Suposem que G és un grup resoluble, i que

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$$

és una resolució de G. Llavors, G_1 és un subgrup normal de G tal que G/G_1 és commutatiu; per tant, $D(G) \subseteq G_1$ (cf. **4.3.2**). Ara bé, com que $D(A_n) = A_n$, per a $n \geq 5$, una possible resolució de A_n no pot començar mai. Per tant, A_n no admet cap resolució. □

Demostració del teorema **4.5.7**: Com que tot subgrup d'un grup resoluble és resoluble, i com que A_n no és resoluble, per a $n \geq 5$, obtenim immediatament el teorema **4.5.7**. □

A continuació es tracta d'establir un criteri de resolubilitat per a grups finits.

Definició 4.5.11. Sigui G un grup qualsevol. Hem definit el derivat de G com el subgrup $D(G) := [G,G]$, generat pels commutadors $[g,h]$ d'elements de G. Per inducció, posem $D^0(G) := G$ i, per a tot nombre natural $n \geq 1$, definim el derivat k-èsim de G com $D^k(G) := D(D^{k-1}(G))$.

4.5.12. Recordem (cf. la proposició **4.3.2**) que el derivat d'un grup és un subgrup normal; en particular, per a un grup qualsevol G, obtenim una cadena de subgrups

$$D^0(G) = G \supseteq D(G) \supseteq D^2(G) \supseteq \cdots \supseteq D^k(G) \supseteq D^{k+1}(G) \supseteq \cdots$$

de manera que $D^{k+1}(G)$ és un subgrup normal de $D^k(G)$. De fet, es pot obtenir un resultat una mica més fort.

Proposició 4.5.13. *Sigui G un grup. Per a tot $k \geq 0$, el derivat k-èsim de G és un subgrup normal de G.*

Demostració: Podem fer la demostració per inducció sobre k. Per a això, és suficient tenir en compte que $D^0(G) = G$ i el resultat següent. □

Lema 4.5.14. *Siguin G un grup i N un subgrup normal de G. Llavors el subgrup derivat de N, $D(N)$, és un subgrup normal de G.*

Demostració: Si $\varphi : G \longrightarrow H$ és un morfisme de grups, és clar que $\varphi(D(G)) \subseteq D(H)$, perquè $D(G)$ és generat pels commutadors $[g,g']$, $g,g' \in G$, i se satisfà que $\varphi([g,g']) = [\varphi(g),\varphi(g')] \in D(H)$. En particular, per a tot morfisme de grups $\varphi : N \longrightarrow N$ tindrem que $\varphi(D(N)) \subseteq D(N)$. Però com que $N \subseteq G$ és normal, per a tot $g \in G$ podem considerar el morfisme de conjugació $\varphi_g : N \longrightarrow N$, donat per $h \mapsto g \cdot h \cdot g^{-1}$. I el fet que per a tot $g \in G$ sigui $\varphi_g(D(N)) \subseteq D(N)$ ens diu que $D(N)$ és un subgrup normal de G, com volíem demostrar. □

Proposició 4.5.15 (Criteri de resolubilitat)**.** *Sigui G un grup qualsevol. Condició necessària i suficient perquè G sigui resoluble és que existeixi $k \geq 1$ tal que $D^k(G) = \{1\}$.*

DEMOSTRACIÓ: Suposem que existeix $k \geq 1$ tal que $D^k(G) = \{1\}$ i considerem la successió $G_0 := G \supseteq D(G) \supseteq \cdots \supseteq D^k(G) = \{1\}$. Com que per a tot i, $1 \leq i \leq k$, $D^i(G) \subseteq D^{i-1}(G)$ és normal i $D^{i-1}(G)/D^i(G)$ és commutatiu, tenim que G és resoluble i la successió $D^0(G) = G \supseteq D(G) \supseteq \cdots \supseteq D^k(G) = \{1\}$ és una resolució de G.

Recíprocament, suposem que G és resoluble i sigui $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$ una resolució de G. Com que G_0/G_1 és abelià, resulta que $D(G_0) \subseteq G_1$. Per inducció, suposem que $i \geq 2$ i que $D^{i-1}(G) \subseteq G_{i-1}$; com que, per la hipòtesi de resolubilitat de G, el grup quocient G_{i-1}/G_i és abelià, resulta que $D(G_{i-1}) \subseteq G_i$. Però, a partir de la hipòtesi d'inducció, obtenim que $D^i(G) \subseteq D(G_{i-1})$ i, per tant, que $D^i(G) \subseteq G_i$. Finalment, com que $G_r = \{1\}$, tenim que $D^r(G) = \{1\}$, com calia provar. □

4.6 Grups simples

Sigui G un grup. Recordem que $\{1\}$ i G són subgrups normals de G.

Definició 4.6.1. Sigui G un grup. Es diu que el grup G és un grup simple si els únics subgrups normals de G són el trivial, $\{1\}$, i el total, G.

Proposició 4.6.2. *Els grups simples commutatius són exactament els grups cíclics d'ordre primer.*

DEMOSTRACIÓ: Clarament, si G és un grup cíclic d'ordre primer, els únics subgrups de G són els $\{1\}$ i G; per tant, G és simple (i commutatiu). Recíprocament, suposem que G és un grup commutatiu i simple. Si p és un divisor primer de l'ordre de G, en virtut del teorema de Cauchy (cf. **3.7.6**), existeix un element $g \in G$ d'ordre p; llavors, el subgrup generat per g és no trivial i normal; per tant, si G és simple, és tot G; és a dir, G és cíclic d'ordre p, primer. □

Corol·lari 4.6.3. *Siguin p un nombre primer i G un p-grup. Llavors, G és simple si, i només si, G és d'ordre p. És a dir, tot grup d'ordre p^n, amb p primer i $n \geq 2$, no és simple.*

DEMOSTRACIÓ: En efecte, el centre d'un p-grup $G \neq \{1\}$ és un subgrup no trivial de G (cf. **3.4.15**); i és normal. Per tant, si $G \neq \{1\}$ és un p-grup simple, llavors $Z(G) = G$ i G és commutatiu; per tant, cíclic d'ordre p. □

Teorema 4.6.4. *Per a tot $n \geq 5$, el grup alternat A_n és simple.*

DEMOSTRACIÓ: Suposem que $n \geq 5$ i que $N \subseteq A_n$ és un subgrup normal no trivial (és a dir, diferent de $\{1\}$). Cal veure que $N = A_n$ i, per a això, com que A_n és generat pels 3-cicles, és suficient veure que tot 3-cicle pertany a N. Ara bé, com que $n \geq 5$, tots els 3-cicles són conjugats (cf. **3.6.9**); per tant, la normalitat de N ens permet reduir la prova del teorema a veure que N conté algun 3-cicle.

Notem que si el resultat és cert, llavors N conté els 3-cicles i no pot contenir cap transposició; per tant, el màxim nombre d'elements de $\{0, 1, \ldots, n-1\}$ que són fixos per

un element $\sigma \in N$, $\sigma \neq 1$, ha de ser $n-3$, i un element $\sigma \in N$ per al qual se satisfaci la propietat ha de ser un 3-cicle. Anem, doncs, a veure això. Sigui $\sigma \in N$, $\sigma \neq 1$, un element tal que el nombre d'elements de $\{0, 1, \ldots, n-1\}$ fixos per σ sigui maximal. Anem a veure que σ és un 3-cicle i haurem acabat. Per a això, distingirem dos casos.

Primerament, suposem que σ sigui un producte de transposicions disjuntes (òbviament, en una quantitat parella), posem $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2k}$, i posem $\tau_1 =: (a, b)$, $\tau_2 =: (c, d)$, amb $a, b, c, d \in \{0, 1, \ldots, n-1\}$ i $\#\{a, b, c, d\} = 4$, i $\sigma' := \tau_3 \circ \cdots \circ \tau_{2k}$, de manera que $\sigma = (a, b) \circ (c, d) \circ \sigma'$, i σ' deixa fixos a, b, c, d. Com que $n \geq 5$, podem considerar $e \in \{0, 1, \ldots, n-1\}$ de manera que $\#\{a, b, c, d, e\} = 5$, i definir $\tau := (c, d, e) \in A_n$. Llavors, $\rho := [\tau, \sigma] = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in N$, perquè N és normal i, per tant, conté el conjugat $\sigma'' := \tau \circ \sigma \circ \tau^{-1}$ de $\sigma \in N$, i conté σ^{-1}.

Ara, notem que $\sigma'' = (\tau \circ (a, b) \circ (c, d) \circ \tau^{-1}) \circ (\tau \circ \sigma' \circ \tau^{-1}) = (a, b) \circ (d, e) \circ (\tau \circ \sigma' \circ \tau^{-1}) \neq \sigma$ (per exemple, perquè σ'' envia d a e mentre que σ envia d a c); per tant, $\rho = \sigma'' \circ \sigma^{-1} \neq 1$. D'altra banda, tot element de $\{0, 1, \ldots, n-1\}$ que sigui fix per σ i diferent de a, b, c, d, e també és fix per ρ; i, a més a més, a, b també són fixos per ρ. Això implica que la quantitat de punts fixos per $\rho \in N$, $\rho \neq 1$, és més gran que la corresponent a σ, contràriament a la hipòtesi.

Això ens duu al segon cas; en la descomposició de σ com a producte de cicles disjunts, hi ha algun cicle de longitud més gran o igual que 3; és a dir, podem escriure σ en la forma $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$, on $\tau_1, \ldots, \tau_k$ són cicles disjunts, i $\tau_1 = (a_1, a_2, \ldots, a_r)$, $r \geq 3$, amb $a_1, \ldots, a_r \in \{0, 1, \ldots, n-1\}$. Clarament, σ mou, com a mínim, a_1, a_2, $\ldots$, a_r; i si només mogués aquests elements i fos $r = 3$, ja tindríem que σ és un 3-cicle, com desitgem. En cas contrari, σ hauria de moure algun altre element de $\{0, 1, \ldots, n-1\}$; però si només en mogués un altre, hauria de ser $\sigma = (a_1, \ldots, a_4)$, que no pot ser perquè $(a_1, \ldots, a_4)$ és una permutació senar i, en conseqüència, no pertany a N. Per tant, σ mou un quart i un cinquè elements, b_4, $b_5 \in \{0, 1, \ldots, n-1\}$. Notem que, si $r = 3$, llavors podem prendre b_4, b_5 com elements moguts pel cicle τ_2; si $r = 4$, podem prendre $b_4 = a_4$ i b_5 un element mogut pel cicle τ_2; i si $r \geq 5$, podem prendre $b_4 = a_4$ i $b_5 = a_5$. En qualsevol cas, podem considerar $\tau := (a_3, b_4, b_5) \in A_n$ i, com abans, obtenim que $\rho := [\tau, \sigma] = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in N$. Ara, tenim que $\rho \neq 1$, perquè $\rho(a_3) = b_4$, i que ρ deixa més elements fixos que σ, contràriament a la hipòtesi que σ deixa fixos una quantitat maximal d'elements de $\{0, 1, \ldots, n-1\}$. En efecte, els elements que eren fixos per σ també ho són per ρ, perquè τ només mou elements que ja mou σ; però, a més a més, a_2, que no és fix per σ, ho és per ρ. Aquesta contradicció acaba la prova. □

4.7 El teorema de Jordan-Hölder

La definició de grup resoluble involucra una cadena de subgrups, cadascun normal en l'anterior; estudiem una mica més aquest tipus de cadenes.

Definició 4.7.1. Sigui G un grup. Una cadena o torre de subgrups de G és una successió finita

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$$

de subgrups de G. La cadena s'anomena normal si per a tot i, $1 \leq i \leq m$, G_i és un subgrup normal de G_{i-1}. La cadena s'anomena abeliana (respectivament, cíclica) si és

normal i per a tot i, $1 \leq i \leq m$, el grup quocient G_{i-1}/G_i és abelià (respectivament, cíclic).

Observació 4.7.2. Així, un grup resoluble és un grup per al qual existeix una cadena abeliana (finita) que acaba en el subgrup trivial.

Proposició 4.7.3. *Siguin G, H, grups, $\varphi : G \longrightarrow H$, un morfisme de grups, i suposem que $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m$ és una cadena normal de subgrups de H. Posem $G_i := \varphi^{-1}(H_i)$, $0 \leq i \leq m$. Llavors, $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$ és una cadena normal de subgrups de G. Si la cadena $\{H_i\}_{0\leq i\leq m}$ és abeliana (respectivament, cíclica), llavors la cadena $\{G_i\}_{0\leq i\leq m}$ és abeliana (respectivament, cíclica).*

Demostració: Per a $1 \leq i \leq m$, sigui $\varphi_i : G_{i-1} \longrightarrow H_{i-1}$ la restricció del morfisme φ a $G_{i-1} := \varphi^{-1}(H_{i-1})$; com que l'antiimatge d'un subgrup normal per un morfisme de grups és un subgrup normal, obtenim que $G_i = \varphi^{-1}(H_i) = \varphi_i^{-1}(H_i) \subseteq G_{i-1}$ és un subgrup normal; això prova la primera part. Ara, tenim que φ_i proporciona, per restricció i pas al quocient, un morfisme $\varphi_i' : G_{i-1} \longrightarrow H_{i-1} \longrightarrow H_{i-1}/H_i$, el nucli del qual és exactament $\varphi_i^{-1}(H_i) = G_i$; per tant, tenim que G_{i-1}/G_i s'inclou com un subgrup de H_{i-1}/H_i. Si aquest segon quocient és abelià, també ho és el primer, perquè tot subgrup d'un grup abelià és un gup abelià; i si el segon és cíclic, també ho és el primer, perquè tot subgrup d'un grup cíclic és un gup cíclic. Això proporciona la demostració volguda. □

Corol·lari 4.7.4. *Siguin G, H, grups i $\varphi : G \longrightarrow H$ un morfisme de grups. Llavors, G és resoluble si, i només si, ho són* $\ker\varphi$ *i* $\operatorname{im}\varphi$. □

Observació 4.7.5. Siguin G, H, grups i $\varphi : G \longrightarrow H$ un morfisme de grups. Llavors, si $\ker\varphi$ i H són resolubles, també ho és G. I si G ho és, també ho és $\ker\varphi$; però H no ho és necessàriament.

Definició 4.7.6. Sigui G un grup. Un refinament d'una cadena $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$ de subgrups de G és una cadena de la forma

$$G = G_0' \supseteq G_1' \supseteq \cdots \supseteq G_n' = G_m$$

tal que per a tot índex $1 \leq i \leq m$ existeix un índex j, $1 \leq j \leq n$, i $G_i = G_j'$; és a dir, que s'obté en intercalar una cadena finita de subgrups, potser cap, entre cada dos subgrups consecutius de la cadena original.

Exemple 4.7.7. Per al grup simètric S_4, la cadena $S_4 \supsetneq A_4 \supsetneq V_4 \supsetneq \{1\}$ admet el refinament (no trivial) $S_4 \supsetneq A_4 \supsetneq V_4 \supsetneq \{1, (0,1)(2,3)\} \supsetneq \{1\}$.

Corol·lari 4.7.8. *Sigui G un grup resoluble. Tot refinament d'una resolució de G és una resolució de G.* □

Proposició 4.7.9. *Sigui G un grup finit. Tota cadena abeliana de G (si existeix) admet un refinament cíclic amb quocients d'ordre primer.*

Demostració: És suficient provar que si G és un grup abelià finit, llavors G admet una cadena cíclica d'ordres primers. En efecte, podrem aplicar aquest fet a cada quocient G_{i-1}/G_i i prendre antiimatges per la projecció $G_{i-1} \longrightarrow G_{i-1}/G_i$.

Podem raonar per inducció sobre l'ordre de G; de fet, més precisament, per inducció sobre la quantitat de divisors primers, comptant-los amb les seves multiplicitats respectives, de l'ordre de G. Si G és un grup d'ordre primer, llavors $G \supseteq \{1\}$ és una cadena

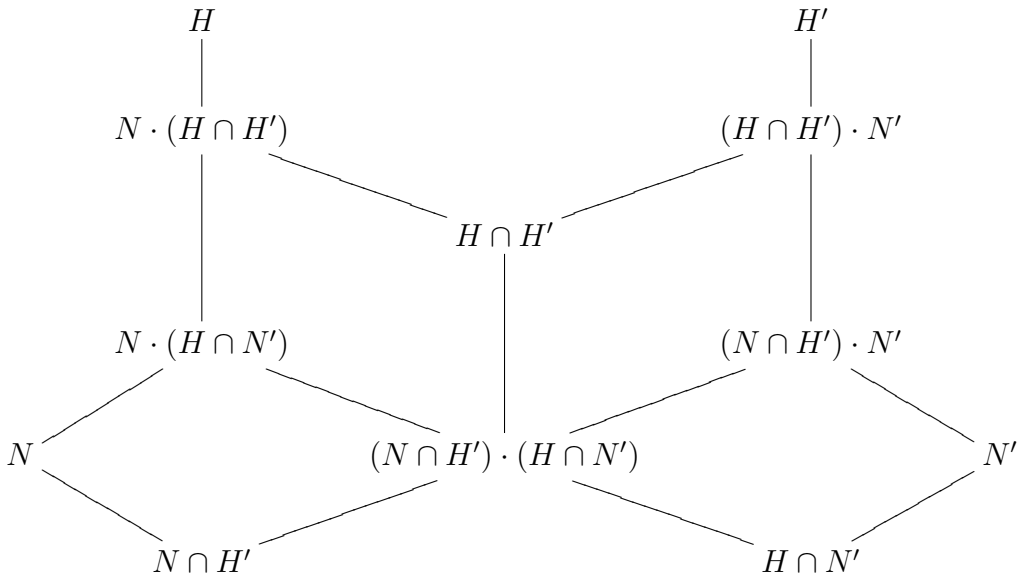
cíclica amb quocients d'ordre primer, com calia veure. En el cas general, suposem que G és un grup abelià no trivial i prenem un element $g \in G$, $g \neq 1$. Llavors, si canviem g per una potència adequada de g, obtenim que g és d'ordre primer, posem p. Llavors, en la cadena $G \supseteq \langle g \rangle \supsetneq \{1\}$, el quocient $\langle g \rangle / \{1\}$ és cíclic d'ordre primer p, mentre que el grup quocient $G/\langle g \rangle$ és abelià amb un factor primer menys al seu ordre que el grup G. Per hipòtesi d'inducció, aquest grup admet una cadena com la volguda, i podem considerar-ne l'antiimatge en G per la projecció $G \longrightarrow G/\langle g \rangle$. Aquesta cadena de G acaba en $\langle g \rangle$, i podem completar-la amb el grup trivial, de manera que la cadena completada satisfà les condicions requerides. □

Corol·lari 4.7.10. *Sigui G un grup finit. Llavors, G és resoluble si, i només si, G admet una cadena cíclica amb quocients d'ordre primer i que acaba en el subgrup trivial.* □

Teorema 4.7.11 (Teorema de Zassenhaus o lema de la papallona)**.** *Siguin G un grup, $H, H' \subseteq G$ subgrups, i $N \subseteq H$ i $N' \subseteq H'$ subgrups normals. Llavors, les inclusions $N \cdot (H \cap N') \subseteq N \cdot (H \cap H')$ i $(N \cap H') \cdot N' \subseteq (H \cap H') \cdot N'$ són subgrups normals i els grups quocients respectius són isomorfs; és a dir,*

$$\frac{N \cdot (H \cap H')}{N \cdot (H \cap N')} \cong \frac{(H \cap H') \cdot N'}{(N \cap H') \cdot N'}.$$

Demostració: Considerem el diagrama següent, d'inclusions de subgrups:



Cal notar, primerament, que els grups escrits tenen sentit com a subgrups de G. Ens mirarem el costat esquerre; el dret s'obté, anàlogament, per simetria. Com que $N \subseteq H$ és normal, H està inclòs en el normalitzador de N, de manera que $H \cap H'$ i $H \cap N'$ també i, per tant, tenen sentit els grups $N \cdot (H \cap H') = (H \cap H') \cdot N$ i $N \cdot (H \cap N') = (H \cap N') \cdot N$ (cf. **3.4.9**, **2.6.4**); a més a més, com que N és subgrup normal de H, la cadena de subgrups $N \subseteq N \cdot (H \cap N') \subseteq N \cdot (H \cap H') \subseteq H$ ens diu que N és subgrup normal de $N \cdot (H \cap H')$ i de $N \cdot (H \cap N')$. En particular, té sentit considerar els grups quocient $\dfrac{N \cdot (H \cap H')}{N}$ i $\dfrac{N \cdot (H \cap N')}{N}$.

D'altra banda, $(N \cap H') \cdot (H \cap N')$ és un subgrup de $H \cap H'$, i és normal, perquè els dos subgrups $N \cap H'$ i $H \cap N'$ de $H \cap H'$ són normals. En particular, té sentit considerar el grup

quocient $\dfrac{H\cap H'}{(N\cap H')\cdot(H\cap N')}$. Volem veure que els dos grups quocients $\dfrac{N\cdot(H\cap H')}{N\cdot(H\cap N')}$ i $\dfrac{(H\cap H')\cdot N'}{(N\cap H')\cdot N'}$ són isomorfs; i ho farem veient que cadascun és isomorf al grup quocient $\dfrac{H\cap H'}{(N\cap H')\cdot(H\cap N')}$.

Per a això, considerem el morfisme de grups $\pi : H\cap H' \longrightarrow \dfrac{N\cdot(H\cap H')}{N}$, composició de la inclusió $H\cap H' \longrightarrow N\cdot(H\cap H')$ amb la projecció $N\cdot(H\cap H') \longrightarrow \dfrac{N\cdot(H\cap H')}{N}$. Clarament, π és exhaustiu i el seu nucli és la intersecció $N\cap(H\cap H') = N\cap H'$. Ara, notem que el subgrup normal $(N\cap H')\cdot(H\cap N') \subseteq H\cap H'$ conté el nucli anterior, de manera que, en virtut de **2.5.14**, tenim un isomorfisme de grups

$$\frac{H\cap H'}{(N\cap H')\cdot(H\cap N')} \cong \frac{\pi(H\cap H')}{\pi((N\cap H')\cdot(H\cap N'))}.$$

Com que π és exhaustiu, tenim que $\pi(H\cap H') = \dfrac{N\cdot(H\cap H')}{N}$; i, d'altra banda, tenim que $\pi((N\cap H')\cdot(H\cap N')) = \dfrac{N\cdot((N\cap H')\cdot(H\cap N'))}{N} = \dfrac{N\cdot(H\cap N')}{N}$. En virtut del tercer teorema d'isomorfia (**2.6.4**), obtenim que

$$\frac{H\cap H'}{(N\cap H')\cdot(H\cap N')} \cong \frac{N\cdot(H\cap H')}{N\cdot(H\cap N')}.$$

Efectivament, la normalitat de $(N\cap H')\cdot(H\cap N')$ en $H\cap H'$ i l'exhaustivitat de π impliquen la normalitat de $\dfrac{N\cdot(H\cap N')}{N}$ com a subgrup de $\dfrac{N\cdot(H\cap H')}{N}$ i, per tant, la de $N\cdot(H\cap N')$ com a subgrup de $N\cdot(H\cap H')$; i, en conseqüència, podem aplicar el tercer teorema d'isomorfia i concloure.

L'altre isomorfisme,

$$\frac{H\cap H'}{(N\cap H')\cdot(H\cap N')} \cong \frac{(H\cap H')\cdot N'}{(N\cap H')\cdot N'},$$

s'obté, anàlogament, per simetria. □

Definició 4.7.12. Sigui G un grup. Dues cadenes normals de G que s'acabin en el neutre,

$$G = H_0 \supseteq H_1 \supsetneq \cdots \supsetneq H_n = \{1\}, \qquad G = H'_0 \supseteq H'_1 \supsetneq \cdots \supsetneq H'_m = \{1\},$$

s'anomenen equivalents si $m = n$ i existeix una permutació $\sigma \in S_n$ tal que per a tot $i \in \{0, 1, \ldots, n-1\}$ és

$$\frac{H_i}{H_{i+1}} \cong \frac{H'_{\sigma(i)}}{H'_{\sigma(i)+1}}.$$

És a dir, si, llevat de l'ordre, els quocients consecutius de l'una i de l'altra són isomorfs.

Teorema 4.7.13 (Schreier)**.** *Sigui G un grup qualsevol. Dues cadenes normals de G que acabin en el neutre admeten refinaments equivalents.*

DEMOSTRACIÓ: Siguin

$$G =: H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\},$$

$$G = H'_0 \supseteq H'_1 \supseteq \cdots \supseteq H'_m = \{1\},$$

cadenes normals de G. Posem

$$H_{i,j} := H_{i+1} \cdot (H_i \cap H'_j), \qquad 0 \leq i \leq n-1, \quad 0 \leq j \leq m,$$

$$H'_{j,i} := (H_i \cap H'_j) \cdot H'_{j+1}, \qquad 0 \leq i \leq n, \quad 0 \leq j \leq m-1.$$

Com que $H_{i+1} \subseteq H_i$, $0 \leq i \leq n-1$, i $H'_{j+1} \subseteq H'_j$, $0 \leq j \leq m-1$, són subgrups normals, els grups $H_{i,j}$ i $H'_{j,i}$ tenen sentit i estem en la situació del lema de la papallona (cf. **4.7.11**); per tant, obtenim que, per a $0 \leq i \leq n-1$, $0 \leq j \leq m-1$, $H_{i,j+1} \subseteq H_{i,j}$ és un subgrup normal, $H'_{j,i+1} \subseteq H'_{j,i}$ és un subgrup normal, i

$$\frac{H_{i,j}}{H_{i,j+1}} \cong \frac{H'_{j,i}}{H'_{j,i+1}}, \qquad 0 \leq i \leq n-1, \quad 0 \leq j \leq m-1.$$

Ara, notem que, per a $0 \leq i \leq n-1$ i $0 \leq j \leq m-1$ és $H_{i,0} = H_i$, i $H_{i,m} = H_{i+1}$, de manera que obtenim un refinament

$$H_i = H_{i,0} \supseteq H_{i,1} \supseteq \cdots \supseteq H_{i,m-1} \supseteq H_{i,m} = H_{i+1},$$

de la cadena $H_i \supseteq H_{i+1}$. Si els posem un darrere l'altre, per a $0 \leq i \leq n-1$, obtenim un refinament de la cadena $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\}$ format per $n \cdot m$ inclusions.

Anàlogament, per a $0 \leq i \leq n-1$ i $0 \leq j \leq m-1$ és $H'_{j,0} = H'_j$, i $H'_{j,n} = H'_{j+1}$, de manera que obtenim un refinament

$$H'_j = H'_{j,0} \supseteq H'_{j,1} \supseteq \cdots \supseteq H'_{j,n-1} \supseteq H'_{j,n} = H'_{j+1},$$

de la cadena $H'_j \supseteq H'_{j+1}$. I de nou, si els posem un darrere l'altre, per a $0 \leq j \leq m-1$, obtenim un refinament de la cadena $G = H'_0 \supseteq H'_1 \supseteq \cdots \supseteq H'_m = \{1\}$ format per $n \cdot m$ inclusions.

Així, tenim dues cadenes normals de G, que s'acaben totes dues en el grup trivial, formades per $n \cdot m$ inclusions cadascuna, i de manera que els grups quocients es poden aparellar per isomorfismes:

$$\frac{H_{i,j}}{H_{i,j+1}} \cong \frac{H'_{j,i}}{H'_{j,i+1}}, \qquad 0 \leq i \leq n-1, \quad 0 \leq j \leq m-1,$$

com calia demostrar. □

Definició 4.7.14. Una sèrie de composició per a un grup G és una cadena normal que acaba en el subgrup trivial $\{1\}$ i tal que tots els quocients són grups simples no trivials.

Observació 4.7.15. No és cert que tots els grups admetin una sèrie de composició. Per exemple, considerem $G = \mathbb{Z}$, el grup additiu dels nombres enters. Tot subgrup no trivial és de la forma $n\mathbb{Z}$, i no és simple, de manera que una hipotètica sèrie de composició, que hauria d'acabar en la forma $n\mathbb{Z} \supsetneq \{0\}$, no té el darrer quocient simple.

Proposició 4.7.16. *Tot grup finit admet alguna sèrie de composició.*

DEMOSTRACIÓ: Prenem $G_0 := G$; si $G = \{1\}$, ja hem acabat. Si $G \neq \{1\}$, sigui G_1 un subgrup normal maximal de G; és a dir, un subgrup normal tal que $G \supsetneq G_1$ i que G/G_1 no admeti subgrups normals no trivials. Llavors, l'ordre de G_1 és menor estricte que l'ordre de G i podem raonar per inducció. □

Teorema 4.7.17. (Jordan-Hölder) *Dues sèries de composició d'un mateix grup, si existeixen, són equivalents.*

DEMOSTRACIÓ: Considerem dues sèries de composició per a un grup G. En virtut del teorema de Schreier (cf. **4.7.13**), cadascuna admet un refinament de manera que els dos refinaments són equivalents. Ara bé, un refinament d'una sèrie de composició només es pot obtenir en afegir subgrups que ja hi ha a la cadena, perquè els quocients successius d'una sèrie de composició són simples. D'altra banda, l'equivalència entre els dos refinaments proporciona una bijecció entre tots els quocients d'una cadena i tots els de l'altra de tal manera que els quocients que es corresponen per la bijecció són grups isomorfs. En particular, els quocients trivials d'un refinament estan en bijecció amb els quocients trivials de l'altre; per tant, els altres, que són els simples, també estan en bijecció. Això és, l'equivalència estableix una bijecció entre els quocients de les cadenes originals; i això és dir que les cadenes originals són equivalents. □

Observació 4.7.18. No és cert, ni tan sols per a grups finits, que si dos grups admeten sèries de composició equivalents llavors els grups siguin isomorfs. Per exemple, es pot demostrar fàcilment (és un fet que es proposa com a exercici) que si p és un nombre primer, llavors dos p-grups qualssevol del mateix ordre, p^n, admeten sèries de composició formades per n quocients cíclics d'ordre p. Per exemple, un grup cíclic d'ordre 4 i un producte cartesià de dos grups cíclics d'ordre 2 admeten una sèrie de composició de la forma $G \supsetneq C \supsetneq \{1\}$, on tots els quocients són grups cíclics d'ordre 2.

Corol·lari 4.7.19. *Un grup finit G és resoluble si tots els quocients d'una sèrie de composició per a G són cíclics d'ordre primer.* □

4.8 Grups de simetries

Per a acabar aquest capítol dedicat a grups, farem una pinzellada a l'estudi de grups de simetries d'objectes geomètrics.

En un curs de geomeria lineal se solen esudiar els desplaçaments dels espais euclidians de dimensions 2 o 3. Això implica l'estudi, explícit o implícit, dels grups ortogonals o ortogonals especials de dimensions 2 o 3 sobre el cos $\mathbb{R}$ dels nombres reals. Recordem-ne les definicions.

Definició 4.8.1. Per a tot nombre natural $n \geq 1$, considerem l'anell $\mathbf{M}(n, \mathbb{R})$ (no commutatiu si $n > 1$), de les matrius quadrades de n files i n columnes i coeficients en $\mathbb{R}$ (cf. el darrer dels exemples en **1.6.6**). Per a una matriu A, indiquem per A^t la seva transposada. Considerem, també, els grups següents, de matrius invertibles:

$$\mathbf{GL}(n, \mathbb{R}) := \{A \in \mathbf{M}(n, \mathbb{R}) : \det A \in \mathbb{R}^*\}, \qquad \text{grup lineal general;}$$

$$\mathbf{SL}(n,\mathbb{R}) := \{A \in \mathbf{GL}(n,\mathbb{R}) : \det A = 1\}, \qquad \text{grup lineal especial;}$$

$$\mathbf{O}(n,\mathbb{R}) := \{A \in \mathbf{GL}(n,\mathbb{R}) : A^{-1} = A^t\}, \qquad \text{grup ortogonal;}$$

$$\mathbf{SO}(n,\mathbb{R}) := \{A \in \mathbf{O}(n,\mathbb{R}) : \det A = 1\}, \qquad \text{grup ortogonal especial.}$$

Notem que $\mathbf{SL}(n,\mathbb{R}) \subseteq \mathbf{GL}(n,\mathbb{R})$ i $\mathbf{SO}(n,\mathbb{R}) \subseteq \mathbf{O}(n,\mathbb{R})$ són subgrups normals, perquè coincideixen amb el nucli del morfisme determinant corresponent:

$$\det : \mathbf{GL}(n,\mathbb{R}) \longrightarrow \mathbb{R}^*, \qquad \det : \mathbf{O}(n,\mathbb{R}) \longrightarrow \{\pm 1\} \subseteq \mathbb{R}^*.$$

I que $\mathbf{SO}(n,\mathbb{R}) = \mathbf{O}(n,\mathbb{R}) \cap \mathbf{SL}(n,\mathbb{R})$.

4.8.2. Considerem el grup especial ortogonal $\mathbf{SO}(3,\mathbb{R})$, de les rotacions de l'espai euclidià 3-dimensional. En particular, aquest grup conté un subgrup isomorf al grup $\mathbf{SO}(2,\mathbb{R})$, de les rotacions del pla euclidià, i també conté un subgrup isomorf al grup ortogonal $\mathbf{O}(2,\mathbb{R})$, de les rotacions i simetries del pla (els desplaçaments o isometries). De fet, una simetria respecte d'una recta del pla es pot considerar com la restricció d'una rotació, a l'espai, d'angle π i d'eix la recta de simetria. Un teorema no gens difícil de demostrar, però una mica entretingut (cf., per exemple, [Artin 1991], cap. 5, sec. 9, theorem (9.1)), descriu els subgrups finits del grup $\mathbf{SO}(3,\mathbb{R})$. El resultat es pot enunciar com segueix.

Teorema 4.8.3. *Sigui $G \subseteq \mathbf{SO}(3,\mathbb{R})$ un subgrup finit. Llavors, G és d'un dels tipus següents:*

(a) *$G \cong C_n$, un grup cíclic d'ordre n; es pot pensar com el grup de les rotacions respecte d'un eix i que deixen fix un n-àgon regular en el pla perpendicular a l'eix amb baricentre en el punt d'intersecció de l'eix i el pla* (*cf.* **4.4.7**).

(b) *$G \cong D_{2\cdot n}$, un grup diedral d'ordre $2n$; es pot pensar com el grup dels desplaçaments d'un pla que deixen fix un n-àgon regular en aquell pla* (*cf.* **4.4.7**).

(c) *El grup tetraèdric, de les rotacions de l'espai que deixen fix un tetràedre regular.*

(d) *El grup octaèdric, de les rotacions de l'espai que deixen fix un octàedre regular, o bé un cub.*

(e) *El grup icosaèdric, de les rotacions de l'espai que deixen fix un icosàedre regular, o bé un dodecàedre regular.* □

Observació 4.8.4. Notem que els objectes geomètrics que apareixen en aquest enunciat són exactament els polígons regulars (convexos) del pla, i els políedres regulars (convexos), de l'espai tridimensional; o sigui, els anomenats sólids platònics.

D'altra banda, observem que si considerem els políedres duals, és a dir, els que tenen vèrtexs en els baricentres de les cares i arestes que uneixen vèrtexs que corresponen a cares adjacents, el tetràedre és autodual, el cub i l'octàedre són duals l'un de l'altre, i el dodecàedre i l'icosàedre també són duals l'un de l'altre. I a políedres duals els correspon el mateix grup.

Es tracta, ara, de descriure els grups tetraèdric, octaèdric i icosaèdric; és a dir, de determinar-ne la classe d'isomorfia corresponent.

Proposició 4.8.5. *El grup tetraèdric és isomorf al grup alternat A_4.*

Demostració: És clar que tota rotació de l'espai que deixi fix un tetràedre regular proporciona una permutació dels quatre vèrtexs. Això proporciona una acció del grup tetraèdric en el conjunt dels quatre vèrtexs i, per tant, un morfisme del grup tetraèdric en S_4. Ara, notem que si una rotació deixa fixos dos dels vèrtexs, ha de ser una rotació d'eix l'aresta que els uneix; i l'única rotació que deixa fix un tetràedre i una de les seves arestes és la identitat. Això demostra que el morfisme anterior és injectiu (l'ùnica rotació que deixa fixos tots quatre vèrtexs és la identitat), i també que cap transposició no pertany a la imatge. En particular, el grup tetraèdric s'identifica amb un subgrup de S_4.

D'altra banda, per a cada vèrtex, tenim dues rotacions (d'un terç de volta en cada sentit) d'eix que conté el vèrtex i el baricentre del triangle oposat; i per a cada parella d'arestes oposades disposem de la rotació de mitja volta i eix que passa pels baricentres de les dues arestes. Això fa un total de 12 rotacions, que és molt senzill identificar amb les permutacions de A_4. Així, A_4 és un subgrup de la imatge del morfisme; i com que aquesta imatge no conté cap transposició, ha de ser exactament A_4. Això acaba la prova. □

Proposició 4.8.6. *El grup octaèdric és isomorf al grup simètric S_4.*

Demostració: Una rotació de l'espai que deixi fix un cub ha de permutar les quatre diagonals del cub; això proporciona una acció del grup octaèdric en el conjunt de les quatre diagonals i, per tant, un morfisme del grup octaèdric en S_4. Ara, notem que si una rotació deixa fixes dues diagonals, també deixa fix el pla que les conté i, per tant, és una rotació d'eix ortogonal a aquest pla. En particular, si una rotació ρ deixa fixes les quatre diagonals, deixa fixos els sis plans que aquestes diagonals determinen dues a dues, i l'eix de la rotació ρ és ortogonal a aquests sis plans; com que no són plans paral·lels, la rotació ρ és la identitat. Això demostra que el morfisme del grup octaèdric en S_4 és injectiu.

Ara, és clar que una rotació d'un quart de volta i eix la recta que uneix els baricentres de dues cares oposades del cub permuta cíclicament les quatre diagonals; per tant, el grup octaèdric conté un cicle d'ordre 4. I una rotació de mitja volta i eix que passi pels baricentres de dues arestes oposades transposa les dues diagonals que corresponen a aquestes arestes i deixa fixes les altres dues. Això fa que el grup octaèdric contingui (amb una numeració conveninet de les diagonals) les dues permutacions $(0,1,2,3)$ i $(0,1)$; com que aquestes generen S_4 (cd. **3.5.18**), el grup octaèdric s'identifica amb S_4. □

Proposició 4.8.7. *El grup icosaèdric és isomorf al grup alternat A_5.*

Demostració: El grup icosaèdric actua en el conjunt de les 12 cares del dodecàedre i l'acció és transitiva; és a dir, hi ha una única òrbita, i és de cardinal 12. El grup d'isotropia d'una de les cares és format per les rotacions que deixen fixa aquesta cara; és a dir, per les 5 rotacions d'eix ortogonal a la cara en el seu baricentre i amplituds múltiples d'un cinquè de volta. Per tant, com que el cardinal de l'òrbita coincideix amb l'índex del grup d'isotropia, tenim que aquest índex és 12, i com que l'ordre del grup d'isotropia és 5, obtenim que el grup icosaèdric és d'ordre 60.

Cada parella de vèrtexs no adjacents d'una cara del dodecàedre determina unívocament un cub inscrit en el dodecàedre, amb vèrtexs en vèrtexs del dodecàedre. Per a veure-ho, siguin C_1 una cara, a i d dos vèrtexs no adjacents de C_1, i considerem en C_1 l'aresta bc paral·lela a la diagonal ad de C_1. Aquesta aresta bc ho és d'una altra cara, C_2, del dodecàedre, i podem considerar en C_2 la diagonal $a'd'$ paral·lela a aquesta aresta. Les quatre diagonals del dodecàedre que contenen els punts a, a', d', d són les diagonals d'un cub inscrit en el dodecàedre, determinat unívocament per a, d. Notem que cada cara del dodecàedre conté una, i només una, de les arestes del cub. Com a conseqüència, el nombre de cubs inscrits en el dodecàedre és exactament el nombre de parelles de vèrtexs no adjacents a cada cara; és a dir, exactament 5.

Ara, observem que una rotació que deixi fix el dodecàedre ha de permutar aquests cinc cubs; això proporciona una acció del grup icosaèdric en el conjunt dels cinc cubs i, per tant, un morfisme del grup icosaèdric en el grup simètric S_5. Veiem que aquest morfisme és injectiu. Suposem, doncs, que una rotació, ρ, restringida al conjunt dels cinc cubs, és la identitat; és a dir, que ρ deixa invarinats tots cinc cubs. En particular, els dos cubs que contenen el vèrtex a són invariants per ρ i, per tant, ho és la intersecció dels dos cubs, i la intersecció dels dos cubs amb el dodecàedre, que és exactament la diagonal del dodecàedre que conté a. Així, ρ deixa invariants les cinc diagonals del dodecàedre determinades pels vèrtexs de la cara C_1. Això implica que ρ deixa invariants els cinc plans que les diagonals determinen dues a dues i, per tant, que ρ és la identitat i el morfisme és injectiu.

Per a acabar, només cal notar que qualsevol subgrup d'ordre 60 del grup simetric S_5 és d'index 2 i, per tant, és el grup alternat A_5 (cf. **4.8.8**). Això acaba la demostració. □

Observació 4.8.8. Efectivament, el grup alternat A_5 és l'únic subgrup de S_5 d'ordre 60 o, equivalentment, d'índex 2, perquè un tal grup seria normal, amb quocient abelià i, per tant, estaria inclòs en el derivat de S_5, que és A_5; i aquest subgrup de A_5 és del mateix ordre que A_5.

Capítol 5

Anells

Si una estructura algebraica ens és familiar, encara que no l'haguem formalitzada ni estudiada des del punt de vista estructural, és la d'anell. De fet, ja des dels primers passos en l'aprenentatge, aprenem a sumar, restar i multiplicar nombres i, de seguida, a dividir-los. I, a més a més, aprenem les propietats bàsiques d'aquestes operacions; és a dir, l'estructura d'anell del conjunt dels nombres enters. I, després, quan estudiem els nombres "decimals", aprenem l'estructura de cos dels conjunts dels nombres racionals o reals. Aquest capítol es dedica a un estudi formal més profund de la teoria bàsica d'anells.

5.1 Anells, morfismes, subanells

Definició 5.1.1. Recordem que hem definit un anell $(A, +, \cdot, 0, 1, -)$ (cf. **1.6.5**) com un conjunt A amb dues operacions binàries, $+$, anomenada suma, i $\cdot$, anomenat producte, dues operacions 0-àries, 0 i 1, i una operació 1-ària, $-$, l'oposat per a la suma, de manera que $(A, +, 0, -)$ és un grup commutatiu, que el producte és associatiu, i amb neutre 1, anomenat unitat, i que és distributiu per l'esquerra i per la dreta respecte de la suma. Si, a més a més, el producte és commutatiu, es parla d'un anell commutatiu. Els axiomes d'anell són, doncs, els següents:

(a) per a tot $a, b, c \in A$ és $a + (b + c) = (a + b) + c$;

(b) per a tot $a \in A$ és $a + 0 = 0 + a = a$;

(c) per a tot $a \in A$ és $a + (-a) = (-a) + a = 0$;

(d) per a tot $a, b \in A$ és $a + b = b + a$;

(e) per a tot $a, b, c \in A$ és $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(f) per a tot $a \in A$ és $a \cdot 1 = 1 \cdot a = a$;

(g) per a tot $a, b, c \in A$ és $a \cdot (b + c) = a \cdot b + a \cdot c$;

(h) per a tot $a, b, c \in A$ és $(a + b) \cdot c = a \cdot c + b \cdot c$.

I l'anell és commutatiu si, i només si, se satisfà, a més a més, que per a tot $a, b \in A$ és $a \cdot b = b \cdot a$.

Observació 5.1.2. Notem que si A és un anell i $a \in A$, llavors $a \cdot 0 + a \cdot 0 = a \cdot (0+0) = a \cdot 0 = a \cdot 0 + 0$, de manera que $a \cdot 0 = 0$. Anàlogament, per a tot $a \in A$, és $0 \cdot a = 0$. En particular, en un anell és $1 = 0$ si, i només si, $A = \{0\}$; és a dir, si A és un anell amb un sol element.

Exemples 5.1.3. • Com a exemples bàsics, podem considerar l'anell dels nombres enters, $\mathbb{Z}$, l'anell dels nombres racionals, $\mathbb{Q}$, l'anell dels nombres reals, $\mathbb{R}$, o l'anell dels nombres complexos, $\mathbb{C}$; tots aquests anells són commutatius.

• Uns altres exemples molt importants d'anells són els anells de classes de residus, $\mathbb{Z}/n\mathbb{Z}$ (cf., més endavant, **5.5.22** per a la definició de l'anell quocient en general). En els grups abelians additius $\mathbb{Z}/n\mathbb{Z}$, $n \geq 0$, podem definir l'operació producte de manera que la projecció canònica, $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, o sigui, el morfisme de grups abelians de reducció mòdul n, també sigui un morfisme per a l'operació producte així definida: és a dir, podem definir $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (a \cdot b) + n\mathbb{Z}$, per a $a, b \in \mathbb{Z}$. Aquesta definició no depèn dels representants elegits en les classes i proporciona, juntament amb l'element $1 + n\mathbb{Z}$ com a element neutre per a la multiplicació, una estructura natural d'anell en $\mathbb{Z}/n\mathbb{Z}$.

• Per a tot $n \geq 1$, tenim els anells de matrius de coeficients enters, racionals, reals o complexos, $\mathbf{M}(n;\mathbb{Z})$, $\mathbf{M}(n;\mathbb{Q})$, $\mathbf{M}(n;\mathbb{R})$, $\mathbf{M}(n;\mathbb{C})$, que no són commutatius per a $n \geq 2$.

• Més generalment, donats un anell qualsevol A, no necessàriament commutatiu, i un nombre enter $n \geq 1$, podem considerar l'anell de les matrius quadrades de n files i n columnes i coeficients en A, $\mathbf{M}(n;A)$. Si $n \geq 2$ i $A \neq \{0\}$, aquest anell no és commutatiu, encara que A sigui commutatiu. Per exemple, per a $M := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $N := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, és

$$M \cdot N = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} = N \cdot M.$$

• Un altre exemple clàssic d'anell, en general no commutatiu, és l'anell dels endomorfismes d'un grup abelià G, $\mathrm{End}(G)$, amb la suma i la composició de morfismes de grups.

• (L'anell de grup) Donat un grup qualsevol, G, podem considerar l'anell de grup, $\mathbb{Z}[G]$, definit de la manera següent. Considerem, en el grup $\mathbb{Z}[G] := \bigoplus_{g \in G} \mathbb{Z} \cdot g$, abelià lliure de base G, el producte definit per la fórmula

$$\left(\sum_{g \in F_1} n_g \cdot g \right) \cdot \left(\sum_{g' \in F_2} m_{g'} \cdot g' \right) := \left(\sum_{g \in F_1,\, g' \in F_2} (n_g \cdot m_{g'}) \cdot (g \cdot g') \right), \qquad n_g, m_{g'} \in \mathbb{Z},$$

on F_1, $F_2 \subseteq G$ són subconjunts finits. Llavors, $\mathbb{Z}[G]$ és un anell, commutatiu si ho és G com a grup, i amb element unitat l'element neutre de G.

• Siguin A un anell i X qualsevol conjunt no buit. En el conjunt A^X, de les aplicacions de X en A, hi ha una única estructura d'anell per a la qual la suma i el producte d'aplicacions $f, g \in A^X$ són donats per $(f+g)(x) := f(x) + g(x)$ i $(f \cdot g)(x) := f(x) \cdot g(x)$, per a tot $x \in X$; els elements neutres corresponents són les aplicacions $0 : X \longrightarrow A$ i $1 : X \longrightarrow A$ donades per $0(x) := 0$, $1(x) := 1$, per a tot $x \in X$; és a dir, les aplicacions constants de valors 0 i 1, respectivament. L'anell A^X és commutatiu si, i només si, A ho és.

• En particular, Per a $X = \mathbb{N}$, el conjunt dels nombres naturals, tenim l'anell de les aplicacions $s : \mathbb{N} \longrightarrow A$; és a dir, l'anell de les successions d'elements de A.

Definició 5.1.4. Recordem que, donats anells A, B, un morfisme d'anells de A en B és una aplicació $\varphi : A \longrightarrow B$ que és morfisme per a totes les operacions d'anell, i que és suficient la comprovació que $\varphi(1) = 1$ i que per a tota parella d'elements $a, b \in A$ és $\varphi(a + b) = \varphi(a) + \varphi(b)$ i $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ (cf. **2.2.2**).

Observació 5.1.5. Així com les condicions $\varphi(0) = 0$ i $\varphi(-a) = -\varphi(a)$ es dedueixen de la condició sobre la suma i del fet que A i B són grups amb la suma, no succeeix el mateix per a la condició $\varphi(1) = 1$; cal imposar-la, perquè no es dedueix dels axiomes d'anell de A i de B.

Per exemple, si considerem l'aplicació $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ donada per $\varphi(n) := (n, 0)$, és clar que se satisfà que $\varphi(m + n) = \varphi(m) + \varphi(n)$ i que $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, però no és $\varphi(1) = 1$, perquè l'element neutre del producte de $\mathbb{Z} \times \mathbb{Z}$ és $1 = (1, 1) \neq (1, 0) = \varphi(1)$; per tant, aquesta aplicació φ no és un morfisme d'anells, tot i que sí que és morfisme dels grups additius. Per a la definició de l'anell producte, cf., més endavant, **5.4.1**.

Exemples 5.1.6. • Per a tot anell A, la identitat $\mathrm{id}_A : A \longrightarrow A$, definida per $a \mapsto a$, és un morfisme d'anells. S'anomena el morfisme identitat o idèntic de l'anell A.

• Siguin A, B, C anells i $\varphi : A \longrightarrow B$, $\psi : B \longrightarrow C$ morfismes d'anells. Llavors, l'aplicació composició $\psi \circ \varphi : A \longrightarrow C$, donada per $(\psi \circ \varphi)(a) := \psi(\varphi(a))$, és un morfisme d'anells.

• Per a tot nombre enter $n \geq 0$, la projecció canònica (o reducció mòdul n) $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ és un morfisme d'anells; de fet, les operacions de $\mathbb{Z}/n\mathbb{Z}$ s'han definit de manera que aquesta projecció sigui un morfisme d'anells.

Definició 5.1.7. Recordem que un morfisme d'anells $\varphi : A \longrightarrow B$ és un isomorfisme si, i només si, admet un morfisme invers; és a dir, si existeix un morfisme d'anells $\psi : B \longrightarrow A$ tal que $\psi \circ \varphi = \mathrm{id}_A$ i $\varphi \circ \psi = \mathrm{id}_B$. Se satisfà que els isomorfismes d'anells són exactament els morfismes bijectius d'anells. En particular, la identitat és un isomorfisme i la composició d'isomorfismes és un isomorfisme.

Definició 5.1.8. Un subanell d'un anell A és un subconjunt $B \subseteq A$ al qual es poden restringir totes les operacions de A i tal que per a aquestes restriccions B és un anell. Així, cal que la suma i el producte d'elements de B pertanyin a B, que els neutres de A pertanyin a B, i que els oposats dels elements de B pertanyin a B. Si se satisfan aquestes condicions, les propietats d'anell se satisfan automàticament, perquè se satisfan per a tots els elements de A. Notem que si A és commutatiu, llavors B també és commutatiu; però pot ser que B sigui commutatiu sense que A ho sigui.

Observació 5.1.9. En particular, A és un subanell de A; però si $A \neq \{0\}$, llavors l'anell $\{0\}$ no és un subanell de A, perquè no podem restringir 1 a $\{0\}$, ja que $1 \neq 0$.

Exercici 5.1.10. Siguin A, B anells i $\varphi : A \longrightarrow B$ un morfisme d'anells. Llavors, $\operatorname{im}\varphi$ és un subanell de B. Més generalment, per a tot subanell $A' \subseteq A$, la seva imatge per φ, $\varphi(A') \subseteq B$, és un subanell, tant de B com de $\operatorname{im}\varphi$.

Exercici 5.1.11. Els subanells d'un anell A són exactament les imatges dels morfismes d'anells $\varphi : B \longrightarrow A$, per a tots els anells B per als quals n'existeixi algun.

Exercici 5.1.12. Si A és un anell i $\{B_i\}_{i \in I}$ és una família no buida de subanells $B_i \subseteq A$, $i \in I$, la seva intersecció, $\bigcap_{i \in I} B_i \subseteq A$, és un subanell de A.

Definició 5.1.13. Si A és un anell qualsevol, el centre de A és el subconjunt format per tots els elements $a \in A$ tals que per a tot element $b \in A$ és $a \cdot b = b \cdot a$. El centre de A és un subanell de A, i és commutatiu.

Exercici 5.1.14. Siguin K un anell commutatiu i $n \geq 1$ un nombre natural, i considerem l'aplicació $\psi : K \longrightarrow \mathbf{M}(n; K)$ definida, per a tot $a \in K$, per $\psi(a) := a \cdot 1$, on 1 denota la matriu identitat de $\mathbf{M}(n; K)$. Llavors, ψ és un morfisme injectiu d'anells que identifica K amb el centre de l'anell $\mathbf{M}(n; K)$.

Exercici 5.1.15. Sigui $\psi : \mathbb{C} \longrightarrow \mathbf{M}(2; \mathbb{R})$ l'aplicació definida per $\psi(a + bi) := \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, per a $a, b \in \mathbb{R}$. Llavors ψ és un morfisme injectiu d'anells; per tant, ψ identifica $\mathbb{C}$ amb un subanell de $\mathbf{M}(2; \mathbb{R})$.

Exercici 5.1.16. Siguin G un grup i $H \subseteq G$ un subgrup. Llavors, l'anell de grup $\mathbb{Z}[H]$ és un subanell de $\mathbb{Z}[G]$.

5.2 Elements invertibles. Cossos

Tot i que tots els elements d'un anell admeten un invers per a la suma, només alguns elements admeten invers per al producte. En altres paraules, si A és un anell, tot element $x \in A$ és part d'una solució, $(x, -x)$, de l'equació $X + Y = 0$. L'equació equivalent per al producte és l'equació $X \cdot Y = 1$, ja que 1 és l'element neutre per al producte, com 0 ho és per a la suma. Però no és cert que tots els elements $x \in A$ siguin part d'una solució d'aquesta darrera equació.

Definició 5.2.1. Sigui A un anell. Un element $a \in A$ s'anomena invertible, o també es diu que a és una unitat de A, si existeix un element $b \in A$ tal que $a \cdot b = b \cdot a = 1$; això és dir que a admet un invers per la dreta i per l'esquerra per a l'operació producte i per al neutre 1 (cf. **1.4.5**).

Observació 5.2.2. Si per a algun element $a \in A$ existeix $b \in A$ tal que $a \cdot b = b \cdot a = 1$, llavors l'element b és únic, i s'anomena l'invers de a. De fet, només cal que a admeti un invers per la dreta, b, i un invers per l'esquerra, b'; llavors, $b = b'$ i és un element invers de a. En efecte, si b', $b \in A$ són tals que $a \cdot b = b' \cdot a = 1$, llavors $b' = b' \cdot 1 = b' \cdot (a \cdot b) = (b' \cdot a) \cdot b = 1 \cdot b = b$, perquè l'operació producte és associativa i admet 1 com a element neutre.

Observació 5.2.3. Sigui A un anell, i considerem $A^* := \{a \in A : a \text{ és invertible}\}$, el subconjunt dels elements invertibles de A. Clarament, $1 \in A^*$; a més a més, per a $a, b \in A^*$ és $a \cdot b \in A^*$, ja que $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = 1$, de manera que $b^{-1} \cdot a^{-1}$ és l'invers de l'element $a \cdot b$; i per a $a \in A^*$, és $a^{-1} \in A^*$ i $(a^{-1})^{-1} = a$. Això ens diu que A^* té una estructura de grup (commutatiu, si A és un anell commutatiu) determinada unívocament pel producte de A; s'anomena el grup multiplicatiu de l'anell A. També se'l denota per $\mathbf{GL}(1, A)$ (matrius invertibles 1×1 de coeficients en A).

Observació 5.2.4. Sigui A un anell. El conjunt dels elements de A que admeten un invers per l'esquerra (o per la dreta) no té per què ser un grup; de fet, pot ser que hi hagi elements invertibles per l'esquerra que no ho siguin per la dreta, i recíprocament. Per exemple, sigui A l'anell dels endomorfismes del grup abelià additiu de les successions de nombres

enters; és a dir, $A := \mathrm{End}_{grup}(\mathbb{Z}^{\mathbb{N}}, +)$, amb la suma i la composició d'endomorfismes. Considerem els elements $T, S \in A$ donats per $s \mapsto T(s)$, on $T(s)(n) := s(n+1)$, per a tot $n \geq 0$ i tota successió $s \in \mathbb{Z}^{\mathbb{N}}$, i per $s \mapsto S(s)$, on $S(s)(0) := 0$, i $S(s)(n+1) := s(n)$, per a tot $n \geq 0$ i tota successió $s \in \mathbb{Z}^{\mathbb{N}}$. Llavors, $T \circ S = 1 \in A$, mentre que $S \circ T \neq 1$, perquè $(S \circ T)(s)(0) = 0$, mentre que $s(0)$ pot ser qualsevol nombre enter. Per tant, S admet invers per l'esquerra, però no per la dreta, i T admet invers per la dreta, però no per l'esquerra (recordem que si per a una operació associativa i amb neutre un element admet invers per l'esquerra i invers per la dreta, aquests coincideixen i és un element invers).

Definició 5.2.5. Un anell commutatiu K s'anomena un cos si $0 \neq 1$ i tot element no nul de K és invertible.

Observació 5.2.6. La definició també es pot aplicar al cas d'anells no commutatius; en aquest cas, però, s'acostuma a parlar d'àlgebres de divisió o bé de cossos no commutatius, fent explícita la no commutativitat del producte. Així, es reserva la paraula cos per als commutatius i es parla d'àlgebres de divisió en el cas general.

Exemples 5.2.7. • Com a exemples bàsics podem considerar els cossos dels nombres racionals, $\mathbb{Q}$, dels nombres reals, $\mathbb{R}$, dels nombres complexos, $\mathbb{C}$, i els cossos $\mathbb{Z}/p\mathbb{Z}$, on p és un nombre enter primer qualsevol. Els cos $\mathbb{Q}$ és subcòs de $\mathbb{R}$ i de $\mathbb{C}$, i el cos $\mathbb{R}$ és subcòs de $\mathbb{C}$.

• L'anell $\mathbb{Q}(i) := \{a + b \cdot i : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$, on $i^2 = -1$, és un cos, subcòs del cos dels nombres complexos.

• Per a exemples de cosos no commutatius, proposem els exercicis següents.

Exercici 5.2.8. Sigui $\mathbb{H} := \mathbb{H}_{\mathbb{R}}$, un $\mathbb{R}$-espai vectorial de dimensió 4, amb una base $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. En $\mathbb{H}$, existeix una única estructura d'anell tal que $\mathbf{1}$ és element unitat per a la multiplicació i se satisfan les igualtats $\mathbf{i}^2 = \mathbf{j}^2 = -\mathbf{1}$, i $\mathbf{k} = \mathbf{i} \cdot \mathbf{j} = -\mathbf{j} \cdot \mathbf{i}$. Aquest anell $\mathbb{H}$ és un cos no commutatiu, que s'anomena el cos dels quaternions de Hamilton. L'invers d'un quaternió no nul $q := x \cdot \mathbf{1} + y \cdot \mathbf{i} + z \cdot \mathbf{j} + t \cdot \mathbf{k}$, $x, y, z, y \in \mathbb{R}$, és el producte $q^{-1} = \overline{q} \cdot N(q)^{-1}$, on $\overline{q} := x \cdot \mathbf{1} - y \cdot \mathbf{i} - z \cdot \mathbf{j} - t \cdot \mathbf{k}$ és el quaternió conjugat de q, i $N(q) := q \cdot \overline{q} = x^2 + y^2 + z^2 + t^2$ és la seva norma. Notem que $\mathbb{R} \cong \mathbb{R} \cdot \mathbf{1} \subsetneq \mathbb{R} \cdot \mathbf{1} \oplus \mathbb{R} \cdot \mathbf{i} \subsetneq \mathbb{H}$ són subcossos, i que $\mathbb{R} \cdot \mathbf{1} \oplus \mathbb{R} \cdot \mathbf{i} \cong \mathbb{C}$. Se sol denotar per $\left(\dfrac{-1, -1}{\mathbb{R}}\right)$.

Exercici 5.2.9. Per a $y, z, t \in \mathbb{R}$ tals que $y^2 + z^2 + t^2 = 1$, $\mathbb{R} \cdot \mathbf{1} \oplus \mathbb{R} \cdot (y \cdot \mathbf{i} + z \cdot \mathbf{j} + t \cdot \mathbf{k}) \subsetneq \mathbb{H}_{\mathbb{R}}$ és un subcòs, isomorf a $\mathbb{C}$. Doncs, tenim una infinitat inclusions $\mathbb{R} \subsetneq \mathbb{C} \subsetneq \mathbb{H}$.

Exercici 5.2.10. Siguin $a, b \in \mathbb{Q}$ nombres racionals no nuls. Considerem un $\mathbb{Q}$-espai vectorial de dimensió 4, $\mathbb{H}_{\mathbb{Q}}$, amb una base $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. En $\mathbb{H}_{\mathbb{Q}}$, existeix una única estructura d'anell tal que $\mathbf{1}$ és element unitat per a la multiplicació i se satisfan les igualtats $\mathbf{i}^2 = a \cdot \mathbf{1}$, $\mathbf{j}^2 = b \cdot \mathbf{1}$, i $\mathbf{k} = \mathbf{i} \cdot \mathbf{j} = -\mathbf{j} \cdot \mathbf{i}$. Aquest anell $\mathbb{H}_{\mathbb{Q}}$ o bé és isomorf a l'anell de matrius $\mathbf{M}(2, \mathbb{Q})$, o bé és una àlgebra de divisió. S'anomena l'àlgebra de quaternions de paràmetres a, b, i se sol denotar per $\left(\dfrac{a, b}{\mathbb{Q}}\right)$.

Observació 5.2.11. Es pot definir una conjugació i una norma de manera semblant al cas dels quaternions de Hamilton i demostrar que els elements invertibles de $\left(\dfrac{a, b}{\mathbb{Q}}\right)$ coincideixen amb els elements de norma invertible. D'altra banda, si l'equació nòrmica, $X^2 - a \cdot Y^2 - b \cdot Z^2 + a \cdot b \cdot T^2 = 0$, admet una solució no trivial $(x, y, z, t) \in \mathbb{Q}^4$, llavors

$(y^2 - bt^2, xt + yz, xy + bzt)$ és una solució no trivial de l'equació $aX^2 + bY^2 = Z^2$. Si (x, y, z) és una solució amb $y \neq 0$ d'aquesta darrera equació, es poden identificar $\mathbf{i}$, $\mathbf{j}$, amb les matrius $\begin{bmatrix} 0 & y \\ a/y & 0 \end{bmatrix}$, $\begin{bmatrix} z/y & x \\ -a \cdot x/y^2 & -z/y \end{bmatrix}$. I, finalment, si a és un quadrat, es poden identificar $\mathbf{i}$, $\mathbf{j}$, amb les matrius $\begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}$ (cf. [Travesa 1992, cap. X, prop. 5.5]).

Proposició 5.2.12. *Siguin A, B anells i $\varphi : A \longrightarrow B$ un morfisme d'anells. Si A és un cos (o, més generalment, una àlgebra de divisió), i $B \neq \{0\}$, llavors φ és injectiu.*

Demostració: Notem que, en particular, φ és un morfisme dels grups additius corresponents, de manera que φ és injectiu si, i només si, $\ker \varphi = \{0\}$. Ara bé, si existís $x \in \ker \varphi$, $x \neq 0$, llavors per a tot element $y \in A$ seria $\varphi(y) = \varphi(x \cdot x^{-1} \cdot y) = \varphi(x) \cdot \varphi(x^{-1} \cdot y) = 0$, de manera que $\varphi = 0$. Però si φ és un morfisme d'anells, com que $B \neq \{0\}$, ha de ser $\varphi(1) = 1 \neq 0$. □

5.3 Divisors de zero. Dominis d'integritat

Així com els elements invertibles d'un anell estan lligats íntimament a les solucions de l'equació $X \cdot Y = 1$, els divisors de zero ho estan a l'equació $X \cdot Y = 0$. I no és cert, en general, que si en un anell és $a \cdot b = 0$ llavors sigui $a = 0$ o bé $b = 0$. Un exemple molt senzill és donat, en l'anell de les funcions reals de variable real (fins i tot, en el subanell de les funcions contínues), per les funcions f, g definides per $f(x) := \dfrac{x + |x|}{2}$, $g(x) := \dfrac{x - |x|}{2}$. Com que $f(1) = 1 \neq 0$ i $g(-1) = -1 \neq 0$, tenim que $f \neq 0$ i que $g \neq 0$. Però, en canvi, $f \cdot g = 0$, perquè per a tot $x \in \mathbb{R}$ és $f(x) \cdot g(x) = \dfrac{x + |x|}{2} \cdot \dfrac{x - |x|}{2} = \dfrac{x^2 - |x|^2}{4} = 0$.

Definició 5.3.1. Sigui A un anell. Un element $a \in A$ s'anomena un divisor de zero per l'esquerra si existeix un element $b \in A$, $b \neq 0$, tal que $a \cdot b = 0$; i s'anomena un divisor de zero per la dreta si existeix un element $b \in A$, $b \neq 0$, tal que $b \cdot a = 0$. Un element $a \in A$ s'anomena un divisor de zero si ho és per la dreta i per l'esquerra. Òbviament, si l'anell és commutatiu, els dos conceptes coincideixen.

Definició 5.3.2. Si per a dos elements $a, b \in A$ és $a \cdot b = 0$, es diu que a és ortogonal a b per l'esquerra i que b és ortogonal a a per la dreta. Si $a \cdot b = 0 = b \cdot a$, es diu que a i b són ortogonals.

Observació 5.3.3. Notem que pot ser que un element sigui divisor de zero per la dreta i, alhora, ser invers per la dreta. En efecte, reprenem l'exemple de l'observació **5.2.4** i considerem l'endomorfisme $U \in A$ donat per $s \mapsto U(s)$, on $U(s)(0) := s(0)$, i $U(s)(n) := 0$, per a tot $n > 0$ i tota successió $s \in \mathbb{Z}^{\mathbb{N}}$. Llavors, és $U \circ S = 0$, mentre que $S \circ U \neq 0$; i també $T \circ U = 0$, mentre que $U \circ T \neq 0$ (i recordem que $T \circ S = 1$). Així, U és divisor de zero per l'esquerra i divisor de zero per la dreta. I S és un divisor de zero per la dreta i, alhora, és un invers per la dreta; i T és un divisor de zero per l'esquerra i, alhora, és un invers per l'esquerra.

Exercici 5.3.4. Ara bé, si un element té invers per l'esquerra, no pot ser divisor de zero per l'esquerra. I, anàlogament, si té invers per la dreta, no pot ser divisor de zero per la dreta.

Observació 5.3.5. Si un anell A és diferent de l'anell $\{0\}$, l'element $0 \in A$ és un divisor de zero, perquè $0 \cdot 1 = 1 \cdot 0 = 0$, i $1 \neq 0$.

Definició 5.3.6. Un domini d'integritat és un anell commutatiu K tal que $1 \neq 0$ i que no té cap més divisor de zero que 0. També es parla de domini o d'anell íntegre.

Exemples 5.3.7. • L'anell $\mathbb{Z}$ dels nombres enters és un domini d'integritat; en efecte, si m, n són nombres enters diferents de zero, el seu producte, $m \cdot n$, és un nombre enter diferent de zero; per tant, l'únic nombre enter divisor de zero és 0.

• D'altra banda, l'anell $\mathbb{Z}/6\mathbb{Z}$ no és un domini d'integritat. En efecte, els divisors de zero de $\mathbb{Z}/6\mathbb{Z}$ són els elements 0, 2, 3 i 4.

• Més generalment, per a un nombre enter $n \geq 2$, l'anell $\mathbb{Z}/n\mathbb{Z}$ admet divisors de zero si, i només si, n és un nombre enter compost. En efecte, si $n = a \cdot b$ és una descomposició de n com a producte de dos nombres enters $a, b \notin \{0, 1, -1\}$, llavors a i b són divisors de zero en $\mathbb{Z}/n\mathbb{Z}$. Amb tota generalitat, la classe mòdul n d'un nombre enter a és un divisor de zero en $\mathbb{Z}/n\mathbb{Z}$ si, i només si, $\mathrm{mcd}(n, a) \neq 1$.

• Tot cos K és un domini d'integritat; en efecte, si $a \in K$, $a \neq 0$, podem considerar l'invers $b \in K$ de a, de manera que $a \cdot b = 1$. Ara, si $z \in K$ i $z \cdot a = 0$, tenim que $0 = 0 \cdot b = z \cdot a \cdot b = z \cdot 1 = z$; per tant, l'únic divisor de zero en K és 0.

• Com a conseqüència, tot subanell d'un cos o d'un domini d'integritat és un domini d'integritat.

• Recíprocament, tot domini d'integritat és subanell d'algun cos. En efecte, la construcció següent proporciona el cos de fraccions d'un domini d'integritat. Notem que és una generalització directa del procés habitual de construcció del cos dels nombres racionals a partir de l'anell dels nombres enters.

Exercici 5.3.8. Sigui K un domini d'integritat. En el conjunt $K \times (K - \{0\})$, definim la relació

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d - c \cdot b = 0, \qquad a, b, c, d \in K, \quad b, d \neq 0.$$

(a) La relació $\sim$ és una relació d'equivalència per a la qual se satisfan les propietats

$$\begin{aligned} &(a, b) \sim (a', b') \quad \text{i} \quad (c, d) \sim (c', d') \implies (a \cdot d + c \cdot b, b \cdot d) \sim (a' \cdot d' + c' \cdot b', b' \cdot d'), \\ &(a, b) \sim (a', b') \quad \text{i} \quad (c, d) \sim (c', d') \implies (a \cdot c, b \cdot d) \sim (a' \cdot c', b' \cdot d'), \end{aligned}$$

per a $a, a', b, b', c, c', d, d' \in K$, $b, b', d, d' \neq 0$. Denotem per $\dfrac{a}{b}$ la classe d'equivalència de la parella (a, b), $a, b \in K$, $b \neq 0$, i per Q el conjunt de totes les classes d'equivalència. En Q, podem definir les operacions suma i producte per les fórmules

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}, \qquad a, b, c, d \in K, \quad b, d \neq 0.$$

(b) El conjunt Q admet una única estructura de cos amb aquestes operacions binàries com a suma i producte; els element neutres són les classes $0 := \dfrac{0}{1}$, per a la suma, i $1 := \dfrac{1}{1}$, per al producte; l'element oposat de $\dfrac{a}{b}$ és $-\dfrac{a}{b} = \dfrac{-a}{b}$, $a, b \in K$, $b \neq 0$, i l'invers de $\dfrac{a}{b} \neq 0$ és $\dfrac{b}{a}$, per a $a, b \in K$, $a, b \neq 0$. Notem que per a tot $b \in K$, $b \neq 0$, és $0 = \dfrac{0}{b} = \dfrac{0}{1}$ i $1 = \dfrac{1}{1} = \dfrac{b}{b}$. El cos Q s'anomena el cos de fraccions de K.

(c) L'aplicació $K \longrightarrow Q$ definida per l'assignació $a \mapsto \dfrac{a}{1}$ és un morfisme injectiu d'anells, de manera que podem identificar cada element $a \in K$ amb la classe $\dfrac{a}{1} \in Q$ i l'anell K amb un subanell de Q.

(d) Si $\varphi : K \longrightarrow L$ és un morfisme d'anells tal que per a tot $a \in K - \{0\}$ l'element $\varphi(a) \in L$ és invertible, aleshores φ s'estén de manera única a un morfisme d'anells $Q \longrightarrow L$, que és injectiu si $L \neq \{0\}$. Com a conseqüència, Q és el més petit de tots els cossos que contenen K com a subanell.

Aquesta darrera propietat és especialment important des del punt de vista estructural; per exemple, cf., més endavant, **5.6.14**.

5.4 L'anell producte. Elements idempotents

En les seccions anteriors hem vist que els elements invertibles d'un anell són les solucions de l'equació $X \cdot Y = 1$, i que els divisors de zero són les solucions de l'equació $X \cdot Y = 0$, tals que $X \neq 0$ o $Y \neq 0$. Els elements idempotents són les solucions de l'equació $X^2 = X$; i estan relacionats de manera natural amb l'anell producte.

Definició 5.4.1. Sigui $\{A_i\}_{i\in I}$ una família no buida d'anells. Un anell A amb una família de morfismes d'anells $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$ és un producte de la família $\{A_i\}_{i\in I}$ si se satisfà la propietat universal que per a tot anell B i tota família de morfismes d'anells $\{\psi_i : B \longrightarrow A_i\}_{i\in I}$ hi ha un únic morfisme d'anells $\psi : B \longrightarrow A$ tal que per a tot $i \in I$ és

$$\forall\{\psi_i\}_{i\in I}\ \exists!\psi\ \forall i \in I$$

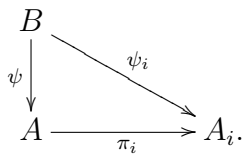


Diagrama 5.1: Propietat universal del producte d'anells

Els anells A_i s'anomenen els factors del producte i els morfismes $\pi_i : A \longrightarrow A_i$ s'anomenen les projeccions canòniques del producte en els seus factors (cf. **1.2.1**, **2.7.2**).

Proposició 5.4.2. *Sigui $\{A_i\}_{i\in I}$ una família no buida d'anells. Si existeix un anell producte, aquest és únic llevat d'un únic isomorfisme que commuta amb les projeccions canòniques. És a dir, si $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$, $\{\pi'_i : A' \longrightarrow A_i\}_{i\in I}$ són productes de la família $\{A_i\}_{i\in I}$, llavors existeix un únic morfisme d'anells $\varphi : A \longrightarrow A'$ tal que per a tot $i \in I$ és*

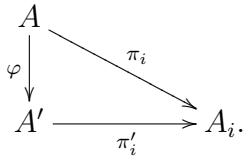


Diagrama 5.2: Unicitat del producte d'anells

A més a més, φ és un isomorfisme (cf. **1.2.4**, **2.7.3**). □

Proposició 5.4.3. *Sigui $\{A_i\}_{i\in I}$ una família no buida d'anells. Aleshores existeix un anell producte de la família $\{A_i\}_{i\in I}$.*

DEMOSTRACIÓ: Com en el cas de grups, només cal construir-ne un model. En el grup additiu producte (cf. **2.7.1**),

$$A := \prod_{i\in I} A_i,$$

podem definir una única estructura d'anell de manera que les projeccions canòniques $\pi_i : A \longrightarrow A_i$ siguin morfismes d'anells. En efecte, cal que el producte sigui definit per $\{a_i\}_{i\in I} \cdot \{b_i\}_{i\in I} := \{a_i \cdot b_i\}_{i\in I}$, i que l'element unitat sigui la família $\{1_i\}_{i\in I}$, on $1_i \in A_i$ és l'element unitat de A_i. Ara bé, aquestes definicions tenen sentit i fan que, efectivament, la família de les projeccions $\{\pi_i : A \longrightarrow A_i\}_{i\in I}$ sigui un producte d'anells. La comprovació és un exercici senzill. □

Observacions 5.4.4. • Notem que si tots els anells A_i són commutatius, llavors A és commutatiu.

• Si consideréssim el producte d'una família d'anells commutatius com un anell commutatiu amb una família de projeccions tal que se satisfés la propietat universal per a tota família de morfismes d'anells commutatius (és a dir, de manera que l'anell B de la propietat universal només pugui ser commutatiu), llavors el producte de la família, considerat com a producte d'anells, coincidiria amb el producte de la família, considerat com a producte d'anells commutatius.

• Si la família és finita; és a dir, si el conjunt I és finit, posem $I = \{0, 1, \ldots, n-1\}$, s'escriu sovint $A = \prod_{i=0}^{n-1} A_i = A_0 \times A_1 \times \cdots \times A_{n-1}$.

Observació 5.4.5. Notem que si en la família $\{A_i\}_{i\in I}$ hi ha dos índexs $i, j \in I$, $i \neq j$, per als quals és $A_i \neq \{0\}$ i $A_j \neq \{0\}$, llavors el producte d'anells té divisors de zero no trivials: per exemple, considerem els elements $e_i := \{0_k, 1_i\}_{k\in I, k\neq i}$, $e_j := \{0_k, 1_j\}_{k\in I, k\neq j}$, on $0_k \in A_k$ és l'element neutre de la suma de A_k i $1_i \in A_i$, $1_j \in A_j$ són els elements unitat de A_i i A_j, respectivament; llavors, és $e_i \neq 0$, $e_j \neq 0$, però $e_i \cdot e_j = 0$. Notem que els elements e_i i e_j són elements centrals de l'anell producte i que $e_i^2 = e_i$ i $e_j^2 = e_j$.

En particular, un anell producte només és un domini d'integritat en el cas en què un dels anells A_i és un domini d'integritat i per a tot $j \in I$, $j \neq i$, és $A_j = \{0\}$.

Observació 5.4.6. Podríem considerar les aplicacions naturals d'inclusió $A_j \xrightarrow{\psi_j} \prod_{i\in I} A_i$, definides per a $j \in I$ per $a_j \mapsto \{a_i\}_{i\in I}$, on $a_i = 0$ per a $i \neq j$. Les aplicacions ψ_j, encara que sempre són morfismes dels grups commutatius additius corresponents, només són morfismes d'anells en el cas en què tots els anells A_i o tots menys un són l'anell $\{0\}$. En general, doncs, no permeten identificar l'anell A_j amb cap subanell de l'anell producte.

Definició 5.4.7. Siguin A un anell i I un conjunt no buit. Per a tot $i \in I$, posem $A_i := A$, i considerem la família d'anells $\{A_i\}_{i\in I}$. El producte d'aquesta família s'escriu en la forma $A^I := \prod_{i\in I} A$. A més a més, l'aplicació $\psi : A \longrightarrow A^I$ definida per $a \mapsto \{a_i\}_{i\in I}$, on $a_i := a$, per a tot $i \in I$ és un morfisme injectiu d'anells; s'anomena la inclusió diagonal de A en A^I. En particular, A s'identifica amb un subanell de A^I.

Definició 5.4.8. Siguin A un anell i $e \in A$ un element. Es diu que e és un element idempotent si $e^2 = e$.

Exemples 5.4.9. • Per a tot anell A, els elements $e = 0$ i $e = 1$ són idempotents. S'anomenen els idempotents trivials.

• Sigui K un domini d'integritat. Llavors, els únics elements idempotents de K són els trivials, $e = 0$ i $e = 1$. En efecte, l'equació $e^2 = e$ es pot escriure en la forma $e \cdot (e-1) = 0$; i, si K és un domini d'integritat, això implica que $e = 0$ o bé $e - 1 = 0$; és a dir, $e = 0$ o bé $e = 1$.

• Siguin A un anell i $e \in A$ un element idempotent. Llavors, $1 - e \in A$ és un element idempotent, i ortogonal a e.

• Acabem de veure (cf. **5.4.5**) que si un anell és producte d'anells no trivials, aleshores conté algun element idempotent no trivial i central. El recíproc també és cert; si un anell conté algun element idempotent no trivial i central, llavors és producte d'anells. Ho veiem en els resultats que segueixen.

Proposició 5.4.10. *Sigui A un anell i suposem que $e \in A$ és un element idempotent i central de A. Llavors, els grups abelians additius $A \cdot e = e \cdot A$ i $A \cdot (1-e) = (1-e) \cdot A$ amb el producte de A, admeten una estructura d'anell de manera que els elements unitat són e i $1 - e$, respectivament, i per a aquests anells es té un isomorfisme $A \cong A \cdot e \times A \cdot (1-e)$.*

Proposició 5.4.11. *Més generalment, sigui A un anell i suposem que $e_1, \ldots, e_n \in A$ són elements idempotents, centrals, ortogonals dos a dos, i tals que $e_1 + \cdots + e_n = 1$. Llavors, els grups abelians $A \cdot e_i = e_i \cdot A$, $1 \leq i \leq n$, amb el producte de A, admeten una estructura d'anell de manera que els elements unitat corresponents són els e_i i, a més a més, es té un isomorfisme d'anells $A \cong A \cdot e1 \times A \cdot e_2 \times \cdots \times A \cdot e_n$.*

Demostració: Exercici. □

Observació 5.4.12. La condició que els idempotents siguin centrals no es pot suprimir de l'enunciat de les proposicions anteriors. Per a veure-ho, notem que els elements $e := \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ i $1 - e := \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in \mathbf{M}(2, \mathbb{Z})$ són idempotents ortogonals de suma 1; però no és cert que $\mathbf{M}(2, \mathbb{Z})$ sigui el producte de dos anells el producte dels quals sigui la restricció del producte de matrius i els elements unitat dels quals siguin e i $1 - e$, respectivament. En efecte, a fi que e sigui l'element unitat de $\mathbf{M}(2, \mathbb{Z}) \cdot e$, caldria que $e \cdot (m \cdot e) = (m \cdot e) \cdot e$, per a tota matriu $m \in \mathbf{M}(2, \mathbb{Z})$; però això no és així. Posem $m = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$; llavors,

$$(m \cdot e) \cdot e = m \cdot e = \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & d \end{bmatrix} = e \cdot (m \cdot e),$$

si $b \neq 0$; per tant, e no seria l'element unitat.

Observació 5.4.13. El producte d'elements idempotents que no commuten no té per què ser idempotent. Per exemple, considerem, en $\mathbf{M}(2, \mathbb{Z})$, els elements

$$e_1 := \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \qquad e_2 := \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \qquad e_3 := \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \qquad e_4 := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Llavors, $e_1^2 = e_1$, $e_2^2 = e_2$, $e_3^2 = e_3$, de manera que e_1, e_2, e_3 són idempotents. A més a més, $e_1 \cdot e_2 = 0$, que és idempotent, mentre que $e_2 \cdot e_1 = e_4$, que no és idempotent, sinó que $e_4^2 = 0$; és a dir, e_4 és nilpotent. D'altra banda, $e_1 \cdot e_3 = e_3$, i $e_3 \cdot e_1 = e_1$, de manera que $e_1 \cdot e_3 \cdot e_1 = e_1$ i $e_3 \cdot e_1 \cdot e_3 = e_3$, mentre que cap d'aquests elements no és invertible.

5.5 Ideals i anells quocient. Característica d'un anell

Definició 5.5.1. Sigui A un anell. Un A-mòdul per l'esquerra és un grup abelià additiu, E, juntament amb una acció per l'esquerra de A en E, $A \times E \longrightarrow E$, que denotem per $(\lambda, v) \mapsto \lambda \cdot v$, per a la qual se satisfan les condicions de compatibilitat següents (cf. la definició de K-mòdul per al cas K commutatiu, **1.8.1**):

(a) (L'acció respecta la suma de E, en el sentit que la distribueix.) Per a tot $\lambda \in K$ i tota parella d'elements $v, w \in E$, és $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$.

(b) (L'acció respecta el neutre de E.) Per a tot $\lambda \in K$, $\lambda \cdot 0 = 0$.

(c) (L'acció respecta l'oposat de E.) Per a tot $\lambda \in K$ i tot $v \in E$, $\lambda \cdot (-v) = -(\lambda \cdot v)$.

(d) (L'acció és compatible amb les sumes de K i de E en el sentit que distribueix, en E, la suma de K.) Per a tota parella d'elements $\lambda, \mu \in K$ i tot element $v \in E$ és $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$.

(e) (L'acció és compatible amb els neutres de les sumes de K i de E.) Per a tot element $v \in E$ és $0 \cdot v = 0$.

(f) (L'acció és compatible amb els oposats per a les sumes de K i de E.) Per a tot element $\lambda \in K$ i tot element $v \in E$ és $(-\lambda) \cdot v = -(\lambda \cdot v)$.

(g) (L'acció és compatible amb el producte de K, en el sentit que s'hi associa per l'esquerra.) Per a tota parella d'elements $\lambda, \mu \in K$ i tot element $v \in E$ és $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$.

(h) (L'acció del neutre del producte de K és la identitat.) Per a tot element $v \in E$ és $1 \cdot v = v$.

Definició 5.5.2. Sigui A un anell. Anàlogament, un A-mòdul per la dreta és un grup abelià additiu, E, juntament amb una acció per la dreta de A en E, $A \times E \longrightarrow E$, que denotem per $(\lambda, v) \mapsto v \cdot \lambda$, per a la qual se satisfan les condicions de compatibilitat següents:

(a) (L'acció respecta la suma de E, en el sentit que la distribueix.) Per a tot $\lambda \in K$ i tota parella d'elements $v, w \in E$, és $(v + w) \cdot \lambda = v \cdot \lambda + w \cdot \lambda$.

(b) (L'acció respecta el neutre de E.) Per a tot $\lambda \in K$, $0 \cdot \lambda = 0$.

(c) (L'acció respecta l'oposat de E.) Per a tot $\lambda \in K$ i tot $v \in E$, $(-v) \cdot \lambda = -(v \cdot \lambda)$.

(d) (L'acció és compatible amb les sumes de K i de E en el sentit que distribueix, en E, la suma de K.) Per a tota parella d'elements $\lambda, \mu \in K$ i tot element $v \in E$ és $v \cdot (\lambda + \mu) = v \cdot \lambda + v \cdot \mu$.

(e) (L'acció és compatible amb els neutres de les sumes de K i de E.) Per a tot element $v \in E$ és $v \cdot 0 = 0$.

(f) (L'acció és compatible amb els oposats per a les sumes de K i de E.) Per a tot element $\lambda \in K$ i tot element $v \in E$ és $v \cdot (-\lambda) = -(v \cdot \lambda)$.

(g) (L'acció és compatible amb el producte de K, en el sentit que s'hi associa per la dreta. Aquesta és l'única diferència entre les definicions de mòdul per l'esquerra i de mòdul per la dreta.) Per a tota parella d'elements $\lambda, \mu \in K$ i tot element $v \in E$ és $v \cdot (\lambda \cdot \mu) = (v \cdot \lambda) \cdot \mu$. Notem que si un producte $\lambda \cdot \mu$ actua en un vector v, primer actua λ i després actua μ, contràriament als mòduls per l'esquerra, en què primer actua μ i, després, λ.

(h) (L'acció del neutre del producte de K és la identitat.) Per a tot element $v \in E$ és $v \cdot 1 = v$.

Observació 5.5.3. Anàlogament que per al cas dels anells commutatius, i tant en el cas de mòduls per l'esquerra com en el de mòduls per la dreta, les propietats (b) i (c) es dedueixen formalment de la propietat (a), i les propietats (e) i (f) es dedueixen formalment de la propietat (d); per tant, és suficient predicar les propietats (a), (d), (g) i (h), a més a més, òbviament, de les propietats de grup commutatiu additiu de E.

Exemples 5.5.4. • Per a tot anell A, A és també un A-mòdul per l'esquerra i un A-mòdul per la dreta.

• Més generalment, si A és un anell i $n \geq 1$ és un nombre enter, el grup abelià producte, A^n, és un A-mòdul per l'esquerra, i un A-mòdul per la dreta, amb les accions $A \times A^n \longrightarrow A^n$ donades per $\lambda \cdot (a_0, \ldots, a_{n-1}) := (\lambda \cdot a_0, \ldots, \lambda \cdot a_{n-1})$, i $(a_0, \ldots, a_{n-1}) \cdot \lambda := (a_0 \cdot \lambda, \ldots, a_{n-1} \cdot \lambda)$, respectivament.

• Per a tot anell A i tot $m, n \geq 1$, el grup abelià additiu $\mathbf{M}(m, n; A)$, de les matrius de m files i n columnes i coeficients en A és un A-mòdul per l'esquerra i, també, un A-mòdul per la dreta, amb l'acció de multiplicació habitual per l'esquerra o per la dreta d'un escalar per una matriu.

Definició 5.5.5. Siguin A un anell i E un A-mòdul per l'esquerra (respectivament, per la dreta). Un subgrup additiu $F \subseteq E$ és un A-submòdul si l'acció de A es pot restringir a F; en aquest cas, els axiomes de A-mòdul se satisfan automàticament i F és un A-mòdul per l'esquerra (respectivament, per la dreta).

Així, si A és un anell i E és un A-mòdul per l'esquerra, un subgrup additiu $F \subseteq E$ és un A-submòdul (per l'esquerra) de E si, i només si, per a tot $v \in F$ i tot $\lambda \in A$ és $\lambda \cdot v \in F$.

Exemples 5.5.6. • Siguin A un anell, E un A-mòdul per l'esquerra (respectivament, per la dreta), i $\{F_i\}_{i \in I}$ una família no buida de A-submòduls de E. Llavors, la intersecció $\bigcap_{i \in I} F_i$ és un A-submòdul de E.

• Siguin A un anell, E un A-mòdul per l'esquerra (respectivament, per la dreta), i $S \subseteq E$ un subconjunt qualsevol. El submòdul generat per S és la intersecció de tots els submòduls de E que contenen S. Es representa per $\langle S \rangle_A$.

• Siguin A un anell, E un A-mòdul per l'esquerra (respectivament, per la dreta), i $\{F_i\}_{i \in I}$ una família no buida de A-submòduls de E. El submòdul generat per la reunió $\bigcup_{i \in I} F_i$ s'anomena el submòdul suma, i es representa per $\sum_{i \in I} F_i$; coincideix amb el subconjunt de les sumes finites d'elements dels F_i; és a dir, per a tot $x \in \sum_{i \in I} F_i$, existeix un subconjunt finit $J \subseteq I$ i per a tot $i \in J$ existeix un element $x_i \in F_i$ tals que $x = \sum_{i \in J} x_i$.

• El submòdul generat per un subconjunt $S \subseteq E$ coincideix amb el conjunt de les combinacions lineals (finites) d'elements de S i coeficients en A. Així, $\langle S\rangle_A = \sum_{s\in S} A\cdot s$, si E és un A-mòdul per l'esquerra i $\langle S\rangle_A = \sum_{s\in S} s\cdot A$, si E és un A-mòdul per la dreta, amb les notacions òbvies per a $A\cdot s := \{a\cdot s : a\in A\}$ i per a $s\cdot A := \{s\cdot a : a\in A\}$.

Definició 5.5.7. Siguin A un anell i considerem A-mòduls per l'esquerra (respectivament, per la dreta) E, F. Una aplicació A-lineal, també anomenada un morfisme de A-mòduls, de E en F és un morfisme de grups abelians additius $\varphi : E \longrightarrow F$ per al qual es respecta l'acció de A en E i en F; és a dir, tal que per a tot $\lambda\in A$ i tot $v\in E$ és $\varphi(\lambda\cdot v) = \lambda\cdot\varphi(v)$ (respectivament, $\varphi(v\cdot\lambda) = \varphi(v)\cdot\lambda$).

Exemples 5.5.8. • La identitat d'un A-mòdul (per l'esquerra, o bé per la dreta) és un morfisme de A-mòduls (per l'esquerra, o bé per la dreta).

• La composició de morfismes de A-mòduls (per l'esquerra, o bé per la dreta) és un morfisme de A-mòduls (per l'esquerra, o bé per la dreta).

• Siguin A un anell, E, F, A-mòduls (per l'esquerra, o bé per la dreta) i $\varphi : E \longrightarrow F$ un morfisme de A-mòduls. Llavors, $\ker\varphi \subseteq E$ i $\operatorname{im}\varphi \subseteq F$ són A-submòduls (per l'esquerra, o bé per la dreta).

Exercici 5.5.9. Siguin A un anell, E un A-mòdul per l'esquerra (o bé per la dreta), i $F\subseteq E$ un A-submòdul. El grup abelià quocient E/F admet una única estructura de A-mòdul per l'esquerra (o bé per la dreta) tal que la projecció canònica $\pi : E \longrightarrow E/F$ és un morfisme de A-mòduls. S'anomena el A-mòdul quocient de E per F.

Exercici 5.5.10. Els isomorfismes de A-mòduls per l'esquerra (o bé per la dreta) són exactament els morfismes bijectius.

Exercici 5.5.11. Siguin A un anell i $\varphi : E \longrightarrow F$ un morfisme de A-mòduls per l'esquerra (o bé per la dreta). Se satisfà el primer teorema d'isomorfia: $E/\ker\varphi \cong \operatorname{im}\varphi$, isomorfisme de A-mòduls. A més a més, la descomposició canònica del morfisme φ, com a grups abelians, ho és de morfismes de A-mòduls.

Definició 5.5.12. Sigui A un anell. Els A-submòduls de A s'anomenen ideals. Més precisament, un ideal per l'esquerra de l'anell A és un subgrup additiu $\mathfrak{a}\subseteq A$ tal que per a tot $a\in\mathfrak{a}$ i tot $\lambda\in A$ és $\lambda\cdot a\in\mathfrak{a}$. Un ideal per la dreta de l'anell A és un subgrup additiu $\mathfrak{a}\subseteq A$ tal que per a tot $a\in\mathfrak{a}$ i tot $\lambda\in A$ és $a\cdot\lambda\in\mathfrak{a}$. Un ideal bilateral de l'anell A és un subgrup additiu $\mathfrak{a}\subseteq A$ que és alhora un ideal per l'esquerra i un ideal per la dreta. S'anomenen ideals els ideals per l'esquerra, els ideals per la dreta i els ideals bilaterals.

Observació 5.5.13. Notem que si l'anell A és commutatiu, els conceptes d'ideal per l'esquerra i d'ideal per la dreta coincideixen, de manera que tots els ideals són ideals bilaterals.

Exemples 5.5.14. • Els ideals trivials d'un anell són els ideals A i $\{0\}$; són ideals bilaterals.

• Si $\varphi : A \longrightarrow B$ és un morfisme d'anells, el seu nucli, $\ker(f) := \{a\in A : \varphi(a) = 0\}$, és un ideal bilateral de A. Notem, però, que si $B\neq\{0\}$ (i, per tant, $A\neq\{0\}$), el nucli no és un subanell de A, perquè no conté 1.

• Més generalment, si $\varphi : A \longrightarrow B$ és un morfisme d'anells, i $\mathfrak{b} \subseteq B$ és un ideal (per l'esquerra, per la dreta, o bilateral) de B, llavors $\varphi^{-1}(\mathfrak{b}) \subseteq A$ és un ideal (per l'esquerra, per la dreta, o bilateral, respectivament) de A. I si $\mathfrak{a} \subseteq A$ és un ideal (per l'esquerra, per la dreta, o bilateral) de A, llavors $\varphi(\mathfrak{a}) \subseteq \varphi(A)$ és un ideal (per l'esquerra, per la dreta, o bilateral, respectivament) de l'anell imatge, però no necessàriament un ideal de B.

• Si A és un anell i $\{\mathfrak{a}_i\}_{i\in I}$ és una família no buida d'ideals (per l'esquerra, per la dreta, bilaterals) $\mathfrak{a}_i \subseteq A$, la seva intersecció, $\bigcap_{i\in I} \mathfrak{a}_i \subseteq A$, és un ideal (per l'esquerra, per la dreta, bilateral, respectivament) de A.

Observacions 5.5.15. • Un anell commutatiu K és un cos si, i només si, els únics ideals de K són els trivials.

• Si K és un cos i A és un anell diferent de $\{0\}$, tot morfisme d'anells $K \longrightarrow A$ és injectiu.

Definició 5.5.16. Siguin A un anell i $S \subseteq A$ un subconjunt qualsevol. L'ideal (per l'esquerra, per la dreta, bilateral) generat per S és la intersecció de tots els ideals (per l'esquerra, per la dreta, bilaterals, respectivament) de A que contenen el conjunt S.

Definició 5.5.17. Si $S = \{a\}$, $a \in A$, és un conjunt d'un sol element, l'ideal per l'esquerra generat per S és l'ideal principal per l'esquerra $A \cdot a := \{\lambda \cdot a : \lambda \in A\}$; i l'ideal per la dreta generat per S és l'ideal principal per la dreta $a \cdot A := \{a \cdot \lambda : \lambda \in A\}$. L'ideal bilateral generat per S és el conjunt format pels elements de la forma $\sum_{\lambda,\mu\in A} \lambda \cdot a \cdot \mu$, on tots els elements $\lambda, \mu \in A$, llevat d'una quantitat finita, són 0.

Observació 5.5.18. Més generalment, per a un subconjunt qualsevol $S \subseteq A$, l'ideal per l'esquerra generat per S és el conjunt dels elements de la forma $\sum_{s\in S} \lambda_s \cdot s$, on $\lambda_s \in A$ són tots 0, llevat d'una quantitat finita. Anàlogament, l'ideal per la dreta generat per S és el conjunt dels elements de la forma $\sum_{s\in S} s \cdot \lambda_s$, on $\lambda_s \in A$ són tots 0, llevat d'una quantitat finita.

Proposició 5.5.19. *Tots els ideals de l'anell dels nombres enters, $\mathbb{Z}$, són principals.*

Demostració: En efecte, tot ideal és, en particular, un subgrup additiu; i ja hem vist (cf. la proposició **2.8.6**) que tots els subgrups additius de $\mathbb{Z}$ són generats per un sol element; és a dir, de la forma $n\mathbb{Z}$, amb $n \geq 0$. Per tant, tots els ideals de l'anell $\mathbb{Z}$ són principals. □

Corol·lari 5.5.20. *Sigui $n \in \mathbb{Z}$, $n \geq 2$. Tots els ideals de l'anell $\mathbb{Z}/n\mathbb{Z}$ són principals.*

Demostració: Tot ideal de $\mathbb{Z}/n\mathbb{Z}$ és la imatge per la reducció mòdul n, $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, d'un ideal de $\mathbb{Z}$; i la imatge d'un ideal principal per un morfisme d'anells és un ideal principal de la imatge. Equivalentment, és suficient recordar que $\mathbb{Z}/n\mathbb{Z}$ és un grup cíclic, de manera que tot ideal, com que en particular és un subgrup additiu, admet un sol generador. □

Observació 5.5.21. Com que els ideals de $\mathbb{Z}$ s'identifiquen amb els nombres naturals n, i la relació d'inclusió d'ideals és la relació de divisibilitat en $\mathbb{N}$, resulta que els ideals de $\mathbb{Z}/n\mathbb{Z}$ estan en correspondència bijectiva amb els divisors naturals de n. En efecte, per a $m, n \in \mathbb{N}$, és $m\mathbb{Z} \subseteq n\mathbb{Z}$ si, i només si, m és múltiple de n.

Definició 5.5.22. Siguin A un anell i $\mathfrak{a} \subseteq A$ un subgrup additiu. La condició que s'imposa a $\mathfrak{a}$ perquè aquest subgrup sigui un ideal bilateral de A és exactament la condició que es necessita a fi que el grup abelià additiu quocient $A/\mathfrak{a}$ sigui un anell tal que el morfisme de projecció $A \longrightarrow A/\mathfrak{a}$, donat per $a \mapsto a + \mathfrak{a}$, sigui un morfisme d'anells (exercici). D'aquesta manera s'obté l'anell quocient de A per l'ideal $\mathfrak{a}$. Si l'anell A és commutatiu, llavors l'anell quocient $A/\mathfrak{a}$ també és commutatiu (cf. **2.5.5**).

Observació 5.5.23. Notem que si $\mathfrak{a} \subseteq A$ és un ideal per l'esquerra (o per la dreta) però no bilateral, el grup abelià quocient $A/\mathfrak{a}$ és un A-mòdul per l'esquerra (o per la dreta); però per a poder definir el producte en $A/\mathfrak{a}$ de manera que la projecció $A \longrightarrow A/\mathfrak{a}$ sigui un morfisme d'anells cal que $\mathfrak{a}$ sigui un ideal bilateral. En efecte, a fi que la multiplicació d'una classe qualsevol per la classe de l'element 0 sigui la classe de l'element 0, per qualsevol dels dos costats, cal que l'acció de A en $\mathfrak{a}$ per l'esquerra i per la dreta estigui definida en $\mathfrak{a}$; és a dir, que $\mathfrak{a}$ sigui un ideal bilateral.

Exercici 5.5.24. Anàlogament al cas dels grups commutatius, o dels A-mòduls, donats un anell A i un ideal bilateral $\mathfrak{a} \subseteq A$, el morfisme de projecció $\pi : A \longrightarrow A/\mathfrak{a}$ permet definir una bijecció entre el conjunt dels ideals per l'esquerra (respectivament, per la dreta; respectivament, bilaterals) de l'anell quocient $A/\mathfrak{a}$ i el conjunt dels ideals per l'esquerra (respectivament, per la dreta; respectivament, bilaterals) de A que contenen $\mathfrak{a}$ (cf. **2.5.17**).

Exercici 5.5.25. Siguin A, B, anells i $\varphi : A \longrightarrow B$ un morfisme d'anells. Llavors, $\ker \varphi \subseteq A$ és un ideal bilateral de A, $\operatorname{im} \varphi \subseteq B$ és un subanell de B, i se satisfà el primer teorema d'isomorfia: l'isomorfisme entre els grups abelians $A/\ker(f)$ i $\operatorname{im} \varphi$ ho és d'anells. A més a més, la descomposició canònica del morfisme de grups abelians φ també ho és de morfismes d'anells (cf. **2.5.7**).

Proposició 5.5.26. *Sigui A un anell. Existeix un únic morfisme d'anells $\varphi : \mathbb{Z} \longrightarrow A$.*

Demostració: En efecte, la imatge de $1 \in \mathbb{Z}$ ha d'ésser $1 \in A$ i, en conseqüència, la imatge de $n = \overbrace{1 + \cdots + 1}^{n} \in \mathbb{N}$ en A ha d'ésser $n := \overbrace{1 + \cdots + 1}^{n} \in A$ i la de $-n$, $n \in \mathbb{N}$, ha d'ésser $-n \in A$. Així, només cal comprovar que les assignacions $n \mapsto n \in A$, $-n \mapsto -n \in A$, per a $n \in \mathbb{N}$, defineixen un morfisme d'anells; i aquesta comprovació és rutinària. □

Definició 5.5.27. Sigui A un anell. El nucli de l'únic morfisme d'anells $\varphi : \mathbb{Z} \longrightarrow A$ és un ideal i, per tant, un subgrup additiu de $\mathbb{Z}$; per tant, és de la forma $c\mathbb{Z}$, per a un únic nombre enter $c \geq 0$. Aquest nombre enter c s'anomena la característica de l'anell A. Notem que l'anell $A = \{0\}$ és l'únic anell de característica 1, llevat d'un únic isomorfisme.

Observació 5.5.28. En particular, els anells de característica 0 són els anells que contenen un subanell isomorf a $\mathbb{Z}$. En general, el teorema d'isomorfia ens assegura que un anell A conté un subanell isomorf a $\mathbb{Z}/c\mathbb{Z}$, on c és la característica de A.

Exercici 5.5.29. Sigui A un anell de característica $c > 0$. Llavors, c és el menor nombre natural no nul tal que $c \cdot 1 := \overbrace{1 + \cdots + 1}^{c} = 0$ en A. Si A és de característica 0, llavors per a tot nombre natural $c > 0$ és $c \cdot 1 := \overbrace{1 + \cdots + 1}^{c} \neq 0$ en A.

Observació 5.5.30. Notem que si la característica d'un anell és un nombre compost $c = m \cdot n$, amb $m, n \in \mathbb{N}$, $m, n > 1$, els elements $m, n \in A$ són divisors de zero diferents de zero. Per tant, recíprocament, si A és un domini d'integritat, la seva característica és, o bé 0 o bé un nombre primer p.

Exercici 5.5.31. Siguin B un anell i $A \subseteq B$ un subanell. Llavors, les característiques de A i de B coincideixen.

Exercici 5.5.32. Sigui $\varphi : A \longrightarrow B$ un morfisme d'anells. Llavors, la característica de A és un múltiple de la característica de B. En particular, per a $n \geq 1$, no hi ha morfismes d'anell de $\mathbb{Z}/n\mathbb{Z}$ en $\mathbb{Z}$.

Exercici 5.5.33. Siguin A, B anells. La característica de l'anell producte $A \times B$ és el mínim comú múltiple de les característiques de A i de B.

5.6 Monomorfismes. Epimorfismes

Sovint, especialment en contextos no algebraics, s'acostuma a confondre el concepte de morfisme injectiu amb el concepte de monomorfisme, el concepte de morfisme exhaustiu amb el concepte d'epimorfisme, i el concepte de morfisme bijectiu amb el concepte d'isomorfisme. Però aquests conceptes són, de fet, diferents, encara que en alguns casos particulars hi hagi coincidència entre uns tipus de morfismes i uns altres. De fet, els conceptes de monomorfisme, epimorfisme i isomorfisme volen generalitzar, al context de morfismes, els conceptes d'aplicació injectiva, exhaustiva i bijectiva, que es tenen per a aplicacions entre conjunts.

Definició 5.6.1. Sigui $\varphi : Y \longrightarrow Z$ un morfisme de grups. Es diu que φ és un monomorfisme, o també un morfisme mònic, si per a tot grup X i tota parella de morfismes de grups $\psi, \eta : X \longrightarrow Y$ tals que $\varphi \circ \psi = \varphi \circ \eta$ és $\psi = \eta$. Es diu que φ és un epimorfisme, o també un morfisme èpic, si per a tot grup T i tota parella de morfismes de grups $\psi, \eta : Z \longrightarrow T$ tals que $\psi \circ \varphi = \eta \circ \varphi$ és $\psi = \eta$.

Observacions 5.6.2. • Aquests conceptes s'apliquen a morfismes de conjunts; és a dir, a aplicacions qualssevol entre conjunts qualssevol. En aquest cas, es té que monomorfisme equival a aplicació injectiva i epimorfisme equival a aplicació exhaustiva. Proposem la prova com un exercici senzill.

• Aquests conceptes també s'apliquen, per exemple, en el casos de grups abelians, d'anells, de A-mòduls, per a un anell A, de K-espais vectorials, per a un cos K, i en altres contextos més generals que no tractarem aquí. I no s'ha de confondre el concepte de monomorfisme amb el concepte de morfisme injectiu, ni el d'epimorfisme amb el de morfisme exhaustiu, ni el d'isomorfisme amb el de monomorfisme que alhora és epimorfisme. Efectivament, se satisfan els resultats següents, que precisen més els conceptes i les seves equivalències en situacions diverses.

Proposició 5.6.3. *Sigui $\varphi : Y \longrightarrow Z$ un morfisme de grups (o de grups abelians, o d'anells, o de A-mòduls, per a un anell A). Si φ és injectiu (com a aplicació entre conjunts), llavors és un monomorfisme. Si φ és exhaustiu (com a aplicació entre conjunts), llavors és un epimorfisme.*

Demostració: En aquest cas, la demostració és molt senzilla. En efecte, suposem que φ és una aplicació injectiva i que per a morfismes $\psi, \eta : X \longrightarrow Y$ és $\varphi \circ \psi = \varphi \circ \eta$; llavors, per a tot element $x \in X$ és $\varphi(\psi(x)) = \varphi(\eta(x))$ i, per la injectivitat de φ, és $\psi(x) = \eta(x)$; això és $\psi = \eta$, com calia veure. Anàlogament, si suposem que φ és una aplicació exhaustiva i que per a morfismes $\psi, \eta : Y \longrightarrow T$ és $\psi \circ \varphi = \eta \circ \varphi$, donat $y \in Y$, i per l'exhaustivitat de

φ, podem considerar $x \in X$ tal que $y = \varphi(x)$; llavors, $\psi(y) = \psi(\varphi(x)) = \eta(\varphi(x)) = \eta(y)$, de manera que $\psi = \eta$, com calia veure. □

Corol·lari 5.6.4. *Sigui $\varphi : Y \longrightarrow Z$ un isomorfisme de grups (o de grups abelians, o d'anells, o de A-mòduls, per a un anell A). Llavors, φ és un monomorfisme i un epimorfisme.*

Demostració: En els casos de grups, grups abelians, anells, o A-mòduls, hem vist que els isomorfismes són exactament els morfismes bijectius; per tant, són injectius i exhaustius; així, els isomorfismes són monomorfismes i són epimorfismes. □

Proposició 5.6.5. *Sigui $\varphi : Y \longrightarrow Z$ un monomorfisme de grups, de grups abelians, o de A-mòduls, per a un anell A. Llavors, φ és una aplicació injectiva.*

Demostració: En aquests casos, hem vist que la injectivitat del morfisme φ és equivalent al fet que el nucli sigui trivial; o sigui, que $\ker \varphi = \{e\}$, on e és l'element neutre de Y. Considerem, doncs, $X := \ker \varphi$, i siguin $\psi : X \longrightarrow Y$ la inclusió, donada per $x \mapsto x$, per a tot $x \in X$, i $\eta : X \longrightarrow Y$ el morfisme trivial, donat per $x \mapsto e$, per a tot $x \in X$. Llavors, se satisfà que $\varphi \circ \psi = \varphi \circ \eta$ és el morfisme trivial de X en Z. Però si φ és mònic, la igualtat implica que $\psi = \eta$; és a dir, que per a tot $x \in \ker \varphi$ és $x = e$, de manera que el nucli de φ és trivial, com calia veure. □

Observació 5.6.6. Notem que aquest argument no es pot aplicar al cas d'anells, perquè el nucli d'un morfisme d'anells no és un anell. Però el resultat també és cert. Veiem-ho.

Proposició 5.6.7. *Sigui $\varphi : A \longrightarrow B$ un monomorfisme d'anells. Llavors, φ és una aplicació injectiva.*

Demostració: Suposem que φ no és injectiva i veiem que φ no és mònic. Per a això, considerem $C := \{(x, y) \in A \times A : \varphi(x) = \varphi(y)\}$. És immediat comprovar que $C \subseteq A \times A$ és un subanell. Siguin $\psi, \eta : C \longrightarrow A$ les restriccions a C de les projeccions (primera i segona) de $A \times A$ en A; és a dir, $\psi(x, y) := x$, i $\eta(x, y) := y$, per a tot $(x, y) \in C$. Llavors, per la definició de C, és clar que $\varphi \circ \psi = \varphi \circ \eta$. Ara bé, si φ no és injectiu, existeixen $a, b \in A$, $a \neq b$, tals que $\varphi(a) = \varphi(b)$; llavors, $(a, b) \in C$ però $\psi \neq \eta$, perquè $\psi(a, b) = a \neq b = \eta(a, b)$. □

Observació 5.6.8. Així, en els casos de morfismes de grups, de grups abelians, de A-mòduls, per a un anell A, o d'anells, els monomorfismes són exactament els morfismes injectius. Anem a estudiar, ara, el cas dels epimorfismes.

Proposició 5.6.9. *Sigui $\varphi : Y \longrightarrow Z$ un morfisme de grups abelians o de A-mòduls, per a un anell A. Si φ és èpic, llavors φ és una aplicació exhaustiva.*

Demostració: La demostració es pot fer de manera semblant al cas dels morfismes mònics, si ara considerem el conucli del morfisme. En efecte, en el cas de grups abelians o de A-mòduls, la imatge de φ és un subgrup normal de Z o bé un A-submòdul de Z, de manera que té sentit considerar el quocient $Z/\operatorname{im} \varphi$ com a grup abelià, o com a A-mòdul, i considerar dos morfismes $\psi, \eta : Z \longrightarrow Z/\operatorname{im} \varphi$; d'una banda, la projecció canònica $\psi(z) := z + \operatorname{im} \varphi$; i, de l'altra, el morfisme trivial $\eta(z) := 0$. Com que $\psi \circ \varphi = \eta \circ \varphi$ és el morfisme trivial $Y \longrightarrow Z/\operatorname{im} \varphi$, si φ és èpic resulta que $\psi = \eta$; però llavors, per a tot $z \in Z$ és $0 = \eta(z) = \psi(z) = z + \operatorname{im} \varphi$, d'on $z \in \operatorname{im} \varphi$ i φ és una aplicació exhaustiva. □

Observació 5.6.10. Aquest argument tampoc no es pot aplicar al cas de grups, perquè la imatge pot no ser un subgrup normal i, en conseqüència, el grup quocient $Z/\mathrm{im}\,\varphi$ no té sentit. Cal fer un argument diferent, encara que el resultat també és veritat.

Proposició 5.6.11. *Sigui $\varphi : G \longrightarrow H$ un morfisme de grups. Si φ és èpic, llavors φ és una aplicació exhaustiva.*

Demostració: Veiem que si el morfisme φ no és una aplicació exhaustiva, llavors no és un epimorfisme. Per a això, notem que si el subgrup imatge, $\mathrm{im}\,\varphi$, és d'índex menor o igual que 2, llavors és un subgrup normal de H, podem considerar el conucli $H/\mathrm{im}\,\varphi$, i els morfismes projecció $\psi : H \longrightarrow H/\mathrm{im}\,\varphi$ i trivial $\eta : H \longrightarrow H/\mathrm{im}\,\varphi$. Llavors, se satisfà que $\eta \circ \varphi = \psi \circ \varphi$ (i, a més a més, és el morfisme trivial); i si φ és èpic, això implica que $\eta = \psi$, o sigui, que $\mathrm{im}\,\varphi = H$, i φ és una aplicació exhaustiva. Suposem, doncs, que l'índex de $\mathrm{im}\,\varphi$, és com a mínim 3: $[H : \mathrm{im}\,\varphi] \geq 3$. Cal veure que φ no és èpic; o sigui, que podem construir un grup K, i morfismes de grups $\psi, \eta : H \longrightarrow K$, diferents i tals que $\psi \circ \varphi = \eta \circ \varphi$.

Per a això, considerem K com el grup de les permutacions del conjunt H i com a $\psi : H \longrightarrow K$ el morfisme donat per l'acció de H en H per translacions per l'esquerra; és a dir, per a tot $h \in H$, $\psi(h) : H \longrightarrow H$ és la bijecció $x \mapsto h \cdot x$, per a tot $x \in H$. És clar que $\psi(h) \in K$ i que ψ és un morfisme de grups.

Sigui $R \subseteq H$ un conjunt de representants de les classes laterals $\mathrm{im}\,\varphi \cdot h \in \mathrm{im}\,\varphi \backslash H$, $h \in H$, en el qual triem $r_0 := 1 \in R$ com a representant de la classe $\mathrm{im}\,\varphi$; llavors, per a tot element $x \in H$ existeixen elements únics $y \in \mathrm{im}\,\varphi$ i $r \in R$ tals que $x = y \cdot r$. Com que $\#R \geq 3$, podem considerar una permutació π de R tal que tingui algun punt fix però que no sigui la identitat; per exemple, una transposició. I, a més a més, podem triar-la de manera que l'element fix sigui r_0. Així, existeixen $r_0 = 1, r_1 \in R$ tals que $\pi(r_0) = r_0$, i $\pi(r_1) \neq r_1$. I podem estendre aquesta permutació a una permutació de H, $\sigma \in K$, per la fórmula $\sigma(y \cdot r) := y \cdot \pi(r)$, $y \in \mathrm{im}\,\varphi$, $r \in R$. Notem que, amb la tria $r_0 = 1$ i fix per π, la restricció de σ a $\mathrm{im}\,\varphi$ és la identitat.

Posem $\eta : H \longrightarrow K$ l'aplicació donada per $h \mapsto \sigma \circ \psi(h) \circ \sigma^{-1}$. Clarament, η és la composició de ψ amb l'automorfisme intern de conjugació per σ en H; per tant, η és, efectivament, un morfisme de grups.

Ara, notem que per a tot $k \in \mathrm{im}\,\varphi$, se satisfà la commutativitat del diagrama d'aplicacions

$$\begin{array}{ccc} H & \xrightarrow{\sigma} & H \\ {\scriptstyle \psi(k)}\downarrow & & \downarrow{\scriptstyle \psi(k)} \\ H & \xrightarrow[\sigma]{} & H. \end{array}$$

En efecte; per a $x = y \cdot r$, $x \in H$, $y \in \mathrm{im}\,\varphi$, $r \in R$, és

$$(\psi(k) \circ \sigma)(x) = (\psi(k))(\sigma(x)) = k \cdot \sigma(x) = k \cdot (y \cdot \pi(r)) = (k \cdot y) \cdot \pi(r),$$

i

$$(\sigma \circ \psi(k))(x) = \sigma(k \cdot x) = \sigma(k \cdot (y \cdot r)) = \sigma((k \cdot y) \cdot r) = (k \cdot y) \cdot \pi(r),$$

perquè $k \cdot y \in \mathrm{im}\,\varphi$. Això ens diu que, per a $k \in \mathrm{im}\,\varphi$, és $\sigma \circ \psi(k) \circ \sigma^{-1} = \psi(k)$; és a dir, que per a tot $h \in H$ és $\sigma \circ \psi(\varphi(h)) \circ \sigma^{-1} = \psi(\varphi(h))$; o sigui, que $\psi \circ \varphi = \eta \circ \varphi$.

Per a acabar la prova, només resta veure que $\eta \neq \psi$. Però $\psi(r_1)(1) = r_1 \cdot 1 = r_1$, mentre que $\eta(r_1)(1) = (\sigma \circ \psi(r_1) \circ \sigma^{-1})(1) = (\sigma \circ \psi(r_1))(\sigma^{-1}(1)) = (\sigma \circ \psi(r_1))(1) = \sigma(\psi(r_1)(1)) = \sigma(r_1) = \pi(r_1) \neq r_1$, de manera que $\psi \neq \eta$, com calia veure. □

Corol·lari 5.6.12. *Per a grups, per a grups abelians, o per a A-mòduls, per a un anell A, els isomorfismes són exactament els monomorfismes que, alhora, són epimorfismes.* □

Observació 5.6.13. Però en el cas dels morfismes d'anells el resultat corresponent és fals. En efecte, hi ha morfismes èpics que no són exhaustius.

Exercici 5.6.14. Siguin K un domini d'integritat i Q el seu cos de fraccions (cf. **5.3.8**). Llavors, la inclusió canònica $K \longrightarrow Q$, donada per $a \mapsto \dfrac{a}{1}$, és un epimorfisme d'anells. A més a més, és una aplicació injectiva i, si K no és un cos, no és exhaustiva.

Observacions 5.6.15. • El fet que la inclusió canònica de l'anell $\mathbb{Z}$ dels nombres enters en el cos $\mathbb{Q}$ dels nombres racionals sigui un morfisme èpic d'anells es llegeix dient que dos morfismes d'anells de $\mathbb{Q}$ que coincideixen sobre $\mathbb{Z}$ coincideixen sobre $\mathbb{Q}$.

• Així, tampoc no és cert que per a anells, ni tan sols, per a anells commutatius, isomorfisme sigui equivalent a monomorfisme i epimorfisme; en efecte, la inclusió canònica de $\mathbb{Z}$ en $\mathbb{Q}$ és un monomorfisme i un epimorfisme, però no és un isomorfisme.

5.7 Ideals maximals. Ideals primers

Definició 5.7.1. Sigui A un anell. Un ideal $\mathfrak{m} \subseteq A$ s'anomena maximal si, i només si, $\mathfrak{m} \neq A$ i per a tot ideal $\mathfrak{a} \subsetneq A$ tal que $\mathfrak{m} \subseteq \mathfrak{a}$ és $\mathfrak{m} = \mathfrak{a}$. Si el concepte s'aplica a ideals per l'esquerra, es parla d'ideals maximals per l'esquerra; si s'aplica a ideals per la dreta, es parla d'ideals maximals per la dreta, i si s'aplica a ideals bilaterals, es parla d'ideals maximals; en aquest cas, no s'acostuma a fer referència a la bilateralitat.

Exercici 5.7.2. Considerem l'anell $A := \mathbf{M}(2, \mathbb{Q})$ o, més generalment, $A := \mathbf{M}(2, K)$, on K és un cos.

(a) Els únics ideals bilaterals de A són els trivials. En particular, $\{0\}$ és un ideal maximal de A.

(b) El subconjunt $\mathfrak{a} := \begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix} \subseteq A$, és un ideal maximal per l'esquerra de A. Per tant, l'ideal maximal $\{0\}$ no és un ideal maximal per l'esquerra de A.

(c) El subconjunt $\mathfrak{a} := \begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix} \subseteq A$, és un ideal maximal per la dreta de A. Per tant, l'ideal maximal $\{0\}$ no és un ideal maximal per la dreta de A.

Observació 5.7.3. Per tant, un ideal maximal pot no ser un ideal maximal per l'esquerra o no ser un ideal maximal per la dreta. Ara bé, en el cas que l'anell sigui commutatiu, tots els ideals laterals són bilaterals i els tres conceptes coincideixen.

Exercici 5.7.4. Sigui K un anell commutatiu no nul. Un ideal $\mathfrak{m} \subseteq K$ és maximal si, i només si, l'anell quocient $K/\mathfrak{m}$ és un cos.

Teorema 5.7.5. *Siguin A un anell i $\mathfrak{a} \subsetneq A$ un ideal per l'esquerra, diferent del total. Existeix un ideal maximal per l'esquerra $\mathfrak{m} \subseteq A$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$. Si $\mathfrak{a} \subsetneq A$ és un ideal per la dreta, existeix un ideal maximal per la dreta $\mathfrak{m} \subseteq A$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$. I si $\mathfrak{a} \subsetneq A$ és un ideal bilateral, existeix un ideal bilateral maximal $\mathfrak{m} \subseteq A$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$.*

DEMOSTRACIÓ: (Cf. **A.3.7**) És una aplicació del lema de Zorn. El conjunt dels ideals per l'esquerra (o per la dreta, o bilaterals) diferents del total i que contenen $\mathfrak{a}$ és no buit (el mateix ideal $\mathfrak{a}$ hi pertany). Ordenem aquest conjunt per inclusió i veiem que l'ordre és inductiu; en efecte, la reunió d'una cadena d'ideals per l'esquerra (o per la dreta, o bilaterals) que contenen $\mathfrak{a}$ és un ideal per l'esquerra (o per la dreta, o bilateral) que conté $\mathfrak{a}$; i és diferent de A perquè no conté 1. I aquesta reunió és una fita superior de la cadena. Per tant, l'ordre és inductiu. El lema de Zorn garanteix l'existència d'un element maximal en el conjunt corresponent; i aquest element maximal és, per la definició d'ideal maximal, un ideal maximal per l'esquerra (o per la dreta, o bilateral) de A que conté $\mathfrak{a}$. □

Observació 5.7.6. La demostració d'aquest resultat en general fa servir el lema de Zorn; però aquest axioma no és necessari en molts casos. Per exemple, és un exercici senzill provar que a l'anell $\mathbb{Z}$ dels nombres enters els ideals maximals són, exactament, els ideals $p\mathbb{Z}$, on p és un nombre natural primer; i aquest resultat és independent del lema de Zorn.

5.7.7. Per a la definició i les propietats generals dels ideals maximals hem tractat el cas d'un anell qualsevol. Per a parlar dels ideals primers, ens limitarem al cas d'anells commutatius. De fet, per a anells no commutatius, hi ha conceptes diferents que generalitzen els ideals primers del cas commutatiu; però no són necessaris per als objectius d'aquest curs i, per tant, els obviarem.

Definició 5.7.8. Sigui K un anell commutatiu. Un ideal $\mathfrak{p} \subseteq K$ s'anomena primer si, i només si, $\mathfrak{p} \neq K$ i per a $a, b \in K$, $a, b \notin \mathfrak{p}$ és $a \cdot b \notin \mathfrak{p}$. Equivalentment, si $\mathfrak{p} \neq K$ i per a $a, b \in K$, tals que $a \cdot b \in \mathfrak{p}$, és $a \in \mathfrak{p}$ o bé $b \in \mathfrak{p}$.

Observació 5.7.9. Notem que aquest concepte generalitza la propietat aritmètica de l'anell $\mathbb{Z}$ dels nombres enters que si un nombre primer divideix un producte de nombres enters, llavors divideix algun dels factors. En efecte, la relació de divisibilitat $m|n$, entre nombres enters m i n equival a la relacció d'inclusió inversa, $n\mathbb{Z} \subseteq m\mathbb{Z}$; per tant, la relació p divideix $a \cdot b$ és la relació $a \cdot b \in p\mathbb{Z}$, mentre que les relacions p divideix a o p divideix b són les relacions $a \in p\mathbb{Z}$ o $b \in p\mathbb{Z}$.

Exercici 5.7.10. Siguin K un anell commutatiu i $\mathfrak{p} \subseteq K$ un ideal. Llavors:

(a) L'ideal $\mathfrak{p}$ és primer si, i només si, l'anell quocient $K/\mathfrak{p}$ és un domini d'integritat.

(b) L'ideal $\mathfrak{p}$ és maximal si, i només si, l'anell quocient $K/\mathfrak{p}$ és un cos.

(c) Tot ideal maximal de K és un ideal primer.

Exercici 5.7.11. Siguin K un anell commutatiu i $\mathfrak{a} \subseteq K$ un ideal. La bijecció entre el conjunt d'ideals de $K/\mathfrak{a}$ i el conjunt d'ideals de K que contenen $\mathfrak{a}$ que proporciona el morfisme de projecció $K \longrightarrow K/\mathfrak{a}$ transforma ideals primers en ideals primers. És a dir, els ideals primers de $K/\mathfrak{a}$ es corresponen amb els ideals primers de K que contenen $\mathfrak{a}$. I els ideals maximals de $K/\mathfrak{a}$ es corresponen amb els ideals maximals de K que contenen $\mathfrak{a}$.

Exercici 5.7.12. Sigui K un anell commutatiu. Llavors,

$$\bigcup_{\substack{\mathfrak{p}\subseteq K,\\ \text{primer}}} \mathfrak{p} = \bigcup_{\substack{\mathfrak{m}\subseteq K,\\ \text{maximal}}} \mathfrak{m}, \qquad \text{i} \qquad K - \bigcup_{\substack{\mathfrak{p}\subseteq K,\\ \text{primer}}} \mathfrak{p} = K^*.$$

5.8 Anells de fraccions

En tota aquesta secció, els anells seran commutatius i tals que $1 \neq 0$.

Definició 5.8.1. Siguin K un anell commutatiu i $S \subseteq K$ un subconjunt no buit. Direm que S és un subconjunt multiplicativament tancat (o un subconjunt multiplicatiu) si per a tot $s, t \in S$, el producte $s \cdot t \in S$.

Exemples 5.8.2. Sigui K un anell commutatiu tal que $1 \neq 0$.

• Òbviament, $S := K$, $S = \{0\}$, i $S := \{1\}$ són subconjunts multiplicativament tancats; però, en tot allò que segueix, no tindran gaire interès.

• El subconjunt dels elements invertibles de K, $S = K^*$, és multiplicativament tancat. A més a més, $1 \in S$ i $0 \notin S$.

• Sigui $\mathfrak{p} \subseteq K$ un ideal primer. Llavors, el subconjunt complementari, $S := K - \mathfrak{p}$, és multiplicativament tancat. A més a més, $1 \in S$ i $0 \notin S$.

• Més generalment, sigui $\{\mathfrak{p}_i\}_{i \in I}$ una família no buida d'ideals primers de K. Llavors, $S := K - \bigcup_{i \in I} \mathfrak{p}_i$ és un subconjunt multiplicativament tancat. A més a més, $1 \in S$ i $0 \notin S$. Notem que si $\{\mathfrak{p}_i\}_{i \in I}$ és la família de tots els ideals primers de K, llavors $S = K^*$.

• Sigui K un domini d'integritat; llavors, $S := K - \{0\}$ és un subconjunt multiplicativament tancat. A més a més, $1 \in S$ i $0 \notin S$.

• Si $S \subseteq K$ és un subconjunt multiplicativament tancat, llavors $S \cup \{1\}$ també ho és; i si $0 \notin S$, tampoc $0 \notin S \cup \{1\}$; però $1 \in S \cup \{1\}$.

• Sigui $s \in K$ un element qualsevol. El conjunt de les potències de s, $S := \{s^n : n \geq 0\}$, és un subconjunt multiplicativament tancat que conté $1 = s^0$; a més a més, S conté 0 si, i només si, s és nilpotent.

• Sigui $\mathfrak{a} \subsetneq K$ un ideal diferent del total. Llavors, $S := 1 + \mathfrak{a} = \{1 + a \in K : a \in \mathfrak{a}\}$ és un subconjunt multiplicativament tancat que conté 1 i no conté 0.

• Siguin $L \neq \{0\}$ un anell commutatiu, $K \subseteq L$ un subanell, i $S \subseteq K$ un subconjunt multiplicativament tancat de K. Llavors, S també és un subconjunt multiplicativament tancat de L. I les propietats $0 \notin S$, o bé $1 \in S$, no depenen de si mirem S en K o en L.

5.8.3. Siguin K un anell commutatiu tal que $1 \neq 0$ i $S \subseteq K$ un subconjunt multiplicativament tancat. L'objectiu més immediat que ens plantegem és la construcció d'un anell $S^{-1}K$ i un morfisme d'anells, $\psi : K \longrightarrow S^{-1}K$ tal que $\psi(S) \subseteq (S^{-1}K)^*$; és a dir, que tots els elements de S esdevinguin invertibles en $S^{-1}K$. Això generalitzaria la construcció del cos de fraccions d'un domini d'integritat, en què es pren $S = K - \{0\}$ i s'obté un cos Q que conté K com a subanell i de manera que tots els elements no nuls de K esdevenen invertibles en Q; i el morfisme ψ és, en aquest cas, la inclusió de K en Q.

Notem també que si $0 \in S$, llavors l'anell $S^{-1}K$ només pot ser l'anell $\{0\}$, perquè $0 = \psi(0)$ hauria de ser invertible. Per tant, a partir d'ara, suposarem que $0 \notin S$.

Definició 5.8.4. Siguin K un anelll commutatiu tal que $1 \neq 0$, i $S \subseteq K$ un subconjunt multiplicativament tancat tal que $0 \notin S$. Un anell de fraccions de K respecte de S, també anomenat simetritzat de K en S, o, més sovint, localitzat de K en S, és un anell commutatiu $L = S^{-1}K$ juntament amb un morfisme d'anells $\psi : K \longrightarrow L$ tal que

$\psi(S) \subseteq L^*$ i que per a tot morfisme d'anells commutatius $\eta : K \longrightarrow M$ tal que $\eta(S) \subseteq M^*$ existeix un únic morfisme d'anells $\varphi : L \longrightarrow M$ tal que $\eta = \varphi \circ \psi$; és a dir, tal que el diagrama següent és commutatiu:

$$\forall \eta\ \eta(S) \subseteq M^* \implies \exists! \varphi \qquad \begin{array}{ccc} K & \xrightarrow{\psi} & S^{-1}K \\ & \searrow^{\eta} & \downarrow \varphi \\ & & M. \end{array}$$

Diagrama 5.3: Propietat universal de l'anell de fraccions

Exercici 5.8.5 (Unicitat de l'anell simetritzat)**.** Siguin K un anell commutatiu tal que $1 \neq 0$ i $S \subseteq K$ un subconjunt multiplicativament tancat tal que $0 \notin S$. Suposem que $\psi : K \longrightarrow L$ i $\eta : K \longrightarrow M$ són anells de fraccions de K respecte de S. Llavors, existeix un únic morfisme d'anells $\varphi : L \longrightarrow M$ tal que $\varphi \circ \psi = \eta$, i és un isomorfisme.

Teorema 5.8.6 (Existència de l'anell de fraccions)**.** *Siguin K un anell commutatiu tal que $1 \neq 0$ i $S \subseteq K$ un subconjunt multiplicativament tancat, no buit, i tal que $0 \notin S$. Llavors, existeix un anell de fraccions de K respecte de S.*

Demostració: La construcció és similar a la construcció del cos de fraccions d'un domini d'integritat, de la qual n'és una generalització. Volem que els elements de S siguin invertibles en el nou anell; per tant, volem que aquests elements siguin els "denominadors". Considerem, en el conjunt $K \times S$ la relació definida, per a $a, b \in K$, $s, t \in S$, per

$$(a, s) \simeq (b, t) \text{ si, i només si, existeix } x \in S \text{ tal que } (a \cdot t - b \cdot s) \cdot x = 0.$$

Aquesta relació $\simeq$ és, òbviament, reflexiva i simètrica; veiem-ne la transitivitat. Suposem que $(a, s) \simeq (b, t)$, i $(b, t) \simeq (c, u)$, per a $a, b, c \in K$ i $s, t, u \in S$; això és dir que existeixen $x, y \in S$ tals que $(a \cdot t - b \cdot s) \cdot x = 0$, i $(b \cdot u - c \cdot t) \cdot y = 0$. Llavors, $t \cdot x \cdot y \in S$ i $(a \cdot u - c \cdot s) \cdot t \cdot x \cdot y = (a \cdot t - b \cdot s) \cdot u \cdot x \cdot y + (b \cdot u - c \cdot t) \cdot s \cdot x \cdot y = 0$; per tant, $(a, s) \simeq (c, u)$.

Sigui $S^{-1}K$ el conjunt de les classes d'equivalència, classes que representarem en la forma $\dfrac{a}{s}$, per a $a \in K$ i $s \in S$. Notem que, per a tot $a \in K$ i tot $s, t \in S$ és $\dfrac{a}{s} = \dfrac{a \cdot t}{s \cdot t}$.

Ara cal definir una estructura d'anell en $S^{-1}K$; per a això, donades classes $\dfrac{a}{s}, \dfrac{b}{t} \in S^{-1}K$, $a, b \in K$, $s, t \in S$, notem que les classes

$$\frac{a}{s} + \frac{b}{t} := \frac{a \cdot t + b \cdot s}{s \cdot t}, \qquad \frac{a}{s} \cdot \frac{b}{t} := \frac{a \cdot b}{s \cdot t},$$

no depenen dels representants triats en cada classe i que, per tant, podem definir una suma i una multiplicació en $S^{-1}K$ per aquestes fórmules. En efecte, si $\dfrac{a}{s} = \dfrac{a'}{s'}$ i $\dfrac{b}{t} = \dfrac{b'}{t'}$, per a $a, a', b, b' \in K$ i $s, s', t, t' \in S$, llavors existeixen $x, y \in S$ tals que $(a \cdot s' - a' \cdot s) \cdot x = 0$ i $(b \cdot t' - b' \cdot t) \cdot y = 0$. Ara, tenim que $x \cdot y \in S$ que

$$\begin{aligned} \big((a \cdot t + b \cdot s) \cdot s' \cdot t' - & \ (a' \cdot t' + b' \cdot s') \cdot s \cdot t\big) \cdot x \cdot y \\ = & \ (a \cdot s' - a' \cdot s) \cdot x \cdot t \cdot t' \cdot y + (b \cdot t' - b' \cdot t) \cdot y \cdot s \cdot s' \cdot x = 0, \end{aligned}$$

i que

$$\begin{aligned}(a\cdot b\cdot s'\cdot t' - & \ a'\cdot b'\cdot s\cdot t)\cdot x\cdot y\\ = & \ (a\cdot s' - a'\cdot s)\cdot x\cdot b\cdot t'\cdot y + a'\cdot s\cdot x\cdot (b\cdot t' - b'\cdot t)\cdot y = 0.\end{aligned}$$

Com que $S\neq\varnothing$, existeix algun element $s\in S$; llavors, la suma i la multiplicació que acabem de definir determinen una única estructura d'anell commutatiu en $S^{-1}K$, i és tal que l'element neutre de la suma és $0=\dfrac{0}{s}=\dfrac{0}{t}$, per a tot $t\in S$, que l'oposat de $\dfrac{a}{t}$ és $-\dfrac{a}{t}=\dfrac{-a}{t}$, per a tot $a\in K$ i tot $t\in S$, i que l'element neutre de la multiplicació és $1=\dfrac{s}{s}=\dfrac{t}{t}$, per a tot $t\in S$.

A més a més, resulta que l'aplicació $\psi: K\longrightarrow S^{-1}K$, donada per $a\mapsto\dfrac{a\cdot s}{s}$, per a tot $a\in K$ i tot $s\in S$, està ben definida; i és un morfisme d'anells tal que, per a $t\in S$, és $\psi(t)\cdot\dfrac{1}{t}=1$; és a dir, que $\psi(S)\subseteq(S^{-1}K)^*$.

Només resta comprovar la propietat universal. Siguin, doncs, L un anell commutatiu i $\eta: K\longrightarrow L$ un morfisme d'anells tal que $\eta(S)\subseteq L^*$. Donada una classe $\dfrac{a}{s}\in S^{-1}K$, amb $a\in K$ i $s\in S$, resulta que $\eta(s)\in L^*$, i podem definir $\varphi\left(\dfrac{a}{s}\right):=\dfrac{\eta(a)}{\eta(s)}$. Notem que aquesta definició té sentit, perquè si $\dfrac{a}{s}=\dfrac{a'}{s'}$, amb $a,a'\in K$, $s,s'\in S$, existeix $x\in S$ tal que $(a\cdot s'-a'\cdot s)\cdot x=0$; llavors, $\big(\eta(a)\cdot\eta(s')-\eta(a')\cdot\eta(s)\big)\cdot\eta(x)=\eta\big((a\cdot s'-a'\cdot s)\cdot x\big)=0$; i com que $\eta(x)\in L^*$, $\dfrac{\eta(a)}{\eta(s)}=\dfrac{\eta(a')}{\eta(s')}$. És immediata la comprovació que η és un morfisme d'anells. Finalment, per a $a\in K$, és $\varphi(\psi(a))=\varphi\left(\dfrac{a\cdot s}{s}\right)=\dfrac{\eta(a\cdot s)}{\eta(s)}=\dfrac{\eta(a)\cdot\eta(s)}{\eta(s)}=\eta(a)$, com restava comprovar, perquè $\eta(s)$ és invertible. □

Observacions 5.8.7. Siguin K un anell commutatiu tal que $1\neq 0$ i $S\subseteq K$ un subconjunt multiplicativament tancat tal que $0\notin S$.

• L'anell de fraccions de K respecte de S es denota, sovint, per $S^{-1}K$. En el cas que $S=K-\mathfrak{p}$ és el complementari d'un ideal primer $\mathfrak{p}\subseteq K$, a vegades s'escriu $K_{\mathfrak{p}}$ en lloc de $S^{-1}K$.

• Notem que si $T:=S\cup\{1\}$, llavors $T^{-1}K=S^{-1}K$, de manera que, en parlar d'anells de fraccions, podrem suposar que $1\in S$.

• Notem que si $\psi: K\longrightarrow S^{-1}K$ és el morfisme canònic, no només els elements de S, sinó també els elements invertibles de K es transformen en elements invertibles de $S^{-1}K$. En efecte, si $u\in K^*$, llavors $\psi_(u)\in(S^{-1}K)^*$.

• Si S no conté cap divisor de zero de K, llavors ψ és un morfisme injectiu. En efecte, si per a $a\in K$ és $\psi(a)=0$, llavors $\dfrac{a\cdot s}{s}=\dfrac{0}{s}$, de manera que existeix $u\in S$ tal que $(a\cdot s\cdot s-0\cdot s)\cdot u=0$; és a dir, $a\cdot x=0$, per a $x:=s\cdot s\cdot u\in S$. I com que x no és divisor de zero (perquè S no en conté cap, per hipòtesi), resulta que $a=0$, com calia veure.

• Més generalment, $\ker\psi$ és el conjunt format pels elements de K que són ortogonals als elements de S; és a dir, per a $a\in K$, és $\psi(a)=0$ si, i només si, existeix $u\in S$ tal que $a\cdot u=0$.

• Tot element de $S^{-1}K$ és de la forma $\psi(a) \cdot \psi(s)^{-1}$, per a algun $a \in K$ i algun $s \in S$.

Exercici 5.8.8. Siguin K un anell commutatiu tal que $1 \neq 0$, $S \subseteq K$ un subconjunt multiplicativament tancat, no buit, i tal que $0 \notin S$, i $\psi : K \longrightarrow S^{-1}K$ el morfisme canònic, donat per l'assignació $a \mapsto \dfrac{a \cdot s}{s}$, per a tot $a \in K$ i algun $s \in S$. Llavors, ψ és un epimorfisme d'anells.

Exercici 5.8.9. Siguin K un domini d'integritat, Q el cos de fraccions de K, i $S \subseteq K$ un subconjunt multiplicativament tancat, no buit, i tal que $0 \notin S$. Llavors, es tenen inclusions canòniques d'anells, $K \subseteq S^{-1}K \subseteq Q$, i Q també és el cos de fraccions de $S^{-1}K$. De fet, $S^{-1}K$ és el subconjunt dels elements $\dfrac{a}{s} \in Q$ tals que $a \in K$ i $s \in S$.

Exercici 5.8.10. Sigui $p \in \mathbb{Z}$ un nombre primer. Llavors, per a $S := \mathbb{Z} - p\mathbb{Z}$, el complementari de l'ideal primer $p\mathbb{Z}$, es té que

$$S^{-1}\mathbb{Z} = \mathbb{Z}_{p\mathbb{Z}} = \left\{ \frac{a}{s} : a, s \in \mathbb{Z}, s \notin p\mathbb{Z} \right\} \subseteq \mathbb{Q};$$

és a dir, el subconjunt dels nombres racionals de denominador no divisible per p.

Exercici 5.8.11. Siguin $s \in \mathbb{Z}$ un nombre enter no nul i $S := \{s^n : n \geq 0\}$, el conjunt de les potències de s. Llavors,

$$S^{-1}\mathbb{Z} = \mathbb{Z}\left[\frac{1}{s}\right] = \left\{ \frac{a}{s^n} : a \in \mathbb{Z}, n \geq 0 \right\} \subseteq \mathbb{Q};$$

és a dir, el subconjunt dels nombres racionals de denominador potència de s.

Exercici 5.8.12. Siguin $n \in \mathbb{Z}$, $n \geq 2$, un nombre enter i $S := 1+n\mathbb{Z} = \{1+a\cdot n : a \in \mathbb{Z}\}$, el conjunt dels nombres enters congrus amb 1 mòdul n. Llavors,

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{s} : a, s \in \mathbb{Z},\ s \equiv 1 \pmod{n} \right\} \subseteq \mathbb{Q};$$

és a dir, el subconjunt dels nombres racionals de denominador congru amb 1 mòdul n. L'anell $S^{-1}\mathbb{Z}$ també es pot descriure com el subanell dels nombres racionals de denominador s tal que $\mathrm{mcd}(s, n) = 1$.

Capítol 6

Factorialitat

El teorema fonamental de l'Aritmètica assegura que tot nombre enter no nul és producte de nombres primers, i que, llevat del signe i de l'ordre, aquesta descomposició és única. Aquest fet no és exclusiu dels nombres enters i també se satisfà, per exemple, en els anells de polinomis de coeficients en un cos. Però cal anar amb compte amb els conceptes. De fet, la descomposició no és tant com a producte d'elements primers com a producte d'elements irreductibles. Dediquem aquest capítol a fer un estudi d'aquestes qüestions. En particular, aprofitem per a fer una construcció formal dels anells de polinomis (cf. **1.6.6**) i dels anells de sèries de potències.

6.1 Anells de polinomis

Definició 6.1.1. Sigui A un anell. Podem considerar el conjunt P_A de totes les successions $(a_0, a_1, \dots, a_n, 0, \dots)$ d'elements de A que, a partir d'un lloc, només contenen l'element 0; un cop haurem establert una estructura d'anell en P_A, els anomenarem polinomis de coeficients en A. Els components de la successió s'anomenen els coeficients del polinomi i els polinomis dels quals només un coeficient és diferent de zero s'anomenen monomis. Donats polinomis

$$\alpha = (a_0, a_1, \dots, a_n, 0, \dots),\ \beta = (b_0, b_1, \dots, b_m, 0, \dots) \in P_A,$$

definim la seva suma

$$\alpha + \beta := (a_0 + b_0, a_1 + b_1, \dots, a_t + b_t, \dots) \in P_A$$

i el seu producte

$$\alpha\beta := (c_0, c_1, \dots, c_r, \dots) \in P_A,$$

on

$$c_r := \sum_{i+j=r} a_i b_j, \qquad r \geq 0.$$

Notem que per a $t > \max\{m, n\}$ és $a_t + b_t = 0$ i que per a $r > n + m$ és $c_r = 0$, de manera que, efectivament, tant la suma com el producte de polinomis estan definits com a operacions binàries en el conjunt P_A.

Proposició 6.1.2. *El conjunt P_A, amb la suma i el producte que acabem de definir, admet una única estructura d'anell, que és commutatiu si A és commutatiu; els elements neutres de la suma i del producte són, respectivament, els polinomis*

$$0 = (0, 0, \dots, 0, \dots) \qquad \text{i} \qquad 1 = (1, 0, \dots, 0, \dots).$$

Demostració: Exercici. □

Observació 6.1.3. Com que la suma en P_A es defineix component a component, com a grup additiu, P_A és la suma directa d'una quantitat numerable de còpies del grup additiu de A; és a dir, P_A és un subgrup del grup producte d'una quantitat numerable de còpies del grup additiu de A. Però el producte en P_A no es defineix component a component; per tant, l'anell de polinomis tampoc no es pot pensar com a subanell de l'anell producte d'una quantitat numerable de còpies de l'anell A (cf. la proposició **5.4.3**).

Definició 6.1.4. L'aplicació $A \longrightarrow P_A$ definida per $a \mapsto (a, 0, \dots, 0, \dots)$ és un morfisme injectiu d'anells, de manera que permet identificar A com un subanell de P_A. Els elements de A, pensats com a polinomis, s'anomenen els polinomis constants.

Definició 6.1.5. Llevat del polinomi 0, tot altre polinomi té algun coeficient diferent de zero; i com que tots els coeficients són zero d'un lloc endavant, podem considerar el màxim dels índexs n tal que $a_n \neq 0$; aquest nombre natural n s'anomena el grau del polinomi, i el coeficient n-èsim s'anomena el coeficient dominant o principal del polinomi. Convé definir el grau del polinomi 0 com $-\infty$, amb les convencions habituals, en aquests casos, que per a tot nombre natural n és $-\infty < n$, $-\infty + n = n + (-\infty) = -\infty$, i $-\infty + (-\infty) = -\infty$.

Definició 6.1.6. De la definició de polinomi es dedueix de seguida que el grau d'una suma és menor o igual que el màxim dels graus dels sumands i que el grau d'un producte és menor o igual que la suma dels graus dels factors. En general, cap de les dues desigualtats no és una igualtat. D'altra banda, els polinomis constants són el polinomi 0 i els polinomis de grau 0. Un polinomi s'anomena mònic si el seu coeficient principal, és a dir, el coeficient del seu monomi no nul de grau màxim, és 1 o bé, més generalment, un element invertible $a \in A^*$.

Definició 6.1.7. S'acostuma a donar un nom al polinomi $(0, 1, 0, \dots, 0, \dots)$; si s'anomena $X := (0, 1, 0, \dots, 0, \dots)$, llavors s'escriu $A[X]$ en lloc de P_A i es diu que $A[X]$ és l'anell de polinomis en la indeterminada X i de coeficients en A. Així, la indeterminada X és un polinomi; de fet, és el monomi mònic de grau 1 (i coeficients en A).

Exercici 6.1.8. Sigui K un domini d'integritat. Llavors, l'anell de polinomis $K[X]$ és un domini d'integritat; i si $f(X), g(X) \in K[X]$ són polinomis diferents de zero, llavors $\operatorname{gr}(f(X) \cdot g(X)) = \operatorname{gr}(f(X)) + \operatorname{gr}(g(X))$.

Exercici 6.1.9. Per a qualsevol anell A, en $A[X]$ se satisfà la igualtat

$$(a_0, a_1, \dots, a_n, 0, \dots) = a_0 + a_1 \cdot X + \cdots + a_n \cdot X^n;$$

per tant, tot polinomi s'escriu de manera única en la forma

$$a_0 + a_1 \cdot X + \cdots + a_n \cdot X^n, \qquad a_0, \dots, a_n \in A;$$

és a dir, per a tot polinomi existeix $n \geq 0$ i existeixen $a_0, \dots, a_n \in A$, únics tals que el polinomi és $a_0 + a_1 \cdot X + \cdots + a_n \cdot X^n$.

Exercici 6.1.10. Siguin A un anell i $Z \subseteq A$ un subanell qualsevol. Llavors, $Z[X] \subseteq A[X]$ és un subanell.

Exercici 6.1.11. El polinomi X pertany al centre de l'anell de polinomis $A[X]$; encara més, si tots els coeficients $a_i \in A$ d'un polinomi $f(X) = a_0 + a_1 \cdot X + \cdots + a_n \cdot X^n \in A[X]$ pertanyen al centre de l'anell A, llavors $f(X)$ pertany al centre de $A[X]$. Més generalment, si A és un anell i $Z \subseteq A$ és el centre de A, llavors, el centre de $A[X]$ és $Z[X]$.

Proposició 6.1.12. *Siguin A i B anells i $\varphi : A \longrightarrow B$ un morfisme d'anells. Existeix un únic morfisme d'anells $\widetilde{\varphi} : A[X] \longrightarrow B[X]$ tal que $\widetilde{\varphi}(X) = X$ i que per a tot $a \in A$ és $\widetilde{\varphi}(a) = \varphi(a)$. Aquest morfisme $\widetilde{\varphi}$ s'anomena l'extensió de φ a $A[X]$.*

Demostració: La unicitat de l'expressió d'un polinomi com a combinació lineal de les potències de X i coeficients en A permet definir el valor de $\widetilde{\varphi}$ sobre un polinomi simplement per aplicació de φ als coeficients del polinomi:

$$a_0, \ldots, a_n \in A, \qquad a_0 + a_1 \cdot X + \cdots + a_n \cdot X^n \mapsto \varphi(a_0) + \varphi(a_1) \cdot X + \cdots + \varphi(a_n) \cdot X^n;$$

i es comprova sense cap dificultat que aquesta definició proporciona un morfisme d'anells com el que es demana. □

Definició 6.1.13. Donat un anell A, definim per inducció l'anell de polinomis en les indeterminades $X_1, \ldots, X_n$ com

$$A[X_1, \ldots, X_n] := A[X_1, \ldots, X_{n-1}][X_n];$$

és a dir, $A[X_1, \ldots, X_n]$ és l'anell de polinomis en la indeterminada X_n i de coeficients en l'anell $A[X_1, \ldots, X_{n-1}]$.

Proposició 6.1.14. *Tot polinomi en les indeterminades $X_1, \ldots, X_n$ s'escriu de manera única en la forma*

$$\sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}, \qquad a_{i_1, \ldots, i_n} \in A,$$

en la qual tots els elements $a_{i_1, \ldots, i_n}$ llevat d'una quantitat finita, són 0 i on, per comoditat de notació, denotarem el producte per juxtaposició en lloc d'utilitzar un punt volat. □

Definició 6.1.15. Amb les notacions anteriors, els elements $a_{i_1, \ldots, i_n}$ s'anomenen els coeficients del polinomi.

Observació 6.1.16. Siguin A un anell i B un conjunt, qualssevol. Es pot construir un anell de polinomis $A[B]$, amb B com a conjunt d'indeterminades, de manera que:

(a) $A[B]$ conté com a subanells els anells de polinomis $A[X_1, \ldots, X_n]$, per a tots els subconjunts finits $\{X_1, \ldots, X_n\} \subseteq B$;

(b) $A[B]$ és la reunió d'aquesta família de subanells; i

(c) el conjunt B és un subconjunt del centre de l'anell $A[B]$; és a dir, les indeterminades commuten amb tots els polinomis.

No ens entretindrem en els detalls de la construcció.

Observacions 6.1.17. • Sigui A un anell. En el conjunt de successions d'elements de A, $S_A := A^{\mathbb{N}} = \{(a_n)_{n\geq 0} : a_n \in A\}$, es defineix la suma de successions de la manera usual, component a component, i es defineix un producte de manera que, donades successions $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0} \in S_A$, el seu producte és $(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (c_n)_{n\geq 0}$, on

$$c_n := \sum_{k=0}^{n} a_k \cdot b_{n-k} = \sum_{i+j=n} a_i \cdot b_j$$

(notem la similitud d'aquesta definició amb el producte de polinomis). Això determina una única estructura d'anell en S_A, amb 0 la successió constant de valor $0 \in A$, i 1 la successió $(a_n)_{n\geq 0}$ donada per $a_0 = 1$, i $a_n = 0$, per a $n > 0$. Aquest anell s'anomena l'anell de sèries de potències de coeficients en A, i és commutatiu si, i només si, A és commutatiu.

• Si es posa $X := (0, 1, 0, \dots, 0, \dots) \in S_A$, l'anell S_A es denota per $A[[X]]$. Es té que X és un element central de l'anell, i que, per a tot $n \geq 0$, és $X^n = (0, \dots, 0, 1, 0, \dots)$, amb 1 a la posició n-èsima (notem que la sèrie 1 té l'element $1 \in A$ en la posició 0-èsima).

• Una sèrie $(a_n)_{n\geq 0} \in A[[X]]$ es representa en la forma $(a_n)_{n\geq 0} =: \sum_{n\geq 0} a_n X^n$, i l'element $a_n \in A$ s'anomena el n-èsim coeficient de la sèrie.

• L'aplicació $A \longrightarrow A[[X]]$ donada per $a \mapsto (a, 0, \dots, 0, \dots)$ és un morfisme injectiu d'anells que identifica A amb un subanell de $A[[X]]$.

• Més generalment, l'anell de polinomis $A[X]$ és el subanell de $A[[X]]$ format per les sèries els coeficients de les quals són zero d'un lloc endavant o, dit d'una altra manera, amb només una quantitat finita de coeficients no nuls.

• Donada una sèrie no nul·la, $f(X) := \sum_{n\geq 0} a_n X^n$, s'anomena ordre de la sèrie, i es representa per $\operatorname{ord}(f(X))$, el mínim nombre natural $m \geq 0$ tal que $a_m \neq 0$. Usualment, es fa servir la notació $f(X) := \sum_{n\geq m} a_n X^n$. Se sol escriure $\operatorname{ord}(0) = +\infty$. Notem que per a sèries $f(X)$, $g(X) \in A[[X]]$, se satisfà que $\operatorname{ord}\big(f(X) \cdot g(X)\big) \geq \operatorname{ord}\big(f(X)\big) + \operatorname{ord}\big(g(X)\big)$, amb les convencions habituals, $+\infty + (+\infty) = n + (+\infty) = +\infty + n = +\infty$, i $+\infty > n$, per a $n \in \mathbb{N}$, amb igualtat si els coeficients que determinen l'ordre no són ortogonals; en particular, si l'anell A no té divisors de zero.

• Notem que, en particular, podem parlar de l'ordre d'un polinomi; però en general no podem parlar del grau d'una sèrie de potències.

• Per inducció, es defineixen els anells de sèries en n indeterminades, $A[[X_1, \dots, X_n]] := A[[X_1, \dots, X_{n-1}]][[X_n]]$. Les indeterminades $X_1, \dots, X_n$, són elements centrals de l'anell de sèries.

Exercici 6.1.18. El polinomi $1 - X$ és invertible en l'anell de sèries $A[[X]]$, amb invers donat per la sèrie $\sum_{n\geq 0} X^n$. Més generalment, per a tot element $a \in A$, la sèrie (polinomi) $1 - aX$ és invertible amb inversa la sèrie $\sum_{n\geq 0} a^n X^n$.

6.2 Àlgebres

Definició 6.2.1. Sigui K un anell commutatiu, no nul. Una K-àlgebra associativa i unitària és un anell E amb una acció de K en E compatible amb les operacions de l'anell E en el sentit que tot seguit especifiquem. Denotem les operacions binàries de l'anell E per $+$ i $\circ$, i l'acció $K \times E \longrightarrow E$ per $(\lambda, f) \mapsto \lambda f$, o sigui, per juxtaposició i sense el punt volat, que, en aquesta definició, reservem per al producte de K. Així, amb aquesta acció de K en l'anell E, el grup commutatiu additiu de E és un K-mòdul i, a més a més, se satisfà que per a tots els elements $\lambda, \mu \in K$, $f, g \in E$, és $(\lambda f) \circ (\mu g) = (\lambda \cdot \mu)(f \circ g)$. Aquesta darrera propietat es pot substituir de manera equivalent per la propietat que per a tot $\lambda \in K$ i tots els elements $f, g \in E$, és $(\lambda f) \circ g = \lambda(f \circ g) = f \circ (\lambda g)$. Si l'anell E és commutatiu, es parla d'una àlgebra associativa, unitària i commutativa.

Observacions 6.2.2. • Notem les diferències entre les compatibilitats amb la suma i amb el producte de E que demanem a l'acció de K. D'una banda, demanem que l'acció distribueixi la suma de E: $\lambda(f + g) = \lambda f + \lambda g$; en canvi, per al producte, demanem que l'acció s'hi associï amb qualsevol dels dos factors: $\lambda(f \circ g) = (\lambda f) \circ g = f \circ (\lambda g)$.

Això és similar a allò que succeeix amb l'acció respecte el producte i la suma de K; d'una banda, l'acció distribueix la suma de K: $(\lambda + \mu)f = \lambda f + \mu f$; i, en canvi, s'associa amb el producte: $(\lambda \cdot \mu)f = \lambda(\mu f)$.

• Tot i que es pot definir el concepte de A-àlgebra sobre un anell A no necessàriament commutatiu, ens limitem a fer-ho sobre anells commutatius. Notem que la propietat de compatibilitat amb el producte implica que, per a $\lambda, \mu \in A$, $f, g \in E$, és

$$\begin{aligned}(\lambda \cdot \mu)(f \circ g) = \lambda\big(\mu(f \circ g)\big) \;&= \lambda\big(f \circ (\mu g)\big) = (\lambda f) \circ (\mu g) \\ &= \mu\big((\lambda f) \circ g\big) = \mu\big(\lambda(f \circ g)\big) = (\mu \cdot \lambda)(f \circ g);\end{aligned}$$

per tant, en prendre $f = g = 1$, obtenim que el subanell $A1 \subseteq E$, que és l'òrbita de l'element $1 \in E$, és un subanell commutatiu de E, encara que A no sigui commutatiu. No ens entretindrem en aquestes consideracions, que no calen si A és commutatiu.

Exemples 6.2.3. • Tot anell A, commutatiu o no, és una $\mathbb{Z}$-àlgebra associativa i unitària. És commutativa si, i només si, A és commutatiu.

• Sigui K un anell commutatiu. L'anell de polinomis en una indeterminada X, $K[X]$, és una K-àlgebra (associativa i unitària). També ho és l'anell de sèries de potències, $K[[X]]$.

• Més generalment, l'anell de polinomis $K[X_1, \ldots, X_n]$ i l'anell de sèries $K[[X_1, \ldots, X_n]]$ també són K-àlgebres.

• De fet, si L és un anell i K és un subanell del centre de L, llavors L és una K-àlgebra de la manera òbvia natural: l'estructura d'anell és la de L, i l'acció de K en L és donada per la multiplicació d'elements de K per elements de L que es dedueix de la multiplicació de L per restricció del primer factor a K.

• En particular, si K és un anell commutatiu, l'anell de polinomis $K[X_1, \ldots, X_n]$ també és una $K[X_1, \ldots, X_i]$-àlgebra, per a $0 \leq i \leq n$.

• Sigui K un anell commutatiu. Per a tot $n \geq 1$, el K-mòdul de les matrius quadrades de n files i n columnes i coeficients en K, $\mathbf{M}(n, K)$, és una K-àlgebra (associativa i unitària), amb el producte habitual de matrius: per a $A = [a_{i,j}]_{1 \leq i,j \leq n}, B = [b_{i,j}]_{1 \leq i,j \leq n} \in \mathbf{M}(n, K)$, el producte de matrius és la matriu $C = B \cdot A = [c_{i,j}]_{1 \leq i,j \leq n} \in \mathbf{M}(n, K)$ donada per $c_{i,j} = \sum_{k=1}^{n} b_{i,k} \cdot a_{k,j}$.

• Sigui K un anell commutatiu. Si E és un K-mòdul qualsevol, el K-mòdul dels endomorfismes de E és una K-àlgebra (associativa i unitària), amb la composició habitual d'endomorfismes com a producte en E. S'acostuma a denotar per $\mathrm{End}_K(E)$.

Definició 6.2.4. Siguin K un anell commutatiu i E i F, K-àlgebres (associatives i unitàries). Un morfisme de K-àlgebres (associatives i unitàries) de E en F és una aplicació $\varphi : E \longrightarrow F$ que és alhora un morfisme d'anells i una aplicació K-lineal.

Observació 6.2.5. Com que la imatge d'un morfisme d'anells és un subanell i la imatge d'una aplicació lineal és un submòdul, és clar que la imatge d'un morfisme de K-àlgebres és una K-subàlgebra, amb la definició òbvia de K-subàlgebra com a K-submòdul que, alhora, és un subanell. Notem que la compatibilitat de l'acció i el producte se satisfà automàticament.

D'altra banda, el nucli d'un morfisme de K-àlgebres $\varphi : E \longrightarrow F$ és, en particular, un K-submòdul de E, de manera que té sentit el K-mòdul quocient $E/\ker\varphi$. Aquest K-mòdul és, de manera natural, una K-àlgebra associativa i unitària, amb el producte de classes definit prenent representants. I la projecció $\pi : E \longrightarrow E/\ker\varphi$ és un morfisme de K-àlgebres. I se satisfà el teorema d'isomorfia $E/\ker\varphi \cong \mathrm{im}\,\varphi$, com a K-àlgebres. El morfisme φ factoritza com la composició de morfismes de K-àlgebres

$$\begin{array}{ccc} E & \xrightarrow{\ \varphi\ } & F \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle incl} \\ E/\ker f & \xrightarrow[\ \overline{\varphi}\ ]{} & \mathrm{im}\,\varphi, \end{array}$$

Diagrama 6.1: Primer teorema d'isomorfia de K-àlgebres

on π és la projecció, *incl* és la inclusió, i $\overline{\varphi}$ és l'isomorfisme donat pel teorema d'isomorfia.

Proposició 6.2.6. *Siguin K un anell commutatiu i E una K-àlgebra (associativa i unitària). Per a tot element $v \in E$ existeix un únic morfisme de K-àlgebres (associatives i unitàries) $\varphi_v : K[X] \longrightarrow E$ tal que $\varphi_v(X) = v$.*

Demostració: Donat un polinomi qualsevol, $f(X) = \sum_{k=0}^{n} \lambda_k \cdot X^k$, $\lambda_k \in K$, $0 \leq k \leq n$, l'expressió $f(v) := \sum_{k=0}^{n} \lambda_k \cdot v^k$ determina un únic element de E; podem, doncs, definir una aplicació $\varphi_v : K[X] \longrightarrow E$ per l'assignació $\varphi_v(f(X)) := f(v)$. Se satisfà que φ_v és un morfisme de K-àlgebres (associatives i unitàries) i que $\varphi_v(X) = v$ (això prova l'existència); i també que si un morfisme de K-àlgebres (associatives i unitàries), posem $\psi : K[X] \longrightarrow E$, és tal que $\psi(X) = v$, llavors és $\psi(f(X)) = f(v)$; i això prova la unicitat. □

Definició 6.2.7. Aquest morfisme φ_v sovint és anomenat el morfisme d'avaluació en v o, més informalment, "morfisme de donar el valor v a X".

Definició 6.2.8. Siguin K un anell commutatiu i B un conjunt qualssevol. Una K-àlgebra (associativa, unitària i commutativa) lliure de base B és una K-àlgebra (associativa, unitària i commutativa) $L(B)$ i una aplicació de conjunts $\psi : B \longrightarrow L(B)$ tals que per a

tota K-àlgebra (associativa, unitària i commutativa) E i tota aplicació $f : B \longrightarrow E$, de conjunts, existeix un únic morfisme de K-àlgebres (associatives, unitàries i commutatives) $\varphi : L(B) \longrightarrow E$ tal que $\varphi \circ \psi = f$.

$$\forall f\ \exists!\varphi \qquad \begin{array}{ccc} B & \xrightarrow{\psi} & L(B) \\ & \searrow^{f} & \downarrow{\scriptstyle \varphi} \\ & & E \end{array}$$

Diagrama 6.2: Definició de K-àlgebra (associativa, commutativa i unitària) lliure

Observació 6.2.9. Suposem que $\psi : B \longrightarrow L(B)$, $\psi' : B \longrightarrow L'(B)$ són K-àlgebres (associatives, unitàries i commutatives) lliures de base B. Llavors, existeix un únic morfisme de K-àlgebres (associatives, unitàries i commutatives), $\varphi : L(B) \longrightarrow L'(B)$, tal que $\psi' = \varphi \circ \psi$; i, a més a més, φ és un isomorfisme.

Corol·lari 6.2.10. *Sigui K un anell commutatiu. La K-àlgebra de polinomis $K[X]$ és lliure de base $\{X\}$, com a K-àlgebra associativa, unitària i commutativa, i també com a K-àlgebra asssociativa i unitària, no necessàriament commutativa.* □

Exercici 6.2.11. Sigui K un anell commutatiu. La K-àlgebra $K[X_1, \ldots, X_n]$ és lliure de base $\{X_1, \ldots, X_n\}$, com a K-àlgebra associativa, unitària i commutativa.

Observació 6.2.12. Notem que $X_i \cdot X_j = X_j \cdot X_i$, de manera que per a qualsevol morfisme de K-àlgebres $\varphi : K[X_1, \ldots, X_n] \longrightarrow E$, ha de ser $\varphi(X_i) \cdot \varphi(X_j) = \varphi(X_j) \cdot \varphi(X_i)$. Això fa que, si $n > 1$, $K[X_1, \ldots, X_n]$ no sigui una K-àlgebra associativa i unitària lliure de base $\{X_1, \ldots, X_n\}$; només és lliure per a les K-àlgebres associatives, unitàries i commutatives. No ens entretindren a fer l'estudi de les àlgebres lliures (no necessàriament commutatives).

Exercici 6.2.13. Siguin K un anell commutatiu i B un conjunt, qualssevol. L'anell de polinomis $K[B]$ és la K-àlgebra associativa, unitària i commutativa lliure de base B.

6.3 Divisió de polinomis

Proposició 6.3.1 (Divisió de polinomis)**.** *Siguin K un cos i $f(X), g(X) \in K[X]$, polinomis tals que $g(X) \neq 0$. Llavors, existeixen polinomis $q(X), r(X) \in K[X]$, únics tals que $f(X) = g(X) \cdot q(X) + r(X)$ i $\operatorname{gr}(r(X)) < \operatorname{gr}(g(X))$.*

Demostració: En el cas que $\operatorname{gr}(f(X)) < \operatorname{gr}(g(X))$, l'existència és gairebé immediata. En efecte, posem $q(X) := 0$, $r(X) := f(X)$; llavors, és clar que se satisfan les propietats enunciades: $f(X) = g(X) \cdot q(X) + r(X)$ i $\operatorname{gr}(r(X)) < \operatorname{gr}(g(X))$. Suposem, doncs, que $\operatorname{gr}(f(X)) \geq \operatorname{gr}(g(X))$.

Siguin $f(X) =: a_0 + a_1X + \cdots + a_nX^n$, $a_0, a_1, \ldots, a_n \in K$, $g(X) =: b_0 + b_1X + \cdots + b_mX^m$, $b_0, b_1, \ldots, b_m \in K$, amb $a_n \neq 0$, $b_m \neq 0$, i $n \geq m$. Llavors, el polinomi

$$f(X) - g(X)\frac{a_n}{b_m}X^{n-m} =: c_0 + c_1X + \cdots + c_{n-1}X^{n-1},$$

on $c_0, \ldots, c_{n-1} \in K$, és de grau estrictament menor que el grau, n, de $f(X)$; repetint el mateix procés, el polinomi

$$f(X) - g(X)\frac{a_n}{b_m}X^{n-m} - g(X)\frac{c_{n-1}}{b_m}X^{n-m-1} = \\ = f(X) - g(X)\left(\frac{a_n}{b_m}X^{n-m} - \frac{c_{n-1}}{b_m}X^{n-m-1}\right)$$

és un polinomi de grau menor o igual que $n-2$. Doncs, podem calcular recursivament un polinomi

$$q(X) := \frac{a_n}{b_m}X^{n-m} - \frac{c_{n-1}}{b_m}X^{n-m-1} + \cdots .$$

El procés s'atura quan el grau de la diferència $f(X) - g(X)q(X)$ és menor que el grau, m, de $g(X)$. Definim el polinomi $r(X)$ com aquesta diferència: $r(X) := f(X) - g(X)q(X)$. Llavors, les propietats enunciades se satisfan per definició de $q(X)$ i de $r(X)$.

Demostrem, ara, la unicitat. Suposem que

$$f(X) = g(X)q_1(X) + r_1(X), \qquad \operatorname{gr}(r_1(X)) < \operatorname{gr}(g(X)),$$

$$= g(X)q_2(X) + r_2(X), \qquad \operatorname{gr}(r_2(X)) < \operatorname{gr}(g(X)),$$

on $q_1(X)$, $q_2(X)$, $r_1(X)$, $r_2(X) \in K[X]$. Es té que $r_2(X) - r_1(X) = g(X)(q_1(X) - q_2(X))$, de manera que el grau de $r_2(X) - r_1(X)$, que és menor estricte que el grau de $g(X)$, coincideix amb el grau del producte del polinomi $g(X)$ pel polinomi $q_1(X) - q_2(X)$; però, si $q_1(X) - q_2(X) \neq 0$, el grau d'aquest producte és la suma dels graus dels dos factors, de manera que és més gran o igual que el grau de $g(X)$. Aquesta contradicció obliga que sigui $q_1(X) = q_2(X)$ i, en conseqüència, $r_1(X) = r_2(X)$, com volíem provar. □

Observació 6.3.2. Un repàs acurat d'aquesta demostració ens ensenya que si no suposem que K sigui un cos, sinó només un anell commutatiu qualsevol, però, en canvi, suposem que b_m és un element invertible de K, llavors el procés de la divisió es vàlid sense cap modificació; per tant, a més a més d'obtenir un algoritme per a calcular el quocient i el residu de la divisió entera de polinomis, hem demostrat també el resultat següent.

Corol·lari 6.3.3. *Sigui K un anell commutatiu. Donats polinomis $f(X)$, $g(X) \in K[X]$ tals que $g(X)$ és mònic (i, per tant, $g(X) \neq 0$), existeixen polinomis $q(X)$, $r(X) \in K[X]$ únics tals que $f(X) = g(X)q(X) + r(X)$ i $\operatorname{gr}(r(X)) < \operatorname{gr}(g(X))$.* □

Definició 6.3.4. Una expressió de la forma $f(X) = g(X)q(X) + r(X)$, on $f(X)$, $g(X)$, $q(X)$, $r(X) \in K[X]$, $g(X)$ mònic, i $\operatorname{gr}(r(X)) < \operatorname{gr}(g(X))$, s'anomena la divisió entera (o, simplement, divisió) de $f(X)$ per $g(X)$; els polinomis $q(X)$ i $r(X)$ s'anomenen, respectivament, el quocient i el residu de la divisió entera, mentre que $f(X)$ i $g(X)$ s'anomenen el dividend i el divisor.

Observació 6.3.5. Si l'anell K no fós commutatiu, caldria donar sentit a les fraccions com $\frac{a_n}{b_m}$ que apareixen a la demostració anterior; si es considerés $\frac{a_n}{b_m} := b_m^{-1}a_n$, i anàlogament les altres, obtindríem una divisió entera com la que hem escrit: $f(X) = g(X)q(X) + r(X)$; però si es considerés $\frac{a_n}{b_m} = a_n b_m^{-1}$, obtindríem una divisió entera de la forma $f(X) = q(X)g(X) + r(X)$, amb l'ordre permutat entre el divisor i el quocient. No tractarem el cas no commutatiu, de manera que no ens caldrà distingir entre les divisions enteres per l'esquerra o per la dreta (que és com s'anomenarien aquestes).

Corol·lari 6.3.6. *Per a tot cos K, l'anell de polinomis $K[X]$ és un domini d'ideals principals.*

DEMOSTRACIÓ: Com que l'ideal $\{0\}$ és principal, cal veure que tot ideal $\mathfrak{a} \subseteq K[X]$, $\mathfrak{a} \neq \{0\}$, és principal. Sigui $g(X) \in \mathfrak{a}$, $g(X) \neq 0$, un polinomi de grau mínim en $\mathfrak{a} - \{0\}$; clarament, l'ideal $\mathfrak{a}$ conté l'ideal $g(X)K[X]$. Recíprocament, donat $f(X) \in \mathfrak{a}$, la divisió entera de $f(X)$ per $g(X)$ ens proporciona un residu $r(X) = f(X) - g(X)q(X) \in \mathfrak{a}$ de grau estrictament menor que $\mathrm{gr}(g(X))$; com que $g(X)$ és un polinomi no nul de $\mathfrak{a}$ de grau mínim en $\mathfrak{a} - \{0\}$, ha de ser $r(X) = 0$; és a dir, $f(X) = g(X)q(X) \in g(X)K[X]$. Això prova l'altra inclusió i $\mathfrak{a} = g(X)K[X]$. □

Observació 6.3.7. Notem que la demostració anterior és similar a la demostració habitual del fet que l'anell dels nombres enters, $\mathbb{Z}$, és un domini d'ideals principals.

Proposició 6.3.8. *Siguin K un anell commutatiu i $f(X) := \sum_{n\geq 0} a_n \cdot X^n \in K[[X]]$, $a_n \in K$ per a $n \geq 0$, una sèrie de potències de coeficients en K. La sèrie $f(X)$ és invertible en $K[[X]]$ si, i només si, $a_0 \in K$ és invertible.*

DEMOSTRACIÓ: Sigui $g(X) := \sum_{n\geq 0} b_n \cdot X^n \in K[[X]]$, $b_n \in K$ per a $n \geq 0$, una sèrie de potències de coeficients en K. Si es té que $f(X) \cdot g(X) = 1$, llavors $a_0 \cdot b_0 = 1$ i, per tant, $a_0 \in K$ és invertible.

Recíprocament, la sèrie producte $f(X) \cdot g(X)$ és la sèrie $1 \in K[[X]]$ si, i només si, es tenen les igualtats

$$1 = a_0 \cdot b_0, \qquad 0 = \sum_{k=0}^{n} a_{n-k} \cdot b_k, \quad n > 0.$$

Això equival a dir que $a_0 \in K$ és invertible (amb invers b_0), i que els coeficients b_n, $n > 0$, s'obtenen recursivament a partir dels a_k, $0 \leq k \leq n$, i els $b_0, \ldots, b_{n-1}$. En efecte, les igualtats anteriors es poden escriure en la forma

$$b_0 = a_0^{-1}, \qquad b_n = -a_0^{-1} \cdot \sum_{k=0}^{n-1} a_{n-k} \cdot b_k, \quad n > 0;$$

per tant, si a_0 és invertible, la solució d'aquest sistema proporciona la sèrie inversa, $g(X)$. □

Observació 6.3.9. Sigui K un cos. Tota sèrie de potències no nul·la $f(X) \in K[[X]]$, $f(X) \neq 0$, és de la forma $f(X) = X^{\mathrm{ord}(f(X))} \cdot u(X)$, amb $u(X) \in K[[X]]$ una sèrie invertible.

Corol·lari 6.3.10. *Sigui K un cos. L'anell de sèries de potències $K[[X]]$ és un domini d'ideals principals. Els ideals no nuls són els $X^n \cdot K[[X]]$, per a $n \geq 0$. L'únic ideal primer no nul és l'ideal maximal $X \cdot K[[X]]$, amb quocient $K[[X]]/X \cdot K[[X]] \cong K$.* □

6.4 Divisibilitat i arrels múltiples

Definició 6.4.1. Sigui K un anell commutatiu. Donats elements f, $g \in K$, es diu que g divideix f, o que g és un divisor de f, o que f és divisible per g, si existeix un element

$q \in K$, $q \neq 0$, tal que $f = g \cdot q$. Més generalment, donats elements f, $g \in K$, es diu que f és un múltiple de g si existeix un element $q \in K$, tal que $f = g \cdot q$; s'escriu $g \mid f$.

Observació 6.4.2. Notem que a la definició d'element múltiple d'un altre no es demana que sigui $q \neq 0$; en particular, 0 és múltiple de qualsevol element de K. En canvi, si $K \neq \{0\}$, 1 no és mai un divisor de 0, perquè $1 \cdot q = 0$ implica $q = 0$. Aquesta definició, que estén la definició de divisibilitat de nombres enters, s'aplica a qualsevol anell commutatiu K i, en particular, als anells de polinomis, $K[X]$, de coeficients en un cos K. I en aquest cas, hi ha una relació molt estreta entre la divisibilitat i les arrels dels polinomis. Comencem per definir amb precisió el concepte d'arrel d'un polinomi.

Definició 6.4.3. Donats un anell qualsevol, A, i un polinomi

$$f(X_1, \ldots, X_n) := \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \in K[X_1, \ldots, X_n], \qquad a_{i_1,\ldots,i_n} \in A,$$

l'aplicació (entre conjunts) $A^n \longrightarrow A$ definida per

$$(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n) := \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

s'anomena l'aplicació (o funció) polinòmica definida per $f(X_1, \ldots, X_n)$. Els elements $(x_1, \ldots, x_n) \in A^n$ tals que $f(x_1, \ldots, x_n) = 0$ s'anomenen, segons el context, les arrels en A^n del polinomi $f(X_1, \ldots, X_n)$; o els zeros en A^n de la funció polinòmica associada; o les solucions en A^n de l'equació algebraica $f(X_1, \ldots, X_n) = 0$; o els punts en A^n de la varietat algebraica definida pel polinomi $f(X_1, \ldots, X_n)$.

Observació 6.4.4. En general, el nombre d'arrels d'alguns polinomis (en una indeterminada) pot ésser més gran que el seu grau. Per exemple, per a $K = \mathbb{Z}/8\mathbb{Z}$, el polinomi $X^2 - 1 \in K[X]$, de grau 2, té les quatre arrels $x = 1$, $x = 3$, $x = 5$ i $x = 7 \in K$. Fins i tot, un polinomi pot tenir una quantitat no finita d'arrels (cf. els dos exercicis següents, **6.4.5** i **6.4.6**). Veurem més endavant (cf. el teorema **6.4.16**) que aquest fet no succeeix si l'anell sobre el qual es consideren el polinomi i les arrels és un domini d'integritat; en aquest cas, el comportament és molt més restrictiu i precís.

Exercici 6.4.5. Es demana calcular les arrels en $\mathbf{M}(2, \mathbb{Q})$ del polinomi $X^2 - 1 \in \mathbb{Q}[X]$; és a dir, es demana calcular les matrius $M \in \mathbf{M}(2, \mathbb{Q})$ tals que $M^2 = 1_2$, on $1_2 \in \mathbf{M}(2, \mathbb{Q})$ és la matriu identitat, o sigui, l'element unitat de l'anell de matrius.

Exercici 6.4.6. Considerem $K := \prod_{n \in \mathbb{N}} \mathbb{Z}$, l'anell producte d'una infinitat numerable de còpies de l'anell $\mathbb{Z}$ dels nombres enters. Llavors, K és un anell **commutatiu** i el conjunt de les arrels en K del polinomi $X^2 - 1$ és infinit no numerable.

Proposició 6.4.7. *Siguin K un anell commutatiu i $f(X) \in K[X]$, $f(X) \neq 0$, un polinomi no nul. Un element $a \in K$ és una arrel del polinomi $f(X)$ si, i només si, el polinomi $f(X)$ és divisible pel polinomi $X - a \in K[X]$.*

Demostració: Considerem la divisió entera de $f(X)$ pel polinomi (mònic) $X - a$:

$$f(X) = (X - a) \cdot q(X) + r(X), \qquad q(X), r(X) \in K[X], \qquad \mathrm{gr}(r(x)) < 1.$$

Notem que $r(X)$ és un polinomi constant, $r(X) =: r \in K$. Ara, per a l'aplicació polinòmica definida per $f(X)$, se satisfà que $f(a) = r$, de manera que $f(a) = 0$ si, i només si, $r = 0$; i això és equivalent a dir que $X - a$ divideix el polinomi $f(X)$. $\square$

Definició 6.4.8. La igualtat

$$f(X) = (X - a) \cdot q(X) + f(a)$$

es coneix sovint com la regla de Ruffini. Es pot llegir com "el residu de la divisió d'un polinomi per $X - a$ és el valor que pren el polinomi en a".

Observació 6.4.9. Suposem que K és un anell commutatiu i que $a \in K$ és una arrel del polinomi $f(X) \in K[X]$. Llavors, podem escriure $f(X) = (X - a) \cdot q(X)$, i el polinomi $q(X) \in K[X]$ és únic. Pot succeir, o no, que a sigui una arrel de $q(X)$. Si ho és, existeix un polinomi no nul $q_2(X)$ tal que $q(X) = (X-a)\cdot q_2(X)$; o sigui, $f(X) = (X-a)^2 \cdot q_2(X)$. Com que el grau de $q_2(X)$ és una unitat menor que el grau de $q(X)$ que, alhora, és una unitat menor que el grau de $f(X)$, aquest procés no pot continuar indefinidament; és a dir, existeix un nombre natural $m \geq 1$ tal que $(X - a)^m$ divideix el polinomi $f(X)$ però $(X - a)^{m+1}$ no divideix $f(X)$. I si a no és arrel de $f(X)$, aquest màxim és 0.

Definició 6.4.10. Siguin K un anell commutatiu, $f(X) \in K[X]$, $f(X) \neq 0$, un polinomi no nul, i $a \in K$ un element de K. S'anomena multiplicitat de a com a arrel de $f(X)$ el màxim nombre natural $m \geq 0$ tal que $(X - a)^m$ divideix $f(X)$. Una arrel simple és una arrel de multiplicitat $m = 1$. Una arrel de multiplicitat $m > 1$ s'anomena una arrel múltiple (doble, si $m = 2$; triple, si $m = 3$; etcètera).

Definició 6.4.11. Siguin K un anell commutatiu i $f(X) := a_0+a_1X+\cdots+a_nX^n \in K[X]$, $a_0, a_1, \ldots, a_n \in K$, un polinomi. El polinomi

$$D(f, X) := a_1 + 2 \cdot a_2\, X + \cdots + n \cdot a_n\, X^{n-1} \in K[X]$$

s'anomena el polinomi derivat del polinomi $f(X)$.

Observació 6.4.12. Siguin K un anell commutatiu i $f(X)$, $g(X) \in K[X]$, polinomis qualssevol. La demostració de les propietats següents és un exercici senzill.

(a) $D(f + g, X) = D(f, X) + D(g, X)$.

(b) $D(f \cdot g, X) = D(f, X) \cdot g(X) + f(X) \cdot D(g, X)$.

(c) Si $f(X)$ és un polinomi constant, llavors $D(f, X) = 0$.

Però si hom intenta provar el recíproc de la darrera, hom es troba amb dificultats.

Proposició 6.4.13. *Siguin K un domini d'integritat i $f(X) \in K[X]$ un polinomi. Si K és de característica 0, llavors $D(f, X) = 0$ si, i només si, $f(X)$ és un polinomi constant. Però si K és de característica $p > 0$, llavors $D(f, X) = 0$ si, i només si, $f(X) = g(X^p)$, per a algun polinomi $g(X) \in K[X]$; és a dir, si els únics monomis no nuls de $f(X)$ són de grau múltiple de p.*

Demostració: Escriguem $f(X) = a_0+a_1X+\cdots+a_nX^n$, $a_0, a_1, \ldots, a_n \in K$, i considerem el polinomi derivat,

$$D(f, X) = a_1 + 2 \cdot a_2\, X + \cdots + p \cdot a_p\, X^{p-1} + \cdots + n \cdot a_n\, X^{n-1}.$$

Aquest polinomi és nul si, i només si, els seus coeficients a_1, $2 \cdot a_2$, $\ldots$, $n \cdot a_n$ són tots nuls. Però, com que K és un domini d'integritat, $k \cdot a_k = 0$ si, i només si, $k \cdot 1 = 0 \in K$ o bé $a_k = 0$; i la possibilitat $k \cdot 1 = 0 \in K$ es dóna exactament per a $k = 0$ i, si $\mathrm{car}(A) = p > 0$, per als valors de k múltiples de p. Doncs, només per a aquests valors de k, el coeficient a_k del polinomi $f(X)$ pot ésser qualsevol valor de K. □

Observació 6.4.14. Si l'anell K no és un domini d'integritat, encara hi pot haver més dificultats. Per exemple, el derivat del monomi $3X^2 \in (\mathbb{Z}/6\mathbb{Z})[X]$ és el polinomi 0, tot i que el grau no és múltiple de la característica.

El resultat següent proporciona una caracterització de les arrels múltiples dels polinomis de coeficients en dominis d'integritat.

Proposició 6.4.15. *Siguin K un domini d'integritat, $a \in K$ un element, i $f(X) \in K[X]$ un polinomi no nul. L'element a és una arrel múltiple de $f(X)$ si, i només si, a és una arrel de $f(X)$ i de $D(f, X)$.*

Demostració: Escriguem $f(X) = (X-a)^m \cdot q(X)$, on $m \geq 1$ és la multiplicitat de a com a arrel de $f(X)$; en particular, $q(a) \neq 0$. Llavors,

$$\begin{aligned} D(f,X) &= m(X-a)^{m-1} \cdot q(X) + (X-a)^m \cdot D(q,X) \\ &= (X-a)^{m-1} \cdot \big(m \cdot q(X) + (X-a) \cdot D(q,X)\big). \end{aligned}$$

Clarament, la multiplicitat de a com a arrel de $D(f,X)$ és més gran o igual que $m-1$. Per tant, si $m > 1$, a també és arrel de $D(f,X)$. Recíprocament, si $m = 1$, llavors $D(f,a) = q(a) \neq 0$. □

Teorema 6.4.16. *Siguin K un domini d'integritat i $f(X) \in K[X]$ un polinomi no nul. La suma de les multiplicitats de les arrels $a \in K$ de $f(X)$ és menor o igual que el grau de $f(X)$.*

Demostració: Si $a \in K$ és una arrel de $f(X)$, i si anomenem m la seva multiplicitat, tenim que $f(X) = (X-a)^m \cdot g(X)$, amb $g(X) \in K[X]$ tal que $g(a) \neq 0$, i $\mathrm{gr}(g(X)) = \mathrm{gr}(f(X)) - m < \mathrm{gr}(f(X))$. Les arrels de $f(X)$ diferents de a són exactament les arrels de $g(X)$, i les seves multiplicitats per a $f(X)$ i per a $g(X)$ coincideixen. Això ens diu que si la propietat que volem provar és vàlida per al polinomi $g(X)$, també ho és per al polinomi $f(X)$. Per tant, podem procedir per inducció sobre el grau del polinomi, perquè els polinomis de grau 0 no tenen arrels. □

Observació 6.4.17. Notem que no estem suposant que el domini d'integritat K sigui un domini de factorització única (cf. **6.6.13**); per tant, cal anar en compte a l'hora de veure que la multiplicitat en $f(X)$ d'una arrel de $g(X)$ coincideix amb la multiplicitat com a arrel de $g(X)$. Però, si anomenem $b \in K$ una arrel de $g(X)$, i $n \geq 1$ la seva multiplicitat com a arrel de $g(X)$, podem escriure $g(X) = (X-b)^n \cdot h(X)$, per a $h(X) \in K[X]$, $h(b) \neq 0$. Llavors, se satisfà la igualtat $f(X) = (X-b)^n \cdot k(X)$, on $k(X) := h(X) \cdot (X-a)^m$, i s'obté que $k(b) = h(b) \cdot (b-a)^m \neq 0$, perquè K és un domini d'integritat. Per tant, la multiplicitat de b com a arrel de $f(X)$ és n. □

Acabem la secció amb la demostració d'un resultat important sobre els subgrups finits d'unitats d'un domini d'integritat, que ja havíem avançat en **2.8.5**. Com que tot cos és un domini d'integritat, el resultat següent s'aplica, en particular, a cossos.

Proposició 6.4.18. *Siguin K un domini d'integritat i $G \subseteq K^*$ un subgrup finit del grup de les unitats de K. Llavors, G és cíclic (i format per arrels de la unitat).*

Demostració: Sigui $g \in G$ un element d'ordre màxim, posem n. Com que G és un grup finit i abelià, l'ordre m de qualsevol element de G divideix n; per tant, tots els elements de G són arrels del polinomi $X^n - 1$. Però aquest polinomi té, com a màxim, n arrels en el domini K. I el subgrup generat per g té exactament n elements. Per tant, $G = \langle g \rangle$ és cíclic, d'ordre n, i, evidentment, tots els seus elements són arrels n-èsimes de 1. □

6.5 Dominis principals. Dominis euclidians

Definició 6.5.1. Sigui K un anell commutatiu. Per a tot element $a \in K$, el conjunt $(a) := a \cdot K = K \cdot a = \{\lambda \cdot a : \lambda \in K\}$ és un ideal de K; s'anomena l'ideal principal generat per a.

Observació 6.5.2. Com que $\{0\} = 0 \cdot K$ i $K = 1 \cdot K$, els ideals trivials són principals.

Definició 6.5.3. Un domini d'ideals principals, o domini principal, és un domini d'integritat tal que tots els seus ideals són principals.

Observació 6.5.4. No és cert que tot subanell d'un domini d'ideals principals sigui un domini d'ideals principals. Per exemple, l'anell de polinomis $\mathbb{Q}[X]$ és un domini d'ideals principals, perquè $\mathbb{Q}$ és un cos, mentre que $\mathbb{Z}[X]$, que és un subanell de $\mathbb{Q}[X]$, no és un domini d'ideals principals; per exemple, perquè l'ideal format pels polinomis de terme constant parell, que es pot generar per 2 i X, no és principal.

Per a un ús posterior, convé establir un resultat sobre els ideals d'un domini d'ideals principals (i podem notar que per a aquest resultat no cal fer ús del lema de Zorn).

Proposició 6.5.5. *Siguin K un domini d'ideals principals i $\{\mathfrak{a}_i\}_{i\in I}$ una família no buida d'ideals $\mathfrak{a}_i \subseteq K$, $i \in I$. Llavors, existeix $i \in I$ tal que l'ideal $\mathfrak{a}_i$ és un element maximal de la família $\{\mathfrak{a}_i\}_{i\in I}$; és a dir, tota família no buida d'ideals de K admet un element maximal.*

Demostració: Si tots els ideals de la família són l'ideal $\mathfrak{a}_i = \{0\}$, no hi ha res a provar, perquè qualsevol element de la família és maximal. Suposem, doncs, que existeix $i \in I$ tal que $\mathfrak{a}_i \neq \{0\}$. Llavors, com que K és un domini d'ideals principals, tota cadena creixent d'ideals és estacionària. En efecte, la reunió d'una cadena d'ideals és un ideal, i un generador d'aquesta reunió pertany a algun dels ideals de la cadena, de manera que aquest ideal ja és tota la reunió i tots els ideals posteriors de la cadena coincideixen amb aquest. Així, en el conjunt dels ideals $\mathfrak{b} \subseteq K$ que contenen $\mathfrak{a}_i$, només hi pot haver cadenes finites; per tant, en el conjunt dels ideals $\mathfrak{b} \in \{\mathfrak{a}_i\}_{i\in I}$ que contenen $\mathfrak{a}_i$, només hi pot haver cadenes finites. I si no hi hagués cap element maximal de la família, podríem construir una cadena infinita estrictament creixent d'ideals de la família que contenen $\mathfrak{a}_i$. □

Ara, per a un domini d'ideals principals, retrobem el fet que tot ideal propi està inclòs en un ideal maximal; però sense fer ús del lema de Zorn.

Corol·lari 6.5.6. *Sigui K un domini d'ideals principals. Tot ideal propi de K està inclòs en un ideal maximal.*

Demostració: Apliquem la propietat anterior al conjunt de tots els ideals propis de K que contenen l'ideal propi donat. □

Definició 6.5.7. Sigui K un domini d'integritat. Es diu que K és un domini euclidià (o, també, un anell euclidià) si existeix una aplicació $\sigma : K - \{0\} \longrightarrow \mathbb{N}$ tal que per a tota parella d'elements $a, b \in K$, $a \neq 0$, existeixen elements (no necessàriament únics) $q, r \in K$ tals que $b = a \cdot q + r$, i $r = 0$ o bé $\sigma(r) < \sigma(a)$. L'aplicació σ s'anomena, sovint, el grau de l'anell euclidià, i una igualtat $b = a \cdot q + r$, amb $r = 0$ o bé $\sigma(r) < \sigma(a)$, s'anomena una divisió euclidiana (o entera) de b per a. Els elements q, r s'anomenen el quocient i el residu de la divisió, mentre que b i a s'anomenen el dividend i el divisor, respectivament.

Exemples 6.5.8. • L'exemple paradigmàtic d'anell euclidià és l'anell dels nombres enters, amb l'aplicació grau el valor absolut usual; és a dir, $\sigma(n) := \max\{n, -n\}$, per a $n \in \mathbb{Z}$.

• Sigui K un cos. L'anell de polinomis $K[X]$ és un domini euclidià, amb l'aplicació grau donada pel grau del polinomi; és a dir, $\sigma(f(X)) := \mathrm{gr}(f(X))$, per a $f(X) \in K[X]$.

Observació 6.5.9. Diferents llibres poden portar definicions diferents i no equivalents de domini euclidià. La definició que hem donat només imposa l'existència de divisó, sense propietats especials per al grau. Altres definicions imposen restriccions al grau; per exemple, de manera que els elements invertibles de l'anell siguin els de grau mínim.

Exercici 6.5.10. L'anell dels nombres enters, $\mathbb{Z}$, també és un anell euclidià per a l'aplicació σ donada per $\sigma(n) := 2n$, si $n > 0$, i $\sigma(n) := 1 - 2n$, si $n < 0$. En aquest cas, no hi ha elements $n \in \mathbb{Z}$ tals que $\sigma(n) = 1$, i se satisfà que $\sigma(1) = 2 < 3 = \sigma(-1)$. En particular, els elements invertibles d'un anell euclidià no tenen per què tenir associat el mateix grau.

Teorema 6.5.11. *Tot domini euclidià és d'ideals principals.*

Demostració: Sigui K un domini euclidià, amb aplicació grau $\sigma : K - \{0\} \longrightarrow \mathbb{N}$, i suposem que $\mathfrak{a} \subseteq K$ és un ideal. Si $\mathfrak{a} = \{0\}$, és clar que $\mathfrak{a}$ és principal, generat per 0. Suposem, doncs, que $\mathfrak{a} \neq \{0\}$. Podem considerar un element $a \in \mathfrak{a}$, $a \neq 0$, tal que $\sigma(a)$ sigui mínim en $\mathfrak{a} - \{0\}$; és a dir, tal que per a tot $b \in \mathfrak{a}$, $b \neq 0$, sigui $\sigma(a) \leq \sigma(b)$. Llavors, és clar que $a \cdot K \subseteq \mathfrak{a}$. I recíprocament, donat $b \in \mathfrak{a}$, i com que K és euclidià i $a \neq 0$, existeixen $q, r \in K$ tals que $b = a \cdot q + r$, amb $r = 0$ o bé $\sigma(r) < \sigma(a)$. Però $r = b - a \cdot q \in \mathfrak{a}$, de manera que no pot ser $\sigma(r) < \sigma(a)$, perquè $\sigma(a)$ és mínim en $\mathfrak{a} - \{0\}$. Per tant, ha de ser $r = 0$ i $b = a \cdot q \in a \cdot K$, com calia veure. □

Observació 6.5.12. Si K no se suposa commutatiu, encara es pot definir un concepte de divisió euclidiana per l'esquerra o per la dreta i, per tant, també un concepte d'anell euclidià per l'esquerra o d'anell euclidià per la dreta. Això és útil en alguns contextos; per exemple, per a l'estudi de l'anell dels quaternions de Hurwitz i el teorema de Lagrange dels quatre quadrats (cf. [Samuel 1972]), però no ens hi entretindrem.

6.6 Dominis de factorització única

De la mateixa manera que tot nombre enter no nul es pot escriure com a producte de nombres enters primers, i de manera única llevat de l'ordre i del signe dels factors, una cosa similar succeeix als polinomis de coeficients en un cos. Convé distingir, però, entre les nocions d'element primer i d'element irreductible que, encara que coincideixen en $\mathbb{Z}$ (i també en $K[X]$, per a un cos K), no coincideixen en general. Recordem les definicions.

Definició 6.6.1. Sigui K un anell commutatiu. Un element $p \in K$ s'anomena primer si no és invertible i tota relació de divisibilitat $p \mid a \cdot b$, amb $a, b \in K$, implica que $p \mid a$ o bé $p \mid b$; equivalentment, si l'ideal principal $p \cdot K$ és un ideal primer.

Definició 6.6.2. Sigui K un anell commutatiu qualsevol. Un element $a \in K$ s'anomena irreductible si a no és invertible, i per a tota descomposició $a = b \cdot c$, on $b, c \in K$, és o bé $b \in K^*$ o bé $c \in K^*$. Notem que si $K \neq 0$, llavors l'element $0 \in K$ no és irreductible, perquè $0 = 0 \cdot 0$ i 0 no és invertible.

Observació 6.6.3. En particular, si K és un cos, un polinomi $f(X) \in K[X]$ és irreductible si, i només si, no és divisible per cap polinomi no constant de grau estrictament més petit que el de $f(X)$. Per exemple, tot polinomi de grau 1 de $K[X]$ és irreductible. D'altra banda, el polinomi $2X \in \mathbb{Z}[X]$, tot i que és un polinomi de grau 1, no és irreductible en $\mathbb{Z}[X]$, perquè descompon com a producte dels dos polinomis 2 i X, i cap dels dos no és invertible en $\mathbb{Z}[X]$. Notem que, en canvi, aquest polinomi és irreductible en $\mathbb{Q}[X]$.

Observació 6.6.4. D'altra banda, el fet que un element sigui irreductible en un anell no vol dir que ho sigui en un altre anell que el conté com a subanell. Per exemple, considerem l'anell dels nombres enters de Gauss, $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, que conté $\mathbb{Z}$ com a subanell. El nombre 2 és irreductible en $\mathbb{Z}$, mentre que admet la descomposició $2 = (1 + i)(1 - i)$ en $\mathbb{Z}[i]$, i els elements $1 + i, 1 - i \in \mathbb{Z}[i]$ són irreductibles (de fet, i és invertible en $\mathbb{Z}[i]$ i es té que $i(1 - i) = 1 + i$); per tant, $2 = i(1 - i)^2$, i aquesta és una descomposició de 2 com a producte d'elements irreductibles en $\mathbb{Z}[i]$. Per tant, el fet que un element sigui irreductible o no és un fet lligat molt estretament a l'anell en el qual el considerem.

Observació 6.6.5. El concepte d'element irreductible correspon al fet que l'element no sigui producte d'altres elements, llevat de productes trivials; i el concepte d'element primer correspon al fet que si un producte és múltiple d'un element primer, llavors algun dels factors ho és. Tot i que, per exemple, en $\mathbb{Z}$ i en $K[X]$, K cos, els elements primers i els elements irreductibles coincideixen, aquest fet no és general. Per exemple, si considerem l'anell $A = \mathbb{Z}/6\mathbb{Z}$, tenim que els elements 2, 3 i $4 \in A$ són primers (de fet, generen ideals maximals) però no són irreductibles, ja que $2 = 2^3$, $3 = 3^2$, i $4 = 2^2$.

Proposició 6.6.6. (cf. **5.7.10**) *Sigui K un anell commutatiu qualsevol. Tot ideal maximal és un ideal primer.* □

Proposició 6.6.7. *Sigui K un domini d'integritat qualsevol. Tot element primer $p \in K$, $p \neq 0$, és un element irreductible.*

Demostració: Suposem que $p = b \cdot c$, amb $b, c \in K$; cal veure que b, o bé c, és invertible. Com que el producte $b \cdot c$ és múltiple de p, o bé b és múltiple de p, o bé ho és c. Podem suposar que b és múltiple de p, de manera que existeix $x \in K$ tal que $b = p \cdot x$; per tant, $p = b \cdot c = p \cdot x \cdot c$, d'on $p \cdot (1 - x \cdot c) = 0$ i, com que K és un domini d'integritat i $p \neq 0$, ha de ser $1 - x \cdot c = 0$; això és, $x \cdot c = 1$, de manera que c és invertible. □

Proposició 6.6.8. *Siguin K un domini d'ideals principals i $p \in K$ un element diferent de zero. Les propietats següents són equivalents:*

(a) *L'ideal $p \cdot K$ és maximal.*

(b) *L'ideal $p \cdot K$ és primer.*

(c) *L'element p és irreductible.*

Demostració: Si apliquem els dos resultats anteriors, només resta veure que si p és irreductible, llavors l'ideal $p \cdot K$ és maximal. Sigui $\mathfrak{a} \subsetneq K$ un ideal propi de K que contingui $p \cdot K$; cal veure que $\mathfrak{a} = p \cdot K$. Com que K és un anell d'ideals principals, existeix un element $b \in K$ tal que $\mathfrak{a} = b \cdot K$; i com que $\mathfrak{a} \neq K$, l'element b no és invertible. D'altra banda, la hipòtesi ens diu que $p \in b \cdot K$; per tant, existeix $x \in K$ tal que $p = b \cdot x$.

Ara, com que p és irreductible i b no és invertible, x ha de ser invertible. Però això ens diu que $b = p \cdot x^{-1} \in p \cdot K$; és a dir, que $\mathfrak{a} = b \cdot K \subseteq p \cdot K$, d'on obtenim la igualtat $\mathfrak{a} = p \cdot K$ perquè $p \cdot K \subseteq \mathfrak{a}$. $\square$

Definició 6.6.9. Sigui K un anell commutatiu. Dos elements a, $b \in K$ s'anomenen associats si existeix un element invertible $u \in K$ tal que $b = a \cdot u$.

Observació 6.6.10. Si dos elements d'un anell commutatiu K són associats, generen el mateix ideal. Si, a més a més, K és un domini d'integritat, se satisfà la propietat recíproca: si dos elements generen el mateix ideal, llavors són associats.

Observació 6.6.11. Si escrivim $a \sim b$ per a denotar que a i b són elements associats, se satisfà que la relació $\sim$ és d'equivalència, de manera que permet fer una partició de K en classes d'elements associats. Un element $b \in K$ és múltiple d'un element $a \in K$ si, i només si, cada element de la classe d'elements associats de b és múltiple de cada element de la classe d'elements associats de a. Podem dir, doncs, que la relació de divisibilitat es dóna entre classes d'elements associats. Anàlogament, un element $a \in K$ és irreductible (respectivament, primer) si, i només si, tots els elements associats a a ho són; podem parlar, doncs, de les classes d'elements irreductibles o de les classes d'elements primers.

Observació 6.6.12. Podem considerar el grup K^* dels elements invertibles de K i l'acció de K^* en K donada per multiplicació. Això és una acció per l'esquerra i les classes d'elements associats no són res més que les òrbites de l'acció.

Definició 6.6.13. Un domini d'integritat K s'anomena un domini de factorització única si tot element no nul i no invertible $a \in K$ admet una descomposició de la forma $a = u \cdot p_1 \cdot p_2 \cdots p_r$, $r \geq 1$, on $p_1, p_2, \ldots, p_r \in K$ són elements irreductibles determinats a menys del producte per elements invertibles de K, i $u \in K^*$ és un element invertible; és a dir, si tota classe d'elements associats diferent de la nul·la és producte, de manera única llevat de l'ordre, d'una quantitat finita de classes d'elements irreductibles associats.

Observació 6.6.14. No és veritat que tot domini d'integritat sigui un domini de factorització única. Per exemple, en $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, se satisfà la igualtat $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$; d'altra banda, els elements 3, $2 + \sqrt{-5}$, i $2 - \sqrt{-5}$ són irreductibles (exercici), i no es transformen l'un en cap altre en multiplicar per un element invertible de $\mathbb{Z}[\sqrt{-5}]$. Per tant, encara que 9 admet descomposició com a producte d'elements irreductibles en aquest anell, la descomposició no és única. Més generalment, es pot provar que tot element no nul i no invertible de $\mathbb{Z}[\sqrt{-5}]$ admet una descomposició com a producte d'elements irreductibles; però, en general, aquesta descomposició no és única.

Teorema 6.6.15. *Tot domini d'ideals principals és domini de factorització única.*

Demostració: Sigui K un domini d'ideals principals. Cal veure que tot element no nul de K admet una descomposició com a producte de factors irreductibles i que aquesta és única llevat de productes per elements invertibles. Provem en primer lloc l'existència de descomposició.

Per reducció a l'absurd, suposem que $a_0 \in K$ és un element no nul i no invertible de K que no admet descomposició com a producte d'elements irreductibles de K. Anem a construir una successió infinita d'elements de K que no admeten una tal descomposició.

La hipòtesi feta sobre a_0 implica, en particular, que a_0 no és irreductible; per tant, existeixen elements $a_1, b_1 \in K$, tots dos no invertibles, tals que $a_0 = a_1 \cdot b_1$. Si cadascun dels dos elements a_1 i b_1 admetés descomposició com a producte d'elements irreductibles, en multiplicar-les obtindríem una descomposició per a a_0, fet que contradiria la hipòtesi feta sobre a_0; per tant, algun dels dos elements a_1 o bé b_1 no admet descomposició, i podem suposar que a_1 no n'admet. Repetim el procés amb a_1; obtindrem un element $a_2 \in A$ que no admet descomposició i tal que a_1 és múltiple de a_2, de manera que podrem escriure $a_1 = a_2 \cdot b_2$, amb b_2 no invertible. I així successivament. Doncs, amb la hipòtesi que a_0 no admet descomposició com a producte d'elements irreductibles de K, obtenim l'existència d'una successió d'elements $\{a_n\}_{n\geq 0}$, $a_n \in K$, tal que a_n és múltiple de a_{n+1}, per a tot $n \geq 0$, i que $a_n = a_{n+1} \cdot b_{n+1}$, on $b_{n+1} \in K$ no és invertible. Aquesta successió proporciona la successió estrictament creixent, perquè a_n i a_{n+1} no són associats, d'ideals de K,

$$a_0 \cdot K \subsetneq a_1 \cdot K \subsetneq \cdots \subsetneq a_n \cdot K \subsetneq a_{n+1} \cdot K \subsetneq \cdots .$$

Sigui $\mathfrak{a} := \bigcup_{n\geq 0} a_n \cdot K \subseteq K$; llavors, $\mathfrak{a}$ és un ideal de K que conté estrictament tots els ideals $a_n \cdot K$. Com que K és principal, existeix un element $c \in K$ tal que $\mathfrak{a} = c \cdot K$. Però la definició de $\mathfrak{a}$ ens diu que existeix $n \geq 0$ tal que $c \in a_n \cdot K$, de manera que $c \cdot K \subseteq a_n \cdot K$; i això contradiu el fet que $\mathfrak{a}$ conté estrictament $a_n \cdot K$. Aquesta contradicció acaba la reducció a l'absurd i, en conseqüència, tot element de K admet una descomposició com a producte d'elements irreductibles. (Notem que hem usat aquest mateix argument en la proposició **6.5.5**.)

Per a veure la unicitat de les descomposicions, suposem que per a un element $a \in K$, no nul i no invertible, existeixen elements irreductibles $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s \in K$, $r, s \geq 1$, i elements invertibles $u, v \in K^*$ tals que

$$a = u \cdot p_1 \cdot p_2 \cdots p_r = v \cdot q_1 \cdot q_2 \cdots q_s.$$

Com que K és principal i $p_1 \in K$ és irreductible, l'ideal $p_1 \cdot K$ és primer i, com que el producte $v \cdot q_1 \cdot q_2 \cdots q_s$ pertany a l'ideal $p_1 \cdot K$ i $v \notin p_1 K$, algun dels elements q_j pertany a $p_1 \cdot K$; podem suposar que $q_1 \in p_1 \cdot K$. Ara, com que q_1 és múltiple de p_1 i q_1 és irreductible, tenim que els dos elements són iguals llevat del producte per un element invertible de K; i, com que K és un domini d'integritat, podem simplificar p_1 i q_1 dels dos membres, a canvi de multiplicar-ne algun per un element invertible de K. Obtenim dues descomposicions d'un (altre) element no nul de K amb un factor irreductible menys a cada membre de la igualtat.

Això ho podem continuar fent mentre quedin elements irreductibles en algun dels dos membres de la igualtat; finalment, arribarem a una igualtat entre dos elements invertibles de K. És a dir, obtindrem que $r = s$, i que, llevat de l'ordre i del producte per elements invertibles, $p_i = q_i$. Això acaba la prova. □

Observació 6.6.16. Notem que en la prova de l'existència de descomposicions només es fa servir que l'anell K és un domini d'ideals principals per a arribar a una contradicció amb el fet de tenir una successió infinita estrictament creixent d'ideals principals. Doncs, si per a un domini d'integritat K no existeixen successions infinites estrictament creixents d'ideals principals, tot element admet una descomposició com a producte d'elements irreductibles, encara que potser no de manera única. D'altra banda, existeixen exemples de dominis d'integritat d'ús ampli en matemàtiques en els quals hi ha elements que no admeten cap descomposició com a producte d'elements irreductibles.

Corol·lari 6.6.17. *Sigui K un cos qualsevol. L'anell de polinomis $K[X]$ és un domini de factorització única.* □

Corol·lari 6.6.18. *L'anell $\mathbb{Z}$ dels nombres enters és un domini de factorització única.* □

Usualment treballem amb polinomis de coeficients enters; per tant, serà convenient tenir un bon coneixement de l'anell de polinomis $\mathbb{Z}[X]$. D'una banda, ens interessa saber que hi ha factorització única; de l'altra, de quina manera estan relacionades la irreductibilitat en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$ d'un polinomi de coeficients enters.

Definició 6.6.19. Sigui K un anell commutatiu. Donats elements $a, b, d \in K$, es diu que d és un màxim comú divisor de a i b, i s'escriu $d = \mathrm{mcd}(a, b)$, si se satisfan les dues condicions següents.

(a) a i b són múltiples de d;

(b) per a tot element $\delta \in K$ tal que a i b siguin múltiples de δ, d és múltiple de δ.

Observació 6.6.20. En general, donats elements a, b, d'un anell commutatiu K, no té per què existir cap màxim comú divisor de a i b; ni tan sols en el cas que K sigui un domini d'integritat.

Observació 6.6.21. Com succeeix per als elements irreductibles, els elements primers o, en general, amb les qüestions relacionades amb la divisibilitat, un element d és un màxim comú divisor d'elements a, $b \in K$ si, i només si, qualsevol element de la classe d'elements associats a d és un màxim comú divisor d'elements qualssevol a', b', de les classes d'elements associats a a i b, respectivament. És a dir, el concepte de màxim comú divisor és, de fet, un concepte relatiu a classes d'elements associats. És només en aquest sentit que podem escriure una igualtat $d = \mathrm{mcd}(a, b)$, igualtat que es dóna entre les classes d'elements associats, però no necessàriament entre els elements de K. Així, per exemple, de les dues igualtats $1 = \mathrm{mcd}(2, 3)$ i $-1 = \mathrm{mcd}(2, 3)$, vàlides en $\mathbb{Z}$, es dedueix la igualtat $1 = -1$, com a classes d'elements associats, però no, òbviament, com a nombres enters.

Observació 6.6.22. Siguin K un domini de factorització única i $a \in K$ un element no nul. El conjunt de classes d'elements irreductibles associats que divideixen a és finit. En conseqüència, el conjunt de classes de divisors de a és finit. Llavors, donats elements no nuls $a, b \in K$, i suposat que coneixem els corresponents conjunts finits de divisors irreductibles, l'algoritme de l'escola que consisteix a considerar el producte dels factors irreductibles comuns al dos elements a, $b \in K$, tantes vegades com es pugui, en proporciona un màxim comú divisor. Això ens diu que en tot domini de factorització única se satisfà l'existència de màxim comú divisor; és a dir, el resultat següent.

Proposició 6.6.23. *Si K és un domini de factorització única i $a, b \in K$, llavors existeix $d \in K$ tal que $d = \mathrm{mcd}(a, b)$.* □

Observació 6.6.24 (L'algoritme d'Euclides)**.** En general, tot i la seva existència sobre dominis de factorització única, no sabem calcular màxims comuns divisors d'elements donats. Però hi ha un cas molt important en què això se sap fer. Si K és un cos, disposem d'un algoritme per a calcular el màxim comú divisor de dos polinomis $f(X)$, $g(X) \in K[X]$, l'algoritme d'Euclides. En efecte, donats polinomis qualssevol $f(X)$, $g(X)$, $q(X) \in K[X]$, se satisfà que $\mathrm{mcd}(f(X), g(X)) = \mathrm{mcd}(f(X) - g(X)q(X), g(X))$, i que $\mathrm{mcd}(f(X), 0) = f(X)$.

Si $g(X) = 0$, tenim que $\mathrm{mcd}(f(X), 0) = f(X)$. I si $g(X) \neq 0$, fem servir la divisió entera de polinomis; obtenim una igualtat $f(X) := g(X)q(X) + r(X)$, on $q(X)$, $r(X) \in K[X]$, i $\mathrm{gr}(r(X)) < \mathrm{gr}(g(X)$. Llavors, tenim que $\mathrm{mcd}(f(X), g(X)) = \mathrm{mcd}(g(X), r(X))$. I podem iterar el procés, canviant successivament la parella $(f(X), g(X))$ per la parella $(g(X), r(X))$. El procés s'atura, com a màxim en tantes iteracions com el grau del polinomi $g(X)$ inicial més una, quan obtenim un residu $r(X) = 0$, moment en el qual sabem que el màxim comú divisor cercat és el darrer polinomi $g(X)$ considerat com a divisor. Si ara escrivim les igualtats successives que obtenim i substituïm enrere, obtenim una prova del resultat següent. Els detalls de la demostració es proposen com a exercici.

Corol·lari 6.6.25 (Algoritme estès d'Euclides)**.** *Siguin K un cos, $f(X)$, $g(X) \in K[X]$ polinomis no nuls, i $d(X) \in K[X]$ un màxim comú divisor de $f(X)$ i $g(X)$. Existeixen polinomis $a(X)$, $b(X) \in K[X]$, amb $\mathrm{gr}(a(X)) < \mathrm{gr}(g(X))$ i $\mathrm{gr}(b(X)) < \mathrm{gr}(f(X))$, únics tals que $d(X) = f(X)a(X) + g(X)b(X)$.* □

Definició 6.6.26. Siguin K un cos, i $f(X)$, $g(X) \in K[X]$ polinomis no nuls. Una igualtat $d(X) = f(X)a(X) + g(X)b(X)$, on $d(X) = \mathrm{mcd}(f(X), g(X))$ i $a(X)$, $b(X) \in K[X]$, s'anomena una igualtat de Bézout per a $f(X)$, $g(X)$ i $d(X)$.

Exercici 6.6.27. Sigui K un domini euclidià amb aplicació grau σ. Donats elements $a, b \in K$, existeix $d = \mathrm{mcd}(a, b) \in K$, i existeixen $q, r \in K$ tals que $d = a \cdot q + b \cdot r$. Els elements q i r es poden calcular a partir de l'algoritme d'Euclides i, si $a \neq 0$ i $b \neq 0$, es poden triar de manera que $\sigma(q) < \sigma(b)$, o bé es poden triar de manera que $\sigma(r) < \sigma(a)$.

6.7 Teorema xinès del residu

Definició 6.7.1. Siguin K un anell commutatiu i $\mathfrak{a}, \mathfrak{b} \subseteq K$ ideals. L'ideal producte, $\mathfrak{a} \cdot \mathfrak{b} \subseteq K$, és l'ideal generat pels productes $a \cdot b$ tals que $a \in \mathfrak{a}$ i $b \in \mathfrak{b}$; doncs, el conjunt de les sumes de productes $\displaystyle\sum_{i=1}^{m} a_i \cdot b_j$, amb $a_i \in \mathfrak{a}$ i $b_j \in \mathfrak{b}$, per a $1 \leq i, j \leq m$ i tot $m \geq 1$.

Observacions 6.7.2. • La definició s'estén a una quantitat finita d'ideals. En efecte, sigun $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ ideals d'un anell commutatiu K. El seu producte, $\displaystyle\prod_{i=1}^{n} \mathfrak{a}_i$, és l'ideal generat pels productes $\displaystyle\prod_{i=1}^{n} a_i$ tals que $a_i \in \mathfrak{a}_i$, per a $1 \leq i \leq n$. És el conjunt format per les sumes de productes $\displaystyle\sum_{j=1}^{m} \prod_{i=1}^{n} a_{i,j}$, amb $a_{i,j} \in \mathfrak{a}_i$ per a $1 \leq i \leq n$ i $1 \leq j \leq m$, i $m, n \geq 1$.

• Siguin K un anell commutatiu i $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$, ideals. Llavors, $\displaystyle\prod_{i=1}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$.

• Siguin K un anell commutatiu i $\mathfrak{a}_1 = a_1 \cdot K, \ldots, \mathfrak{a}_n = a_n \cdot K \subseteq K$, $a_1, \ldots, a_n \in K$, ideals principals. Llavors, $\displaystyle\prod_{i=1}^{n} \mathfrak{a}_i = \left(\prod_{i=1}^{n} a_i \right) \cdot K$; és a dir, l'ideal producte és principal i generat pel producte dels generadors dels ideals $\mathfrak{a}_i$.

• Siguin K un anell commutatiu i $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq K$, ideals. Llavors,

(a) $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}$; és a dir, el producte és commutatiu.

(b) $(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c})$; és a dir, el producte és associatiu.

(c) $\mathfrak{a} \cdot K = \mathfrak{a}$; és a dir, l'ideal $K = 1 \cdot K$ és un element neutre per al producte d'ideals.

(d) $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}$; és a dir, el producte és distributiu respecte la suma.

Definició 6.7.3. Sigui K un anell commutatiu. Es diu que dos ideals $\mathfrak{a}, \mathfrak{b} \subseteq K$ són comaximals si $\mathfrak{a} + \mathfrak{b} = K$; és a dir, si existeixen elements $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, tals que $1 = a + b$. Més generalment, es diu que els ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ són comaximals si $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = K$.

Observació 6.7.4. Notem que no és el mateix dir que els ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ són comaximals, que dir que són comaximals dos a dos.

Proposició 6.7.5. *Siguin K un anell commutatiu i $\mathfrak{a}, \mathfrak{b} \subseteq K$ ideals comaximals. Llavors, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$. Més generalment, si $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ són ideals comaximals dos a dos, és a dir, si $\mathfrak{a}_i + \mathfrak{a}_j = K$, per a $i \neq j$, llavors $\displaystyle\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$.*

Demostració: Cal veure que la inclusió $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ és una igualtat. Però, si escrivim $1 = a + b$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, per a tot element $c \in \mathfrak{a} \cap \mathfrak{b}$ és $c = a \cdot c + b \cdot c \in \mathfrak{a} \cdot \mathfrak{b}$, perquè $a \cdot c, b \cdot c \in \mathfrak{a} \cdot \mathfrak{b}$.

Demostrem el cas general per inducció sobre n; en el cas $n = 1$ no hi ha res a dir, i acabem de veure el cas $n = 2$. Suposem, doncs, que $n > 2$ i que el resultat és cert per a famílies de menys de n ideals comaximals dos a dos. Donats ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ comaximals dos a dos, posem $\mathfrak{a} := \mathfrak{a}_1$, i $\mathfrak{b} := \displaystyle\prod_{i=2}^{n} \mathfrak{a}_i$. Com que, per a $2 \leq i \leq n$ és $\mathfrak{a}_1 + \mathfrak{a}_i = K$, existeixen elements $a_i \in \mathfrak{a}_1$, $b_i \in \mathfrak{a}_i$, $2 \leq i \leq n$, tals que $1 = a_i + b_i$. Això és dir que $1 - a_i = b_i \in \mathfrak{a}_i$, de manera que $b := \displaystyle\prod_{i=2}^{n}(1 - a_i) = \prod_{i=2}^{n} b_i \in \mathfrak{b}$. Però se satisfà que $\displaystyle\prod_{i=2}^{n}(1 - a_i) \equiv 1 \pmod{\mathfrak{a}}$, o sigui, que $b = \displaystyle\prod_{i=2}^{n}(1 - a_i) = 1 - a$, per a un cert element $a \in \mathfrak{a}$. Això diu que $1 = a + b$ amb $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, de manera que $\mathfrak{a} + \mathfrak{b} = K$. Per tant, pel cas $n = 2$, és $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$; i, per hipòtesi d'inducció, és $\mathfrak{b} = \displaystyle\prod_{i=2}^{n} \mathfrak{a}_i = \bigcap_{i=2}^{n} \mathfrak{a}_i$; en conseqüència, és

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{a} \cdot \prod_{i=2}^{n} \mathfrak{a}_i = \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cap \left(\bigcap_{i=2}^{n} \mathfrak{a}_i \right) = \bigcap_{i=1}^{n} \mathfrak{a}_i,$$

com calia veure. □

Observació 6.7.6. Notem que, en particular, hem provat que si K és un anell commutatiu i $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ són ideals comaximals dos a dos, llavors, per a $1 \leq i \leq n$, els ideals $\mathfrak{a}_i$, $\mathfrak{b}_i := \displaystyle\prod_{j \neq i} \mathfrak{a}_j \subseteq K$ són comaximals.

Exercici 6.7.7. Siguin K un anell commutatiu i $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ ideals comaximals. Llavors, per a tota família de nombres enters positius $e_1, \ldots, e_n \geq 1$, els ideals $\mathfrak{a}_1^{e_1}, \ldots, \mathfrak{a}_n^{e_n}$ són comaximals; és a dir, si $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = K$, llavors $\mathfrak{a}_1^{e_1} + \cdots + \mathfrak{a}_n^{e_n} = K$.

Teorema 6.7.8 (Teorema xinès del residu)**.** *Sigui K un anell commutatiu i considerem ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ i el morfisme d'anells $\varphi : K \longrightarrow \prod_{i=1}^{n} \frac{K}{\mathfrak{a}_i}$, donat per les projeccions en cadascun dels components del producte; és a dir, $a \mapsto (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$, per a tot $a \in K$.*

(a) *En general, el nucli de φ és $\ker \varphi = \bigcap_{i=1}^{n} \mathfrak{a}_i$.*

(b) *Si φ és exhaustiu, llavors $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ són comaximals dos a dos.*

(c) *Recíprocament, si suposem que $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ són comaximals dos a dos, llavors φ és exhaustiu.*

(d) *Si suposem que $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ són comaximals dos a dos, tenim un isomorfisme canònic*

$$\frac{K}{\prod_{i=1}^{n} \mathfrak{a}_i} \longrightarrow \prod_{i=1}^{n} \frac{K}{\mathfrak{a}_i}.$$

Demostració: És clar que φ és un morfisme d'anells; de fet, és l'únic per al qual les projeccions $\pi_i : K \longrightarrow K/\mathfrak{a}_i$ són les donades per les assignacions $\pi_i(a) = a + \mathfrak{a}_i$.

(a) També és clar que el nucli de φ és la intersecció dels nuclis dels π_i; és a dir, la intersecció $\bigcap_{i=1}^{n} \mathfrak{a}_i$.

(b) Si suposem que φ és exhaustiu, llavors tenim que, per a tot i, $1 \leq i \leq n$, l'element $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}, 1 + \mathfrak{a}_i, \mathfrak{a}_{i+1}, \ldots, \mathfrak{a}_n)$ té alguna antiimatge; és a dir, existeix $a_i \in K$ tal que $a_i \equiv 1 \pmod{\mathfrak{a}_i}$ i $a_i \equiv 0 \pmod{\mathfrak{a}_j}$, per a $j \neq i$; però, llavors, $a_i \in \mathfrak{a}_j$, per a $j \neq i$, i se satisfà que $1 = (1 - a_i) + a_i \in \mathfrak{a}_i + \mathfrak{a}_j$, per a $j \neq i$, com calia veure.

(c) Recíprocament, suposem que $\mathfrak{a}_i + \mathfrak{a}_j = K$, per a $i \neq j$. Llavors, per a $1 \leq i \leq n$, existeixen $a_i \in \mathfrak{a}_i$ i $b_i \in \prod_{j \neq i} \mathfrak{a}_j$ tals que $1 = a_i + b_i$ (cf. l'observació **6.7.6**). Així, donats elements arbitraris $x_1, \ldots, x_n \in K$, podem considerar l'element $x := \sum_{i=1}^{n} x_i \cdot b_i \in K$. Es té que, per a $1 \leq i \leq n$, és $x \equiv x_i \cdot b_i = x_i \cdot (1 - a_i) \equiv x_i \pmod{\mathfrak{a}_i}$, ja que per a $j \neq i$, és $b_j \in \mathfrak{a}_i$, d'on $x_j \cdot b_j \equiv 0 \pmod{\mathfrak{a}_i}$. Això demostra que tot element $(x_1 + \mathfrak{a}_1, \ldots, x_n + \mathfrak{a}_n)$ té una antiimatge $x \in K$.

(d) Només cal aplicar el primer teorema d'isomorfia i tenir en compte els apartats anteriors i la proposició **6.7.5**. □

Observació 6.7.9. Siguin K un anell commutatiu i $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$ ideals comaximals dos a dos. El teorema xinès del residu es pot interpretar en la forma següent. *Donats elements arbitraris $x_1, \ldots, x_n \in K$, el sistema de congruències $x \equiv x_i \pmod{\mathfrak{a}_i}$, $1 \leq i \leq n$, té solució $x \in K$, determinada mòdul el producte $\mathfrak{a}_1 \cdots \mathfrak{a}_n$.*

Observació 6.7.10. En particular, si $K = \mathbb{Z}$, tenim que si $m_1, \ldots, m_n \in \mathbb{Z}$ són nombres enters tals que per a $i \neq j$ és $\mathrm{mcd}(m_i, m_j) = 1$, llavors tot sistema de congruències de la forma

$$x \equiv a_i \pmod{m_i}, \qquad 1 \leq i \leq n, \qquad a_1, \ldots, a_n \in \mathbb{Z},$$

té solució, única mòdul el producte $m_1 \cdots m_n$.

Corol·lari 6.7.11. *Siguin K un anell commutatiu i considerem ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq K$, comaximals dos a dos. Llavors, per als grups d'unitats es té un isomorfisme*

$$\left(\frac{K}{\prod_{i=1}^n \mathfrak{a}_i}\right)^* \cong \prod_{i=1}^n \left(\frac{K}{\mathfrak{a}_i}\right)^*.$$

Demostració: Només cal aplicar les dues propietats següents, de demostració immediata. D'una banda, tot isomorfisme d'anells $K \cong L$ restringeix a un isomorfisme de grups $K^* \cong L^*$ entre els grups dels seus element invertibles. I de l'altra, el grup dels elements invertibles d'un producte d'anells, $\prod_{i \in I} K_i$, és el grup producte, $\prod_{i \in I} K_i^*$, dels seus grups d'elements invertibles. □

Observació 6.7.12. Es defineix la funció φ d'Euler, $\varphi : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$, per l'assinació $\varphi(n) := \#\,(\mathbb{Z}/n\mathbb{Z})^*$, l'ordre del grup multiplicatiu de l'anell de classes de residus de $\mathbb{Z}$ mòdul $n\mathbb{Z}$. El teorema xinès del residu implica la propietat de multiplicativitat de la funció φ: per a $m, n \in \mathbb{Z}_{>0}$, si $\mathrm{mcd}(m, n) = 1$, llavors $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. En particular, si tenim en compte que per a p, primer, i $r \geq 1$, és $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$, reobtenim les fórmules equivalents

$$\varphi(n) = n \cdot \prod_{p|n} \frac{p-1}{p} = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right), \qquad \frac{\varphi(n)}{n} = \prod_{p|n} \frac{p-1}{p} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

els productes estesos al conjunt dels nombres naturals primers p que divideixen n.

6.8 Lema de Gauss. Factorialitat dels anells de polinomis

Definició 6.8.1. Siguin K un domini de factorització única i $f(X) \in K[X]$ un polinomi no nul. S'anomena contingut de $f(X)$ el màxim comú divisor dels coeficients de $f(X)$. Escriurem $\mathrm{cont}(f(X))$ per a denotar el contingut del polinomi $f(X)$; és una classe d'elements associats de K.

Teorema 6.8.2 (Lema de Gauss, versió 1)**.** *Siguin K un domini de factorització única i considerem polinomis no nuls $f(X), g(X) \in K[X]$. Llavors,*

$$\mathrm{cont}(f(X)g(X)) = \mathrm{cont}(f(X))\,\mathrm{cont}(g(X)).$$

Demostració: Siguin $d_f, d_g \in K$ els continguts de $f(X), g(X)$, respectivament. Així, podem escriure $f(X) = d_f \cdot f'(X)$, amb $f'(X) = a'_0 + a'_1 X + \cdots + a'_n X^n \in K[X]$, $a'_0, \ldots, a'_n \in K$, i també $g(X) = d_g \cdot g'(X)$, amb $g'(X) = b'_0 + b'_1 X + \cdots + b'_m X^m \in K[X]$,

$b'_0, \ldots, b'_m \in K$, i $\mathrm{mcd}(a'_0, a'_1, \ldots, a'_n) = \mathrm{mcd}(b'_0, b'_1, \ldots, b'_m) = 1$. El polinomi producte, $f(X)g(X)$, es pot escriure en la forma $f(X)g(X) = d_f \cdot d_g \cdot (a'_0 + a'_1X + \cdots + a'_nX^n) \cdot (b'_0 + b'_1X + \cdots + b'_mX^m) = d_f \cdot d_g \cdot (c_0 + c_1X + \cdots + c_{n+m}X^{n+m})$, on $c_k = \sum_{i+j=k} a'_i \cdot b'_j$, per a $0 \leq k \leq n+m$. Cal, doncs, i és suficient, provar que $\mathrm{mcd}(c_0, c_1, \ldots, c_{n+m}) = 1$.

Ho farem per reducció a l'absurd. Si fos $\mathrm{mcd}(c_0, c_1, \ldots, c_{n+m}) \neq 1$, existiria un element irreductible $p \in K$ tal que tots els coeficients c_k, $0 \leq k \leq n+m$, serien múltiples de p. Ara bé, ni tots els coeficients $a'_0, a'_1, \ldots, a'_n$ ni tampoc tots els coeficients $b'_0, b'_1, \ldots, b'_m$ són múltiples de p, perquè $\mathrm{cont}(f'(X)) = \mathrm{cont}(g'(X)) = 1$. Podem considerar, doncs, els menors índexs r, s, $0 \leq r \leq n$, $0 \leq s \leq m$, tals que ni a'_r ni b'_s són múltiples de p; així, per a $0 \leq i < r$, i per a $0 \leq j < s$, a'_i i b'_j són múltiples de p. Ara, tenim que $c_{r+s} = \sum_{i+j=r+s} a'_i \cdot b'_j$ és múltiple de p, per hipòtesi; d'altra banda, $\sum_{i+j=r+s,\,(i,j)\neq(r,s)} a'_i \cdot b'_j$ també és múltiple de p, ja que un dels dos factors de cada sumand ho és (en efecte, o bé $i < r$ o bé $j < s$); en conseqüència, la diferència, $a'_r \cdot b'_s$, entre les dues expressions és múltiple de p. Però això és contradictori amb l'elecció de r i s, ja que K és un domini de factorització única i el producte $a'_r \cdot b'_s$ no pot ser múltiple de p perquè no ho és cap dels dos factors. □

Corol·lari 6.8.3 (Lema de Gauss, versió 2)**.** *Siguin K un domini de factorització única, Q el seu cos de fraccions, $f(X) \in K[X]$ un polinomi no nul, i $g(X), h(X) \in Q[X]$ polinomis tals que $f(X) = g(X) \cdot h(X)$. Existeixen elements $c_g, c_h \in Q$ i polinomis $g'(X), h'(X) \in K[X]$, de contingut 1, i tals que $g(X) = c_g \cdot g'(X)$, $h(X) = c_h \cdot h'(X)$, el producte $c_g \cdot c_h \in K$, i $f(X) = (c_g \cdot c_h) \cdot g'(X) \cdot h'(X)$. És a dir, una descomposició de $f(X)$ en $Q[X]$ dóna lloc a una descomposició de $f(X)$ en $K[X]$, amb polinomis del mateix grau que els originals, i proporcionals per una constant de K.*

Demostració: Comencem per la definició dels elements c_g, c_h. Considerem un denominador comú de tots els coeficients de $g(X)$, posem $d_g \in K$, de manera que $d_g \cdot g(X) \in K[X]$; sigui $\delta_g \in K$ el contingut del polinomi $d_g \cdot g(X)$ i posem $d_g \cdot g(X) = \delta_g \cdot g'(X)$, amb $g'(X) \in K[X]$ de contingut 1; i sigui $c_g := \dfrac{\delta_g}{d_g} \in Q$. Definim d_h, δ_h, $h'(X)$ i c_h anàlogament. És clar que $f(X) = g(X) \cdot h(X) = c_g \cdot c_h \cdot g'(X) \cdot h'(X)$. Com que $g'(X) \cdot h'(X)$ és de contingut 1 (cf. el lema de Gauss, **6.8.2**), el producte $c_g \cdot c_h$ ha de ser el contingut del polinomi $f(X)$, de manera que $c_g \cdot c_h \in K$. En efecte, si escrivim $c_g \cdot c_h = \dfrac{a}{b}$, amb $a, b \in K$, primers entre si, tenim que $b \cdot f(X) = a \cdot g'(X) \cdot h'(X)$, de manera que $a = \mathrm{cont}(a \cdot g'(X) \cdot h'(X)) = \mathrm{cont}(b \cdot f(X)) = b \cdot \mathrm{cont}(f(X))$, d'on és clar que a és múltiple de b. Però com que K és un domini de factorització única i $\mathrm{mcd}(a, b) = 1$, b ha d'ésser invertible en K, de manera que $c_g \cdot c_h = \dfrac{a}{b} \in K$. □

Corol·lari 6.8.4 (Lema de Gauss, versió 3)**.** *Siguin K un domini de factorització única, Q el seu cos de fraccions, i $f(X) \in K[X]$ un polinomi no constant. Si $f(X)$ és irreductible en $K[X]$, també ho és en $Q[X]$; d'altra banda, si $f(X)$ és irreductible en $Q[X]$, ho és en $K[X]$ si, i només si, és de contingut 1.* □

Aquest resultat ens permetrà provar un resultat molt important que, en particular, ens dirà que els anells de polinomis $\mathbb{Z}[X_1, \ldots, X_n]$ i, per a qualsevol cos k, els anells de polinomis $k[X_1, \ldots, X_n]$ són de factorització única.

Teorema 6.8.5 (Lema de Gauss, versió 4)**.** *Si K és un domini de factorització única, l'anell de polinomis $K[X]$ també és un domini de factorització única. A més a més, els elements irreductibles de $K[X]$ són els elements irreductibles de K i els polinomis de $K[X]$ de contingut 1 que són irreductibles en $Q[X]$, on Q designa el cos de fraccions de K.*

Demostració: Sigui $f(X) \in K[X]$, $f(X) \neq 0$. Com que l'anell $Q[X]$ és de factorització única, el corol·lari anterior ens ensenya a trobar, a partir d'una descomposició de $f(X)$ com a producte de factors irreductibles en $Q[X]$, una descomposició de $f(X)$ de la forma $f(X) = c \cdot g_1(X) \cdots g_n(X)$, on $c \in K$ i $g_i(X) \in K[X]$ és un polinomi de contingut 1 i irreductible en $Q[X]$. Ara, com que K és un domini de factorització única, l'element c es pot escriure de manera única (llevat de producte per elements invertibles de K) com a producte d'elements irreductibles de K. Això dóna una descomposició de $f(X)$; en efecte, d'una banda, els elements de K només poden descompondre en $K[X]$ com ho fan en K, ja que són polinomis de grau zero; per tant, els elements irreductibles de K també són irreductibles en $K[X]$; d'altra banda, si un polinomi descompon en $K[X]$, la mateixa descomposició val en $Q[X]$, de manera que un polinomi de $K[X]$ de contingut 1 i irreductible en $Q[X]$ és irreductible en $K[X]$.

Resta veure la unicitat de la descomposició. Per a això, suposem que

$$f(X) = c \cdot g_1(X) \cdots g_n(X) = d \cdot h_1(X) \cdots h_m(X),$$

amb $c, d \in K$ i $g_i(X), h_j(X) \in K[X]$, de contingut 1, i irreductibles en $Q[X]$. D'una banda, c, d són el contingut de $f(X)$, de manera que són associats; d'altra banda, la igualtat val en $Q[X]$, que és de factorització única; per tant, $n = m$ i, llevat de permutació dels polinomis, $g_i(X)$ és associat de $h_i(X)$ en $Q[X]$; però, llavors, en virtut del lema de Gauss (**6.8.3**), $g_i(X)$ i $h_i(X)$ són associats en $K[X]$. Això, juntament amb la factorització única en K per al contingut de $f(X)$, demostra la unicitat de la descomposició. □

Corol·lari 6.8.6. *Per a tot $n \geq 0$, l'anell de polinomis $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ és un domini de factorització única.* □

Corol·lari 6.8.7. *Per a tot cos k i tot $n \geq 1$, l'anell de polinomis $k[X_1, X_2, \ldots, X_n]$ és un domini de factorització única.* □

6.9 Criteris d'irreductibilitat de polinomis

Fins ara, no hem parlat de com es pot saber si un polinomi és irreductible, ni tan sols en el cas de coeficients en un cos; només ho sabem per als polinomis de grau 1. En aquesta secció, donarem alguns criteris per a reconèixer si un polinomi és o no irreductible, almenys, per a alguns casos particulars.

Teorema 6.9.1 (Criteri d'Eisenstein)**.** *Siguin K un domini de factorització única, Q el seu cos de fraccions, i $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$, $a_0, a_1, \ldots, a_n \in K$, $a_n \neq 0$, un polinomi. Suposem que existeix un element irreductible $p \in K$ tal que a_n no és múltiple de p, cadascun dels $a_0, a_1, \ldots, a_{n-1}$ és múltiple de p, i a_0 no és múltiple de p^2. Llavors, $f(X)$ és irreductible en $Q[X]$. I si, a més a més, $f(X)$ és de contingut 1, $f(X)$ és irreductible en $K[X]$.*

DEMOSTRACIÓ: Com que a_n no és múltiple de p, el contingut de $f(X)$ no és múltiple de p. Si canviem $f(X)$ dividint-lo pel seu contingut, ni les hipòtesis ni la tesi no canvien, de manera que podem suposar que el polinomi $f(X)$ és de contingut 1. En aquest cas, si existís una descomposició no trivial de $f(X)$ en $Q[X]$, i en virtut del lema de Gauss (cf. **6.8.3**), existiria una descomposició en $K[X]$ de la forma $f(X) = g(X) \cdot h(X)$, amb $g(X), h(X)$ polinomis no constants. Podem escriure $g(X) = b_0 + b_1X + \cdots + b_rX^r$, i $h(X) = c_0 + c_1X + \cdots + c_sX^s$, amb $b_0, b_1, \ldots, b_r, c_0, c_1, \ldots, c_s \in K$, $b_r, c_s \neq 0$, i, a més a més, $1 \leq r, s \leq n-1$.

Com que $b_0 \cdot c_0 = a_0$ és múltiple de p, però no de p^2, exactament un dels dos elements b_0, c_0 no és múltiple de p. Suposem que b_0 no és múltiple de p; llavors, c_0 és múltiple de p. D'altra banda, c_s no és múltiple de p, ja que $b_r \cdot c_s = a_n$ no ho és; per tant, existeix t, $1 \leq t \leq s$, tal que per a $0 \leq j \leq t-1$ és $p \mid c_j$ però $p \nmid c_t$. Per hipòtesi, $a_t = \sum_{i+j=t} b_i \cdot c_j$ és múltiple de p, ja que $t \leq s < n$; a més a més, $\sum_{i+j=t, j<t} b_i \cdot c_j$ és múltiple de p, ja que ho és cada c_j; en conseqüència, $b_0 \cdot c_t$ és múltiple de p. Però ni b_0 ni c_t són múltiples de p; aquesta contradicció ens permet assegurar que $f(X)$ és irreductible en $Q[X]$. I una nova aplicació del lema de Gauss (cf. **6.8.4**) acaba la prova. □

Definició 6.9.2. Un polinomi per al qual se satisfan les hipòtesis del teorema s'anomena un polinomi d'Eisenstein per al primer p.

Exemple 6.9.3. Sigui $a \in \mathbb{Z}$, $a \neq 0, 1, -1$, un nombre enter lliure de quadrats; és a dir, tal que per a tot nombre primer $p \in \mathbb{Z}$, el nombre p^2 no divideix a. Per a tot nombre natural $n \geq 1$ el polinomi $X^n - a$ és irreductible en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$, perquè és un polinomi d'Eisenstein per a qualsevol nombre natural primer p que divideix a.

Destaquem els dos resultats següents que, encara que immediats, són útils molt sovint.

Proposició 6.9.4. *Siguin K un domini d'integritat i $\varphi : K[X] \longrightarrow K[X]$ un isomorfisme qualssevol. Un polinomi $f(X) \in K[X]$ és irreductible si, i només si, ho és $\varphi(f(X))$.* □

Proposició 6.9.5. *Siguin K un anell commutatiu, i $u, v \in K$, u invertible. Existeix un únic morfisme d'anells $\varphi : K[X] \longrightarrow K[X]$ tal que $\varphi(a) = a$, per a tot $a \in K$, i $\varphi(X) = uX + v$; aquest morfisme és un isomorfisme.* □

Proposició 6.9.6. *Sigui p un nombre natural primer. El p-èsim polinomi ciclotòmic,*

$$\Phi_p(X) := \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{p-1} \in \mathbb{Z}[X],$$

és irreductible.

DEMOSTRACIÓ: Posem $g(X) := \Phi_p(X + 1)$; llavors, el polinomi

$$g(X) := \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$$

és un polinomi d'Eisenstein per al primer p; per tant, $g(X)$ és irreductible; en conseqüència, $\Phi_p(X)$ és irreductible. □

Proposició 6.9.7. *Siguin K, L dominis d'integritat, $\varphi : K \longrightarrow L$ un morfisme qualsevol d'anells, i Q el cos de fraccions de L. Anomenem també $\varphi : K[X] \longrightarrow L[X]$ el morfisme d'anells que s'obté en aplicar φ als coeficients dels polinomis de $K[X]$. Sigui $f(X) \in K[X]$ un polinomi tal que $\varphi(f(X)) \neq 0$ i $\operatorname{gr}(\varphi(f(X))) = \operatorname{gr}(f(X))$. Llavors, si $\varphi(f(X))$ és irreductible en $Q[X]$, $f(X)$ no admet cap factorització de la forma $f(X) = g(X) \cdot h(X)$, amb $g(X), h(X) \in K[X]$, $\operatorname{gr}(g(X)) \geq 1$ i $\operatorname{gr}(h(X)) \geq 1$.*

Demostració: Si $f(X)$ tingués una factorització com la de l'enunciat, en aplicar φ obtindríem una factorització de $\varphi(f(X))$ en $Q[X]$, $\varphi(f(X)) = \varphi(g(X)) \cdot \varphi(h(X))$; com que $\operatorname{gr}(\varphi(g(X))) \leq \operatorname{gr}(g(X))$ i també $\operatorname{gr}(\varphi(h(X))) \leq \operatorname{gr}(h(X))$, però $\operatorname{gr}(\varphi(g(X)) \cdot \varphi(h(X))) = \operatorname{gr}(g(X) \cdot h(X))$, hauria de ser $\operatorname{gr}(\varphi(g(X))) = \operatorname{gr}(g(X)) \geq 1$ i $\operatorname{gr}(\varphi(h(X))) = \operatorname{gr}(h(X)) \geq 1$, de manera que obtindríem una descomposició no trivial de $\varphi(f(X))$ en $Q[X]$, contra la hipòtesi que $\varphi(f(X))$ és irreductible. □

Corol·lari 6.9.8 (Criteri de reducció)**.** *Siguin $f(X) \in \mathbb{Z}[X]$ un polinomi no nul i $p \in \mathbb{Z}$ un nombre primer que no divideix el coeficient del monomi principal de $f(X)$. Suposem que per reducció mòdul p dels coeficients de $f(X)$ s'obté un polinomi irreductible en $(\mathbb{Z}/p\mathbb{Z})[X]$; llavors, $f(X)$ és irreductible en $\mathbb{Q}[X]$. Si, a més a més, $f(X)$ és de contingut 1, $f(X)$ és irreductible en $\mathbb{Z}[X]$.* □

Exemple 6.9.9. Siguin $a, b \in \mathbb{Z}$ nombres senars. Els polinomis $X^2 + aX + b$, $X^3 + aX + b$, $X^3 + aX^2 + b \in \mathbb{Z}[X]$ són irreductibles en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$. En efecte, les seves reduccions mòdul 2 són els polinomis $X^2 + X + 1$, $X^3 + X + 1$ i $X^3 + X^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$, que són irreductibles (cf. l'exercici **6.10.17**).

6.10 Un mètode de factorització en $\mathbb{Z}[X]$

En general no hi ha bons algoritmes per a determinar si un polinomi és o no irreductible. Per a polinomis de coeficients enters, però, es pot donar un algoritme que no només serveix per a decidir si un polinomi donat és irreductible o no, sinó que, en cas de ser reductible, en proporciona la descomposició. Aquest algoritme, que descrivim en aquesta secció, està basat en el càlcul de factoritzacions de nombres enters.

Sigui $f(X) := a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$, $n \geq 0$, un polinomi qualsevol del qual volem trobar els seus factors irreductibles.

6.10.1. En primer lloc, podem calcular el contingut del polinomi i factoritzar aquest nombre enter. D'aquesta manera obtenim un factor constant del polinomi descompost en factors irreductibles i un polinomi de contingut 1 de $\mathbb{Z}[X]$ que cal descompondre.

6.10.2. A continuació, calculem el polinomi derivat $D(f, X)$ i, amb l'algoritme d'Euclides en $\mathbb{Q}[X]$, calculem el màxim comú divisor de $f(X)$ i $D(f, X)$ en $\mathbb{Z}[X]$. Si anomenem $d(X) := \operatorname{mcd}(f(X), D(f, X)) \in \mathbb{Z}[X]$, el polinomi $g(X) := \dfrac{f(X)}{d(X)} \in \mathbb{Z}[X]$ té els mateixos factors irreductibles que $f(X)$, però tots són de multiplicitat 1. Al final, per divisió, podrem calcular la multiplicitat de cadascun dels factors irreductibles de $f(X)$ que siguin de multiplicitat més gran que 1.

6.10.3. Doncs, a partir d'aquest punt, podem suposar que $f(X) \in \mathbb{Z}[X]$ és un polinomi primitiu i sense factors irreductibles múltiples. I si el grau n de $f(X)$ és 0 o bé 1, ja hem

acabat, perquè $f(X)$ és irreductible. En cas contrari, com que $f(X)$ és de grau $n \geq 2$, si $f(X)$ no és irreductible, ha de tenir algun divisor de grau menor o igual que la meitat de n. El procés de càlcul dels factors irreductibles de $f(X)$ es fa cercant successivament els factors irreductibles de grau 1, després els de grau 2, i així successivament, fins als de grau $[n/2]$. Cada cop que trobem un factor de $f(X)$, posem $h(X)$, canviem el polinomi $f(X)$ per $\dfrac{f(X)}{h(X)}$, de manera que el nou polinomi $f(X)$ és de grau menor que el grau del polinomi $f(X)$ anterior; per tant, la fita $[n/2]$ va decreixent a mesura que anem trobant factors.

6.10.4. Comencem el procés amb el càlcul dels factors irreductibles de grau 1 del polinomi $f(X)$. Això és equivalent a calcular les arrels racionals de $f(X)$ i és ben conegut que si $\dfrac{a}{b} \in \mathbb{Q}$ és una arrel de $f(X)$ en $\mathbb{Q}$, amb a, $b \in \mathbb{Z}$, $b > 0$, i $\mathrm{mcd}(a, b) = 1$, llavors $a \mid a_0$ i $b \mid a_n$ (exercici); la descomposició en factors primers de a_0 ens dóna una quantitat finita de possibilitats per a a, i la descomposició en factors primers de a_n, una quantitat finita de possibilitats per a b; llavors, el mètode de divisió (per exemple, de Ruffini) aplicat a totes les fraccions $\dfrac{a}{b}$ ens diu immediatament quines d'aquestes possibilitats proporcionen realment factors de $f(X)$ de grau 1, necessàriament irreductibles.

6.10.5. Un cop completat aquest pas, obtenim un nou polinomi $f(X)$ que no és divisible per polinomis de grau 1. Si aquest nou polinomi és de grau 2 o bé de grau 3, ja hem acabat la descomposició. En cas contrari, cerquem un conjunt finit de polinomis de grau 2 que contingui tots els divisors de grau 2 del polinomi $f(X)$.

Suposem que $g(X) := aX^2 + bX + c$ és un polinomi de coeficients enters a, b, c, tals que $a \neq 0$ i que $g(X)$ divideix $f(X)$. Llavors, per a tot nombre enter z, el nombre enter $g(z)$ divideix $f(z)$ (en efecte, si $h(X) \in \mathbb{Z}[X]$ és tal que $f(X) = g(X) \cdot h(X)$, també és $f(z) = g(z) \cdot h(z)$). Aquest fet ens proporciona les condicions de divisibilitat $z^2 \cdot a + z \cdot b + c \mid f(z)$, una per a cada nombre enter $z \in \mathbb{Z}$. Per exemple, podem obtenir les relacions $c \mid a_0$ (que correspon a fer $z = 0$), $a + b + c \mid a_0 + a_1 + \cdots + a_n$ (que correspon a fer $z = 1$), $a - b + c \mid a_0 - a_1 + \cdots + (-1)^n a_n$ (que correspon a fer $z = -1$), $4a + 2b + c \mid a_0 + 2a_1 + \cdots + 2^n a_n$ (que correspon a fer $z = 2$), etcètera. De cadascuna d'aquestes relacions de divisibilitat, i si tenim en compte que, per a tot $z \in \mathbb{Z}$, el nombre de divisors de $f(z)$ és finit (observem que $f(z) \neq 0$ perquè $f(X)$ no té arrels), obtenim una quantitat finita d'equacions lineals. És a dir, per a cada nombre enter z, s'ha de satisfer que $a \cdot z^2 + b \cdot z + c$ sigui igual a algun dels divisors de $f(z)$.

Triem ara tres nombres enters diferents z_1, z_2, z_3 i, per a cadascun d'ells, considerem un divisor, que anomenem $d(z_i)$, de $f(z_i)$; d'aquesta manera obtindrem un sistema d'equacions lineals de matriu (ampliada)

$$\left[\begin{array}{ccc|c} z_1^2 & z_1 & 1 & d(z_1) \\ z_2^2 & z_2 & 1 & d(z_2) \\ z_3^2 & z_3 & 1 & d(z_3) \end{array}\right],$$

on el vector columna $[d(z_1), d(z_2), d(z_3)]^t$ és el terme independent del sistema i el determinant del qual és el determinant de Vandermonde

$$\begin{vmatrix} z_1^2 & z_1 & 1 \\ z_2^2 & z_2 & 1 \\ z_3^2 & z_3 & 1 \end{vmatrix} = (z_1 - z_2)(z_1 - z_3)(z_2 - z_3) \neq 0.$$

En conseqüència, el sistema és de Cramer i té solució única. Així, per a cada família $\{d(z_i)\}_{i=1,2,3}$, obtenim una solució racional (a, b, c) del sistema. Si descartem les solucions que no siguin enteres, obtindrem els possibles polinomis de grau 2 de $\mathbb{Z}[X]$ que divideixen $f(X)$; i, per divisió, obtindrem efectivament els divisors irreductibles de grau 2 de $f(X)$.

Observacions 6.10.6. • Notem que cal factoritzar els nombres enters $f(z_i)$; aquests nombres creixen de la mateixa manera que z_i^n, on n és el grau del polinomi $f(X)$; per tant, pot ésser costós de factoritzar-los. Però tenim el recurs de canviar de valor z_i tantes vegades com vulguem. Així, si per a un valor z no aconseguim factoritzar el nombre $f(z)$, podem canviar de valor i intentar-ho amb un nou valor de z.

• D'altra banda, un cop haguem obtingut una llista de possibles polinomis $aX^2 + bX + c$ divisors de $f(X)$, i si la llista és molt llarga, podem garbellar-la sense necessitat de més factoritzacions abans de procedir a les divisions. En efecte, per a cadascun dels polinomis obtinguts, i per a tots els nombres enters z, cal que se satisfaci que $az^2 + bz + c$ sigui un divisor de $f(z)$. Doncs, per a uns quants valors de z, la comprovació que aquesta propietat de divisibilitat no se satisfà (i per a això no cal factoritzar) permetrà descartar el polinomi $aX^2 + bX + c$ com a possible divisor de $f(X)$.

6.10.7. Un cop obtinguts tots els divisors de grau 2 de $f(X)$, si el polinomi que resta és de grau menor o igual que 5, automàticament és irreductible (perquè no té divisors de graus 1 ni 2). En cas contrari, provem la divisibilitat per un polinomi $g(X) = aX^3 + bX^2 + cX + d$ de coeficients indeterminats, de la mateixa manera que ho hem fet per a grau 2; ara caldrà usar un mínim de quatre nombres enters diferents z_1, z_2, z_3, z_4 per a obtenir un sistema lineal de matriu

$$\left[\begin{array}{cccc|c} z_1^3 & z_1^2 & z_1 & 1 & d(z_1) \\ z_2^3 & z_2^2 & z_2 & 1 & d(z_2) \\ z_3^3 & z_3^2 & z_3 & 1 & d(z_3) \\ z_4^3 & z_4^2 & z_4 & 1 & d(z_4) \end{array}\right],$$

també de Cramer, etcètera.

6.10.8. I així successivament, mentre el grau n del polinomi que resti sigui més gran o igual que $2k+1$, on k és el grau dels factors irreductibles que volem trobar en aquest pas.

Exemple 6.10.9. Intentem factoritzar el polinomi $f(X) = X^8 - X^4 + 1$.

Clarament, el polinomi no té factors irreductibles múltiples, perquè no té arrels complexes múltiples. Cerquem les seves arrels enteres. Com que el polinomi és mònic, les arrels de $f(X)$ només poden ser els divisors del terme independent; és a dir, 1, o -1; però $f(1) = f(-1) = 1 \neq 0$. Per tant, $f(X)$ no té divisors de grau 1.

Cerquem divisors de grau 2. Com que el polinomi $f(X)$ és mònic, i en virtut del lema de Gauss, només cal cercar-ne els divisors de grau 2 de la forma $g(X) = X^2 + bX + c$, $b, c \in \mathbb{Z}$. Si prenem per a z els valors 0, 1, obtenim que $c = g(0) \mid f(0) = 1$ i que $1 + b + c = g(1) \mid f(1) = 1$. Per tant, tenim quatre sistemes de dues equacions lineals:

$$\left.\begin{array}{r} c = 1 \\ 1 + b + c = 1 \end{array}\right\} \qquad \left.\begin{array}{r} c = -1 \\ 1 + b + c = 1 \end{array}\right\}$$

$$\left.\begin{array}{r} c = 1 \\ 1 + b + c = -1 \end{array}\right\} \qquad \left.\begin{array}{r} c = -1 \\ 1 + b + c = -1 \end{array}\right\}$$

El primer té solució $(c, b) = (1, -1)$, el segon, $(c, b) = (-1, 1)$, el tercer, $(c, b) = (1, -3)$, i el quart, $(c, b) = (-1, -1)$. Per tant, els únics polinomis de grau 2 que poden dividir

$f(X)$ són els polinomis X^2-X+1, X^2+X-1, X^2-3X+1, X^2-X-1. Si provem de fer les divisions, obtenim que cap d'aquests polinomis no divideix $f(X)$; per tant, $f(X)$ no té divisors de grau 2 de coeficients enters (ni racionals).

Repetim aquest procediment per al polinomi de grau 3 de coeficients indeterminats $g(X)=X^3+bX^2+cX+d$; per a $z=0,1,-1$, obtenim les condicions $d\in\{1,-1\}$, $1+b+c+d\in\{1,-1\}$, $-1+b-c+d\in\{1,-1\}$, que donen lloc als 8 sistemes de tres equacions

$$\left.\begin{array}{c} d=1\\ 1+b+c+d=1\\ -1+b-c+d=1\end{array}\right\} \qquad \left.\begin{array}{c} d=-1\\ 1+b+c+d=1\\ -1+b-c+d=1\end{array}\right\}$$

$$\left.\begin{array}{c} d=1\\ 1+b+c+d=1\\ -1+b-c+d=-1\end{array}\right\} \qquad \left.\begin{array}{c} d=-1\\ 1+b+c+d=1\\ -1+b-c+d=-1\end{array}\right\}$$

$$\left.\begin{array}{c} d=1\\ 1+b+c+d=-1\\ -1+b-c+d=1\end{array}\right\} \qquad \left.\begin{array}{c} d=-1\\ 1+b+c+d=-1\\ -1+b-c+d=1\end{array}\right\}$$

$$\left.\begin{array}{c} d=1\\ 1+b+c+d=-1\\ -1+b-c+d=-1\end{array}\right\} \qquad \left.\begin{array}{c} d=-1\\ 1+b+c+d=-1\\ -1+b-c+d=-1\end{array}\right\}$$

El càlcul de les solucions d'aquests sistemes dóna com a solucions les ternes de nombres enters $(b,c,d)\in\{(0,-1,1),\ (-1,0,1),\ (-1,-2,1),\ (-2,-1,1),\ (2,-1,-1),\ (1,0,-1),\ (1,-2,-1),\ (0,-1,-1)\}$, de manera que obtenim els 8 possibles polinomis que divideixen $f(X)$: X^3-X+1, X^3-X^2+1, X^3-X^2-2X+1, X^3-2X^2-X+1, X^3+2X^2-X-1, X^3+X^2-1, X^3+X^2-2X-1, X^3-X-1. Fetes les divisions, trobem que cap d'aquests polinomis no divideix $f(X)$, de manera que $f(X)$ no és divisible per cap polinomi de $\mathbb{Z}[X]$ de grau 3.

Observació 6.10.10. Abans de fer les divisions, podem garbellar aquests polinomis; per exemple, si prenem $z=2$, tenim que $f(2)=241$, mentre que els valors de $g(2)$ són, respectivament, 7, 5, 1, -1, 13, 11, 7, i 5; d'aquests, els únics divisors de 241 són 1 i -1, de manera que els únics polinomis que poden dividir $f(X)$ són els polinomis X^3-X^2-2X+1 i X^3-2X^2-X+1. Si calculem els valors que prenen aquests dos polinomis en $z=-2$, obtenim els valors -7 i -13, respectivament, que no són divisors de $f(-2)=241$; per tant, cap dels dos polinomis no és tampoc un divisor de $f(X)$. Ens hem estalviat, doncs, totes les divisions per polinomis.

Exercici 6.10.11. Es demana completar l'algoritme per a un polinomi de grau 4 de coeficients indeterminats per a deduir que $f(X)$ és irreductible.

Observació 6.10.12. Aquest polinomi forma part d'una família infinita de polinomis irreductibles: els polinomis ciclotòmics; de fet, és el polinomi ciclotòmic 24-èsim, $\Phi_{24}(X)$. La introducció dels polinomis ciclotòmics i la demostració de la seva irreductibilitat es deixen per a una altra ocasió.

6.10.13. Hom pot estar temptat de pensar que si un polinomi primitiu de $\mathbb{Z}[X]$ és irreductible, llavors també ho és mòdul p per a algun nombre primer p, de manera que una cerca de la irreductibilitat mòdul p per a suficients nombres primers p resoldria el problema de la irreductibilitat sobre $\mathbb{Z}$. L'exercici següent mostra que això no és així: es poden trobar polinomis mònics i irreductibles de $\mathbb{Z}[X]$ tals que, per a tot nombre primer p, són reductibles en reduir-los mòdul p.

Exercici 6.10.14. (a) Els polinomis $X^4 - 10X^2 + 1$ i $X^4 + 1 \in \mathbb{Z}[X]$ són irreductibles en $\mathbb{Z}[X]$.

(b) Aquests polinomis factoritzen en $\mathbb{Z}/p\mathbb{Z}[X]$, per a tot nombre primer p.

Exercici 6.10.15. (a) Els polinomis $X^5 - 4X + 2$, $3X^5 - 15$ i $2X^{10} - 21 \in \mathbb{Z}[X]$ són irreductibles en $\mathbb{Q}[X]$. Ho són en $\mathbb{Z}[X]$?

(b) El polinomi $X^6 + X^3 + 1 \in \mathbb{Z}[X]$ és irreductible en $\mathbb{Q}[X]$.

(c) Per a tot nombre natural $n \geq 1$, si $m \neq \pm 1$ és un nombre enter lliure de quadrats, el polinomi $X^n - m \in \mathbb{Z}[X]$ és irreductible en $\mathbb{Q}[X]$.

Exercici 6.10.16. Es demana determinar quins dels polinomis següents són irreductibles sobre $\mathbb{Q}$; i, d'aquells que no ho siguin, donar-ne la factorització com a producte de polinomis irreductibles:

(a) $X^4 - 2X^3 + 2X^2 + X + 4 \in \mathbb{Z}[X]$;

(b) $X^4 - 5X^3 + 3X - 2 \in \mathbb{Z}[X]$;

(c) $3X^5 - 4X^3 - 6X^2 + 6 \in \mathbb{Z}[X]$;

(d) $5X^5 - 6X^4 - 3X^2 + 9X - 15 \in \mathbb{Z}[X]$;

(e) $X^6 + 12X^5 + 49X^4 + 96X^3 + 99X^2 + 54X + 15 \in \mathbb{Z}[X]$;

(f) $X^5 + X^4 + 2X^3 + 2X^2 + 2X + 3 \in \mathbb{Z}[X]$.

Exercici 6.10.17. A l'anell de polinomis $(\mathbb{Z}/2\mathbb{Z})[X]$, els polinomis

$$X^2 + X + 1, \qquad X^3 + X + 1, \qquad X^3 + X^2 + 1,$$

són irreductibles; es demana trobar tots els polinomis irreductibles de grau 4.

Exercici 6.10.18. Es demana trobar les arrels de cadascun dels polinomis següents:

(a) $X^3 + 6X^2 + 11X + 6$, en $\mathbb{Z}/12\mathbb{Z}$;

(b) $3X^3 - 4X^2 - X + 4$, en $\mathbb{Z}/5\mathbb{Z}$;

(c) $5X^4 + 2X^2 - 3$, en $\mathbb{Z}/7\mathbb{Z}$;

(d) $X^3 + X + 1$, en $\mathbb{Z}/2\mathbb{Z}$.

Capítol 7

Mòduls finitament generats sobre dominis d'ideals principals

És ben conegut dels cursos bàsics d'àlgebra lineal que si K és un cos, tot K-espai vectorial de dimensió finita és isomorf a un K^n, on $n \geq 0$ és la dimensió de l'espai vectorial. Així, per als espais vectorials finitament generats, tenim un criteri de classificació: dos espais vectorials finitament generats són isomorfs si, i només si, són de la mateixa dimensió. Doncs, la dimensió és un invariant numèric que els determina, llevat d'isomorfisme. De fet, el resultat no es restringeix als espais vectorials de dimensió finita, i tot K-espai vectorial és isomorf a $K^{\#I}$, on $\#I$ és el cardinal d'una K-base, base que existeix en virtut del lema de Zorn (cf. **A.3.6**).

En el cas de mòduls sobre un anell commutatiu arbitrari, la situació és molt més complicada i no es coneix cap teorema **general** de classificació. Però hi ha un cas especialment interessant en el qual es pot donar una resposta de manera prou senzilla: el cas dels mòduls finitament generats sobre un domini d'ideals principals. En particular, això comprèn el cas dels grups abelians ($\mathbb{Z}$-mòduls), i també el cas dels mòduls sobre els anells de polinomis $K[X]$, on K és un cos. I aquest darrer cas inclou la classificació dels endomorfismes dels K-espais vectorials de dimensió finita.

L'objectiu bàsic d'aquest capítol és provar el teorema següent de classificació de mòduls finitament generats sobre dominis d'ideals principals, i d'explicitar-ne conseqüències.

Teorema 7.0.1. *Siguin K un domini d'ideals principals i M un K-mòdul finitament generat. Existeix un nombre enter únic, $r \geq 0$, i elements $d_1, \ldots, d_s \in K$, tals que*

(a) *per a $1 \leq i \leq s$ és $d_i \neq 0$ i $d_i \notin K^*$;*

(b) *per a $1 \leq i \leq s-1$ és $d_i \mid d_{i+1}$;*

(c) *per a $1 \leq i \leq s$, d_i és únic llevat del producte per un element invertible de K; i*

(d) $M \cong K^r \oplus \dfrac{K}{K\,d_1} \oplus \cdots \oplus \dfrac{K}{K\,d_s}$.

L'invariant r s'anomena el rang, i els d_i, els factors invariants de M.

7.1 Preliminars d'àlgebra lineal

Amb la finalitat de no interrompre l'argument bàsic que utilitzarem per a la classificació dels mòduls finitament generats sobre un domini d'ideals principals, que és l'objectiu principal del capítol, encetem la discussió amb un parell de conceptes i de resultats que seran útils a la discussió general i que tenen interès independent.

Definició 7.1.1. Siguin B un anell i $A \subseteq B$ un subanell, qualssevol. Donat un B-mòdul (per l'esquerra o per la dreta), E, podem considerar la restricció a A de l'acció de B en el grup additiu de E. D'aquesta manera E també és un A-mòdul. Es diu que s'obté per restricció d'escalars a A.

Observació 7.1.2. La definició s'aplica, en particular, en el cas que K és un domini d'integritat, Q el seu cos de fraccions, i E un Q-espai vectorial. Llavors, E també és, per restricció d'escalars a K, un K-mòdul.

Proposició 7.1.3. *Siguin K un domini d'integritat, Q el seu cos de fraccions, i E un Q-espai vectorial. Tot subconjunt K-linealment independent, $S \subseteq E$, és Q-linealment independent. En conseqüència, $\#S \leq \dim_Q E$; és a dir, S és de cardinal menor o igual que la dimensió de E com a Q-espai vectorial.*

Demostració: Sigui $S \subseteq E$ un subconjunt K-linealment independent. Si existeix un subconjunt finit $T \subseteq S$ i elements $\lambda_s \in Q$, per a $s \in T$, tals que $\sum_{s\in T} \lambda_s\, s = 0$, podem considerar un denominador comú, $d \in K$, de tots els coeficients λ_s, $s \in T$, de manera que $d \cdot \lambda_s \in K$. Llavors, $\sum_{s\in T} (d\,\lambda_s)\, s = d \sum_{s\in T} \lambda_s\, s = 0$, i $d\,\lambda_s = 0$, perquè T és K-linealment independent. Però, llavors, per a tot $s \in T$ és $\lambda_s = 0$, com calia provar per a veure la Q-independència lineal de T. □

Observació 7.1.4. Notem que per a considerar un denominador comú d'una quantitat finita d'elements del cos de fraccions Q de K, només cal que K sigui un domini d'integritat, sense cap més condició de factorialitat. En efecte, donats $\lambda_1, \ldots, \lambda_n \in Q$, existeixen elements $a_i, b_i \in K$, $b_i \neq 0$, per a $1 \leq i \leq n$, tals que $\lambda_i = \dfrac{a_i}{b_i}$; llavors, podem considerar $d = b_1 \cdots b_n \in K$. Com que K és un domini d'integritat, resulta que $d \neq 0$, i que $d\,\lambda_i = b_1 \cdots b_{i-1}\, a_i\, b_{i+1} \cdots b_n \in K$, per a $1 \leq i \leq n$.

Proposició 7.1.5. *Siguin K un domini d'integritat, Q el seu cos de fraccions, E, E', Q-espais vectorials i M un K-mòdul. Considerem E i E' com a K-mòduls per restricció d'escalars a K i suposem que existeixen aplicacions K-lineals injectives $\varphi : M \longrightarrow E$, $\varphi' : M \longrightarrow E'$. Llavors, la dimensió del subespai vectorial de E generat per $\varphi(M)$ coincideix amb la dimensió del subespai vectorial de E' generat per $\varphi'(M)$.*

Demostració: Donat un subconjunt qualsevol $S \subseteq M$, resulta que $\varphi(S)$ és Q-linealment independent en E si, i només si, és K-linealment independent en E, o també en $\varphi(M)$; però com que φ és un K-isomorfisme de M en $\varphi(M)$, això equival a dir que S és K-linealment independent en M. I, anàlogament, això equival a dir que $\varphi'(S)$ és Q-linealment independent en E'.

En particular, $\varphi(S)$ és un subconjunt Q-linealment independent maximal de $\varphi(M)$; si, i només si, $\varphi'(S)$ és un subconjunt Q-linealment independent maximal de $\varphi'(M)$; si, i només si, S és un subconjunt K-linealment independent maximal de M.

Com que φ i φ' són injectives i, per tant, determinen bijeccions amb les seves imatges corresponents, els cardinals dels subconjunts Q-linealment independents maximals de $\varphi(M)$ i $\varphi'(M)$ coincideixen, com calia provar. □

Definició 7.1.6. Siguin K un domini d'integritat qualsevol, Q el seu cos de fraccions, i M un K-mòdul per al qual existeix una aplicació K-lineal injectiva $\varphi : M \longrightarrow E$, en un Q-espai vectorial, considerat com a K-mòdul per restricció d'escalars. S'anomena rang de M, i es denota rang (M), la dimensió del Q-subespai vectorial de E generat per $\varphi(M)$; notem que és independent de E i de φ.

Observació 7.1.7. Siguin K un domini d'integritat i Q el seu cos de fraccions. La definició anterior s'aplica a tot K-submòdul, $M \subseteq N$, d'un K-mòdul lliure, N.

En efecte, si N és un K-mòdul lliure de base B, tenim que $N = \bigoplus_{v\in B} K\,v$. Considerem el Q-espai vectorial lliure de base B, posem E; podem escriure'l en la forma $E = \bigoplus_{v\in B} Q\,v$ i, llavors, les assignacions

$$\sum_{v\in C} a_v\,v \mapsto \sum_{v\in C} a_v\,v, \qquad C \subseteq B,\ \text{finit}, \quad a_v \in K,\ \text{per a } v \in C,$$

no depenen de l'elecció de C i determinen una aplicació K-kineal injectiva, $\varphi : N \longrightarrow E$, que identifica N amb un K-submòdul de E.

Ara, la inclusió de M en N seguida de la inclusió φ de N en E és una aplicació K-lineal injectiva de M en E i, per tant, estem en les condicions de la definició. Notem que, en particular, rang $(M) \leq \#B$.

7.2 Teorema de classificació. Existència

Teorema 7.2.1. *Siguin K un domini d'ideals principals, M un K-mòdul lliure de dimensió finita, m, i $N \subseteq M$ un K-submòdul, que suposem no nul. Llavors,*

(a) *N és lliure de dimensió $n \leq m$; i*

(b) *existeix una K-base $\{e_1, \ldots, e_m\}$ de M i existeixen elements $d_1, \ldots, d_n \in K$, tals que per a $1 \leq i \leq n-1$ és $d_i \mid d_{i+1}$, i el conjunt $\{d_1\,e_1, \ldots, d_n\,e_n\}$ és una K-base de N.*

Demostració: A fi d'obtenir ideals de K a partir dels K-mòduls M i N i dels seus K-submòduls, serà útil considerar el dual lineal de M, $\widehat{M} := \mathrm{Hom}_K(M, K)$, perquè la imatge de qualsevol submòdul de M per qualsevol forma lineal $u \in \widehat{M}$ és un K-submòdul de K; o sigui, un ideal de K. A més a més, com que K és un domini d'ideals principals, obtindrem ideals principals, dels quals podrem considerar-ne elements generadors, definits llevat del producte per elements invertibles de K.

D'altra banda, a fi de relacionar el rang dels K-submòduls de M amb la dimensió de M, convindrà considerar el cos de fraccions Q de K i el Q-subespai vectorial generat per aquests K-submòduls dins del Q-espai vectorial generat per M, que és de dimensió m.

Observem que, com que M és K-lliure, $\widehat{M}$ també. En efecte, sigui $\{x_1, \ldots, x_m\}$ una K-base de M; llavors les formes coordenades respecte d'aquesta base, $\pi_i : M \longrightarrow K$,

$1 \leq i \leq m$, definides per $\pi_i(x_j) := \begin{cases} 1, \text{ si } j = i, \\ 0, \text{ si } j \neq i, \end{cases}$ constitueixen una K-base de $\widehat{M}$: la base dual de la base $\{x_1, \ldots, x_m\}$. Notem que si M és de dimensió 1, llavors $M = K\,x_1$ i, com que $\{x_1\}$ és linealment independent, M s'identifica amb $K = K\,1$; d'aquesta manera, els K-submòduls de M, i, en particular, N, s'identifiquen amb els ideals de K, que són principals; és a dir, amb els ideals $K\,d_1$, $d_1 \in K$. Això prova el teorema en el cas $m = 1$. Es tracta, ara, de procedir per inducció. I convé estudiar amb deteniment el pas inductiu. Construirem els elements e_1 i $e_1' := d_1\,e_1$.

Considerem el conjunt d'ideals $\mathcal{I}(N) := \{u(N) \subseteq K : u \in \widehat{M}\}$; com que $u(N) \subseteq K$ és principal, existeix $d_u \in K$ tal que $u(N) = K\,d_u$, i podem escriure el conjunt d'ideals $\mathcal{I}(N)$ en la forma $\mathcal{I}(N) := \{K\,d_u \subseteq K : u \in \widehat{M}\}$. Tenim que $\mathcal{I}(N)$ és un conjunt no buit d'ideals d'un domini d'ideals principals; per tant, existeix un element maximal del conjunt. Així, existeix una forma lineal $u_0 \in \widehat{M}$ tal que l'ideal $K\,d_{u_0}$ és maximal en el conjunt $\mathcal{I}(N)$. (Notem, però, que pot ser que sigui $K\,d_{u_0} = K$ i, per tant, no podem dir que $K\,d_{u_0}$ sigui un ideal maximal de K.) Però, com que $N \neq \{0\}$, existeix algun índex i, $1 \leq i \leq m$, tal que $\pi_i(N) \neq \{0\}$ i, per tant, en el conjunt $\mathcal{I}(N)$, hi ha algun ideal no nul; en conseqüència, $d_{u_0} \neq 0$ i, per la definició $K\,d_{u_0} = u_0(N)$, existeix $e' \in N$ tal que $u_0(e') = d_{u_0}$. Aquest element e' serà el nostre $e_1' = d_1\,e_1$, i l'element d_{u_0} serà l'element d_1. Però encara hem de treballar una mica; en particular, encara hem de treballar per a definir l'element e_1.

Afirmació 1: Per a tota forma lineal $v \in \widehat{M}$, l'element d_{u_0} divideix l'element $v(e') \in K$.

> En efecte. Donada una forma lineal $v \in \widehat{M}$, sigui $d := \mathrm{mcd}(d_{u_0}, v(e'))$; si veiem que $K\,d_{u_0} = K\,d$, tindrem que $d_{u_0} = \mathrm{mcd}(d_{u_0}, v(e'))$ i, per tant, que $d_{u_0} \mid v(e')$. Ara bé, com que K és un domini d'ideals principals, existeixen elements $b, c \in K$ tals que $d = b\,d_{u_0} + c\,v(e')$; aleshores, per a la forma $w := b\,u_0 + c\,v \in \widehat{M}$, és $w(e') = b\,u_0(e') + c\,v(e') = b\,d_{u_0} + c\,v(e') = d$. D'altra banda, tenim les inclusions $K\,d_{u_0} \subseteq K\,d = K\,w(e') \subseteq w(N) = K\,d_w$ i, com que $K\,d_{u_0}$ és maximal en el conjunt $\mathcal{I}(N)$, obtenim la igualtat $K\,d_{u_0} = K\,d = K\,d_w$, que volíem veure.

Com a conseqüencia d'aquesta afirmació, i com que $\pi_i \in \widehat{M}$, $1 \leq i \leq m$, obtenim que $d_{u_0} \mid \pi_i(e')$, per a tot índex $1 \leq i \leq m$; per tant, per a tot i, $1 \leq i \leq m$, existeix un element $b_i \in K$ tal que $\pi_i(e') = d_{u_0}\,b_i$. Per a aquests escalars $b_i \in K$, podem considerar l'element $e := \sum_{i=1}^{m} b_i\,x_i \in M$, i és clar que

$$d_{u_0}\,e = \sum_{i=1}^{m} d_{u_0}\,b_i\,x_i = \sum_{i=1}^{m} \pi_i(e')\,x_i = e'.$$

A més a més, $d_{u_0} = u_0(e') = u_0(d_{u_0}\,e) = d_{u_0}\,u_0(e)$; i com que $d_{u_0} \neq 0$ i K és un domini d'integritat, $u_0(e) = 1$.

Afirmació 2: $M = K\,e \oplus \ker u_0$ i $N = K\,e' \oplus (N \cap \ker u_0)$.

> En efecte, comencem per provar que les dues sumes són directes i després, de seguida, veurem que sumen M i N, respectivament.
>
> Per a això, com que $e' = d_{u_0}\,e$, resulta que $K\,e' \subseteq K\,e$, i com que $N \cap \ker u_0 \subseteq \ker u_0$, si veiem que $K\,e \cap \ker u_0 = \{0\}$, també tindrem que l'altra intersecció és nul·la:

$K\,e' \cap (N \cap \ker u_0) = \{0\}$. Però si $x \in K\,e \cap \ker u_0$, existeix $\lambda \in K$ tal que $x = \lambda\,e$ i que $u_0(x) = 0$; així, $0 = u_0(x) = u_0(\lambda\,e) = \lambda\,u_0(e) = \lambda$, perquè $u_0(e) = 1$, de manera que $x = 0$.

Per a veure la part de l'afirmació que fa referència a les sumes, notem que les inclusions $K\,e \oplus \ker u_0 \subseteq M$ i $K\,e' \oplus (N \cap \ker u_0) \subseteq N$ són immediates. Vegem les contràries. Donat $x \in M$, podem escriure $x = u_0(x)\,e + (x - u_0(x)\,e) \in K\,e + \ker u_0$, perquè $u_0(e) = 1$. De manera semblant, donat $y \in N$, $u_0(y) \in u_0(N) = K\,d_{u_0}$, de manera que existeix $b \in K$ tal que $u_0(y) = b\,d_{u_0}$; llavors, $u_0(y)\,e = b\,e' \in K\,e'$, i $y - u_0(y)\,e \in N \cap \ker u_0$, de manera que $y = u_0(y)\,e + \big(y - u_0(y)\,e\big) \in K\,e' + (N \cap \ker u_0)$.

Afirmació 3: (O sigui, propietat (a) de l'enunciat) N és lliure de dimensió finita $n \leq m$.

Ho demostrarem per inducció sobre el rang $q := \operatorname{rang}(N)$. Notem que $q \neq 0$, perquè $N \neq \{0\}$ i, per tant, el Q-subespai vectorial generat per N dins del Q-espai vectorial generat per M és no nul.

Ara, per a $q \geq 1$, resulta que $N \cap \ker u_0$ és un K-submòdul de N que admet un K-submòdul suplementari no nul en N, $K\,e'$; per tant, dins del Q-espai vectorial $V := \bigoplus_{i=1}^{m} K\,x_i$, el Q-subespai generat per $N \cap \ker u_0$ és de dimensió $q - 1 < q$. En efecte, tenim que el vector e' és K-linealment independent de $N \cap \ker u_0$ i, per tant, Q-linealment independent del Q-subespai vectorial generat per $N \cap \ker u_0$. Això és dir que $\operatorname{rang}(N \cap \ker u_0) = q - 1$. Podem raonar per inducció i obtenim que $N \cap \ker u_0$ és un K-submòdul lliure de dimensió finita; i com que la reunió de $\{e'\}$ amb una K-base de $N \cap \ker u_0$ és una K-base de N, obtenim que N és lliure de dimensió finita. Ara, per força, la seva dimensió és menor o igual que la del Q-espai vectorial que genera; per tant, $n \leq m$.

Resta demostrar la propietat (b) de l'enunciat, i ho farem per inducció sobre la dimensió, m, de M. I ja ho hem provat en el cas $m = 1$, al començament. Com que si fos $\ker u_0 = \{0\}$, tindríem que $M = K\,e$, de dimensió 1, podem suposar que $\ker u_0 \neq \{0\}$. Com que $\ker u_0$ admet un suplementari de dimensió 1, amb un argument anàleg al que hem usat per a provar que $N \cap \ker u_0$ és lliure de dimensió $q - 1$, ara demostrem que $\ker u_0$ és un K-submòdul lliure de dimensió $m - 1$ de M. I la hipòtesi d'inducció aplicada al K-mòdul lliure $\ker u_0$ i el K-submòdul $N \cap \ker u_0$ ens proporciona l'existència d'una K-base $\{e_2, \ldots, e_m\}$ de $\ker u_0$ i la d'elements $d_2, \ldots, d_n \in K$, no nuls i tals que d_i divideix d_{i+1}, per a $2 \leq i \leq n - 1$, per als quals $\{d_2\,e_2, \ldots, d_n\,e_n\}$ és una K-base de $N \cap \ker u_0$.

Posem $e_1 := e$ i $d_1 := d_{u_0}$, com ja hem comentat més amunt. L'afirmació 2 ens assegura que $\{e_1, e_2, \ldots, e_m\}$ és una K-base de M i que $\{d_1\,e_1, d_2\,e_2, \ldots, d_n\,e_n\}$ és una K-base de N. I hem vist que $d_1 \neq 0$. Només resta veure que d_1 divideix d_2.

Per a això, i com que $\{e_1, \ldots, e_m\}$ és una K-base de M, podem considerar la forma K-lineal $v : M \longrightarrow K$ definida per les assignacions $v(e_1) = v(e_2) = 1$, $v(e_i) := 0$, per a $3 \leq i \leq m$. Llavors,

$$d_1 = d_{u_0} = d_{u_0}\,v(e_1) = v(d_{u_0}\,e_1) = v(d_{u_0}\,e) = v(e') \in v(N) = K\,d_v,$$

de manera que $K\,d_{u_0} \subseteq K\,d_v$ i, per la maximalitat de $K\,d_{u_0}$, tenim que $K\,d_{u_0} = K\,d_v$. Com que $d_2 = d_2\,v(e_2) = v(d_2\,e_2) \in v(N) = K\,d_v$, resulta que d_v divideix d_2 i, com que d_1 i d_v són associats, obtenim la propietat de divisibilitat $d_1 \mid d_2$ que restava provar. □

Ara ja podem provar la part del teorema de classificació, **7.0.1**, que fa referència a l'existència. Més endavant en provarem la unicitat, però, abans, n'obtindrem conseqüències.

Corol·lari 7.2.2. *Siguin K un domini d'ideals principals i M un K-mòdul finitament generat. Existeix un nombre enter $r \geq 0$, i existeixen elements no nuls i no invertibles $d_1, \ldots, d_s \in K$ tals que $M \cong K^r \oplus \dfrac{K}{K\,d_1} \oplus \cdots \oplus \dfrac{K}{K\,d_s}$ i que d_i divideix d_{i+1}, per a $1 \leq i \leq s-1$.*

Demostració: Sigui $G := \{y_1, \ldots, y_m\}$ un conjunt finit de generadors de M, i considerem un K-mòdul lliure, $L(B)$, de base $B := \{x_1, \ldots, x_m\}$, del mateix cardinal, m, que G. Llavors, existeix una única aplicació K-lineal, $\varphi : L(B) \longrightarrow M$, determinada per $\varphi(x_i) := y_i$, $1 \leq i \leq m$, i és exhaustiva. Sigui $L' := \ker\varphi$ el nucli; se satisfà que $M \cong \dfrac{L(B)}{L'}$. Fins aquí, el resultat és general per a mòduls finitament generats sobre anells qualssevol. Ara, en tenir en compte que K és d'ideals principals, i en virtut del teorema **7.2.1**, existeix una K-base $\{e_1, \ldots, e_m\}$ de $L(B)$, i elements no nuls $d_1, \ldots, d_n \in K$, tals que, per a $1 \leq i \leq n-1$, d_i divideix d_{i+1}, i que, si posem $d_i := 0$, per a $n+1 \leq i \leq m$, és

$$M \cong \frac{L(B)}{L'} \cong \frac{\bigoplus_{i=1}^{m} K\,e_i}{\bigoplus_{i=1}^{m} K\,d_i\,e_i} \cong \bigoplus_{i=1}^{m} \frac{K\,e_i}{K\,d_i\,e_i} \cong \bigoplus_{i=1}^{m} \frac{K}{K\,d_i}.$$

Clarament, per a $n+1 \leq i \leq m$ és $K\,d_i = \{0\}$, de manera que $\dfrac{K}{K\,d_i} \cong K$. D'altra banda, per als elements $d_1, \ldots, d_k$, $k \leq n$, que siguin invertibles és $K\,d_i = K$, de manera que $\dfrac{K}{K\,d_i} = \{0\}$.

Així, és suficient escriure $r := m - n$, eliminar els elements $d_1, \ldots, d_k$ tals que $d_i \in K^*$, i renumerar els altres com a $d_1, \ldots, d_s$, per a obtenir la descomposició que se cerca,

$$M \cong K^r \oplus \frac{K}{K\,d_1} \oplus \cdots \oplus \frac{K}{K\,d_s},$$

on $r, s \geq 0$, $d_1, \ldots, d_s \in K$, no nuls i no invertibles, i d_i divideix d_{i+1}, per a $1 \leq i \leq s-1$. □

7.3 Torsió. Components primaris

Definició 7.3.1. Siguin K un domini d'integritat i M un K-mòdul. El subconjunt

$$T(M) := \{v \in M : \text{existeix } d \in K, d \neq 0,\ d\,v = 0\} \subseteq M$$

és un K-submòdul de M; s'anomena el submòdul de torsió de M. Un K-mòdul M s'anomena de torsió si $M = T(M)$; s'anomena sense torsió o lliure de torsió si $T(M) = \{0\}$.

Observació 7.3.2. Si K no és un domini d'integritat, el conjunt $T(M)$ no té per què ser un submòdul. Per exemple, per a $K = \mathbb{Z}/6\mathbb{Z}$ i $M = K$, tenim que $2, 3 \in T(K)$, però $1 = 3 - 2 \notin T(K)$.

Corol·lari 7.3.3. *Siguin K un domini d'ideals principals i M un K-mòdul finitament generat i sense torsió. Llavors, M és un K-mòdul lliure.*

Demostració: Apliquem el corol·lari **7.2.2**, del qual en mantenim les notacions. Donats elements no nuls $d_1, \dots, d_s \in K$, el K-mòdul $\dfrac{K}{K\,d_1} \oplus \cdots \oplus \dfrac{K}{K\,d_s}$ és de torsió, anul·lat pel producte $d_1 \cdots d_s$; per tant, aquesta part de la descomposició de M no hi pot ser, i obtenim que existeix $r \geq 0$ tal que $M \cong K^r$; és a dir, que M és lliure de dimensió r. □

Observació 7.3.4. El resultat no és cert, en general, si l'anell K no és un domini d'ideals principals. Per exemple, si posem $K := \mathbb{Z}[X]$, l'anell de polinomis de coeficients enters, l'ideal $(2, X)$ és finitament generat i sense torsió, però no és un K-mòdul lliure. En efecte, d'una banda, no és principal i, per tant, no és lliure de dimensió 1; i, de l'altra, tot conjunt de més d'un element en K és K-linealment dependent; per tant, K no conté cap submòdul lliure de dimensió més gran que 1; en particular, $(2, X)$ no pot ser lliure com a K-mòdul.

Corol·lari 7.3.5. *Siguin K un domini d'ideals principals i M un K-mòdul finitament generat. Existeix un K-submòdul L de M que és alhora lliure i un suplementari de la torsió de M; és a dir, tal que $M = T(M) \oplus L$. Tot i que L, en general, no és únic, la seva dimensió és un invariant de M; dit d'una altra manera, el K-mòdul quocient $\dfrac{M}{T(M)}$ és lliure i de rang determinat per M.*

Demostració: En virtut del corol·lari **7.2.2**, del qual en mantenim les notacions, tenim que $M \cong K^r \oplus \dfrac{K}{K\,d_1} \oplus \cdots \oplus \dfrac{K}{K\,d_s}$, i el K-submòdul de M que correspon a K^r és lliure, de dimensió r, i alhora és un suplementari de la torsió de M, que és el K-submòdul que es correspon amb $\dfrac{K}{K\,d_1} \oplus \cdots \oplus \dfrac{K}{K\,d_s}$. □

Corol·lari 7.3.6. *Siguin K un domini d'ideals principals, P un conjunt de representants dels elements primers de K, i M un K-mòdul finitament generat. Llavors, existeixen un nombre enter $r \geq 0$, un subconjunt finit $R \subseteq P$, i per a cada $p \in R$ una quantitat finita de nombres enters, $1 \leq e_{p,1} \leq e_{p,2} \leq \cdots \leq e_{p,r_p}$, tals que*

$$M \cong K^r \oplus \bigoplus_{p \in R} \left(\bigoplus_{j=1}^{r_p} \frac{K}{K\,p^{e_{p,j}}} \right).$$

Demostració: Per a tot element $d \in K$, $d \neq 0$, podem considerar la seva descomposició com a producte d'elements primers en K, $d = \varepsilon \prod_{p \in P} p^{v_p(d)}$, on $v_p(d) \geq 0$, i $v_p(d) = 0$ per a tot $p \in P$ llevat, potser, d'una quantitat finita, i $\varepsilon \in K^*$. Si anomenem R el conjunt dels elements $p \in P$ tals que $v_p(d) \neq 0$, llavors R és un conjunt finit i el teorema xinès del residu proporciona un isomorfisme d'anells, i de K-mòduls,

$$\frac{K}{K\,d} \cong \prod_{p \in R} \frac{K}{K\,p^{v_p(d)}}.$$

Notem que, com a K-mòduls, és

$$\prod_{p \in R} \frac{K}{K\,p^{v_p(d)}} \cong \bigoplus_{p \in R} \frac{K}{K\,p^{v_p(d)}},$$

perquè el producte (i, en conseqüència, la suma) només conté una quantitat finita de K-mòduls no nuls. Si ara apliquem aquesta descomposició a cadascun dels factors $\dfrac{K}{K\,d_i}$ de la descomposició $M \cong K^r \oplus \dfrac{K}{K\,d_1} \oplus \cdots \oplus \dfrac{K}{K\,d_s}$, només cal reordenar els sumands per a obtenir l'expressió demanada. □

Definició 7.3.7. Siguin K un domini d'integritat i M un K-mòdul. Per a tot element $d \in K$, la multiplicació per d, $\varphi_d : M \longrightarrow M$, donada per $x \mapsto d\,x$, per a tot $x \in M$, és una aplicació K-lineal, de manera que el seu nucli és un K-submòdul de M. S'anomena el K-submòdul de d-torsió de M; sovint es representa per $M[d] := \ker \varphi_d = \{x \in M :\ d\,x = 0\}$.

Observacions 7.3.8. • Notem que aquesta definició és un refinament de la definició **7.3.1**, i que $T(M) = \bigcup_{d \in K - \{0\}} M[d]$.

• Suposem que K és un domini d'ideals principals i que $p \in K$ és un element primer; llavors, la reunió $T_p(M) := \bigcup_{r \geq 0} M[p^r]$ és un K-submòdul de M, que s'anomena la p^∞-torsió de M. Notem que $T_p(M) := \{x \in M :\ \text{existeix } r \geq 0 \text{ i } p^r\,x = 0\}$ és un K-submòdul de M i, també, de $T(M)$.

Corol·lari 7.3.9. *Siguin K un domini d'ideals principals, P un conjunt de representants dels elements primers de K, i M un K-mòdul finitament generat. Llavors, amb les notacions del corol·lari* **7.3.6**, *tenim que, per a tot $p \in P$, és $T_p(M) \cong \bigoplus_{j=1}^{r_p} \dfrac{K}{K\,p^{e_{p,j}}}$. I, en particular, que $T(M) \cong \bigoplus_{p \in P} T_p(M)$.*

Demostració: Exercici. □

Definició 7.3.10. Siguin K un domini d'ideals principals i M un K-mòdul finitament generat i de torsió. Llavors, $M = T(M) \cong \bigoplus_{p \in P} T_p(M)$; els K-submòduls $T_p(M)$ s'anomenen els components p-primaris de M, i la descomposició, la descomposició en components primaris.

7.4 Unicitat. Factors invariants

A fi d'establir la unicitat de la descomposició d'un K-mòdul finitament generat sobre un domini d'ideals principals, K, convé tenir en compte alguns preliminars immediats.

Definició 7.4.1. Siguin K un anell commutatiu i M un K-mòdul. S'anomena anul·lador de M l'ideal $\mathrm{Ann}(M) := \{a \in K :\ \text{per a tot } v \in M,\ a\,v = 0\} \subseteq K$.

Observació 7.4.2. Siguin K un anell commutatiu i M un K-mòdul. Com que l'acció de $\mathrm{Ann}(M)$ en M és trivial, M és, de manera natural, un $\dfrac{K}{\mathrm{Ann}(M)}$-mòdul.

Exemples 7.4.3. • Per a tot nombre natural n, $\mathbb{Z}/n\mathbb{Z}$ és un $\mathbb{Z}$-mòdul, d'anul·lador $n\mathbb{Z}$.

• Més generalment, si m, n són nombres naturals tals que $n \mid m$, llavors $\mathbb{Z}/n\mathbb{Z}$ és un $\mathbb{Z}/m\mathbb{Z}$-mòdul, d'anul·lador l'ideal $\dfrac{m}{n}\dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

• Siguin K un cos, E un K-espai vectorial de dimensió finita, i $f \in \mathrm{End}_K(E)$ un endomorfisme. Llavors, E és un $K[X]$-mòdul, d'anul·lador l'ideal $m_f(X)\,K[X]$, on $m_f(X)$ és el polinomi mínim de l'endomorfisme f. Notem que E és un K-mòdul finitament generat sobre un anell d'ideals principals, $K[X]$; per tant, el teorema d'estructura s'hi aplica.

Observació 7.4.4. Sigui K un anell commutatiu. Per a ideals diferents, $\mathfrak{a}, \mathfrak{b} \subseteq K$, $\mathfrak{a} \neq \mathfrak{b}$, pot ser que $\dfrac{K}{\mathfrak{a}} \cong \dfrac{K}{\mathfrak{b}}$ com a anells. Per exemple, podem prendre, en un anell de polinomis $K[X,Y]$, els ideals $\mathfrak{a} := X\,K[X,Y]$, i $\mathfrak{b} := Y\,K[X,Y]$. Llavors, com a anells (i també com a K-àlgebres),

$$\frac{K[X,Y]}{\mathfrak{a}} \cong K[Y] \cong K[X] \cong \frac{K[X,Y]}{\mathfrak{b}}.$$

Però, en canvi, si es té un isomorfisme $\dfrac{K}{\mathfrak{a}} \cong \dfrac{K}{\mathfrak{b}}$ com a K-mòduls, llavors ha de ser $\mathfrak{a} = \mathfrak{b}$ (i no n'hi ha prou amb un isomorfisme entre $\mathfrak{a}$ i $\mathfrak{b}$). En efecte, K-mòduls isomorfs tenen el mateix ideal anul·lador.

Teorema 7.4.5. *Siguin K un domini d'ideals principals i M un K-mòdul finitament generat. Els nombres enters $r, s \geq 0$ i els elements $d_1, \ldots, d_s \in K$, no nuls i no invertibles, tals que d_i divideix d_{i+1}, per a $1 \leq i \leq s-1$, i que*

$$M \cong K^r \oplus \bigoplus_{i=1}^{s} \frac{K}{K\,d_i},$$

són únics, llevat del producte de cada d_i per un element invertible de K.

Demostració: Ja hem vist la unicitat de r, que és el rang del K-mòdul lliure $M/T(M)$. Si ara tenim en compte la descomposició en components primaris de la torsió, $T(M) = \bigoplus_{p \in P} T_p(M)$, on P és un conjunt de representants dels elements primers de K, i que es tenen isomorfismes del tipus

$$T_p(M) \cong \bigoplus_{j=1}^{r_p} \frac{K}{K\,p^{e_{p,j}}},$$

(cf. el corol·lari **7.3.9**), és suficient demostrar la unicitat dels nombres enters $e_{p,j} \in \mathbb{N}$.

Ara bé, per a tot nombre natural $k \geq 0$, tenim que

$$p^k\,T_p(M) = \bigoplus_{e_{p,j} > k} \frac{K\,p^k}{K\,p^{e_{p,j}}}.$$

Per tant,

$$\frac{p^k\,T_p(M)}{p^{k+1}\,T_p(M)} = \frac{\displaystyle\bigoplus_{e_{p,j}>k} \frac{K\,p^k}{K\,p^{e_{p,j}}}}{\displaystyle\bigoplus_{e_{p,j}>k+1} \frac{K\,p^{k+1}}{K\,p^{e_{p,j}}}} \cong \bigoplus_{e_{p,j}>k} \frac{K\,p^k}{K\,p^{k+1}} \cong \bigoplus_{e_{p,j}>k} \frac{K}{K\,p}.$$

Així, $\dfrac{p^k\,T_p(M)}{p^{k+1}\,T_p(M)}$ és un $\dfrac{K}{K\,p}$-espai vectorial de dimensió finita, i la seva dimensió no depèn, òbviament, de la descomposició que considerem de $T_p(M)$. Però l'isomorfisme que acabem de mostrar ens ensenya que aquesta dimensió és la quantitat d'exponents $e_{p,j}$ de la descomposició per als quals és $e_{p,j} > k$.

Com a conseqüència, el nombre d'exponents $e_{p,j}$ que prenen el valor $k \geq 1$, fixat, és la diferència entre les dimensions dels $\dfrac{K}{K\,p}$-espais vectorials $\dfrac{p^{k-1}\,T_p(M)}{p^k\,T_p(M)}$ i $\dfrac{p^k\,T_p(M)}{p^{k+1}\,T_p(M)}$. Per tant, la descomposició és única. □

Definició 7.4.6. Siguin K un domini d'ideals principals i M un K-mòdul finitament generat. Els ideals no trivials de K, $K\,d_1$, …, $K\,d_s$, tals que d_i divideix d_{i+1} per a $1 \leq i \leq s-1$, i que $T(M) \cong \bigoplus_{i=1}^{s} \dfrac{K}{K\,d_i}$, s'anomenen els factors invariants de M. Més generalment, si M és un K-mòdul lliure de dimensió finita i $N \subseteq M$ és un K-submòdul, els factors invariants de N en M són els factors invariants de $T(M/N)$.

7.5 Càlcul dels factors invariants

Problema 7.5.1. Sigui K un domini d'ideals principals, i suposem donat un K-mòdul M per una presentació finita; és a dir, per una quantitat finita de generadors i de relacions. Ens plantegem el problema de calcular el tipus d'isomorfisme de M; és a dir, la dimensió de la part lliure i els factors invariants de la torsió.

Comencem per provar el resultat següent.

Proposició 7.5.2. *Siguin K un domini d'ideals principals; L i N, K-mòduls lliures de dimensions finites, i $\varphi : L \longrightarrow N$ una aplicació K-lineal qualsevol. Llavors, existeix un K-submòdul $N' \subseteq L$ tal que $L = \ker\varphi \oplus N'$ i que la restricció de φ a N', $\varphi_{|_{N'}} : N' \longrightarrow \operatorname{im}\varphi$, és un isomorfisme. En particular,* $\dim_K L = \dim_K \ker\varphi + \dim_K \operatorname{im}\varphi$.

Observació 7.5.3. Notem que no diem que L sigui la suma directa del nucli i de la imatge, fet que, òbviament, pot ser fals.

Demostració: En virtut del teorema **7.2.1**, $\operatorname{im}\varphi \subseteq N$ és un K-mòdul lliure de dimensió finita. Sigui $\{u_1, \ldots, u_n\}$ una K-base de $\operatorname{im}\varphi$, i considerem elements $v_1, \ldots, v_n \in L$ tals que $\varphi(v_i) = u_i$, per a $1 \leq i \leq n$. Podem considerar, doncs, l'única aplicació K-lineal $\psi : \operatorname{im}\varphi \longrightarrow L$ tal que $\psi(u_i) := v_i$, $1 \leq i \leq n$. I és clar que $\varphi \circ \psi = \mathrm{id}_{\operatorname{im}\varphi}$; en particular, ψ és injectiva i, en conseqüència, $\operatorname{im}\varphi \cong \operatorname{im}\psi \subseteq L$. Si posem $N' := \operatorname{im}\psi$, tenim que $N' \subseteq L$ és un K-submòdul de L, de manera que és lliure i de dimensió finita; i com que $\{u_1, \ldots, u_n\}$ és una K-base de $\operatorname{im}\varphi$, tenim que $\{\varphi(u_1), \ldots, \varphi(u_n)\} = \{v_1, \ldots, v_n\}$ és una K-base de N'. Només cal veure que $L = \ker\varphi \oplus N'$.

Si $x \in \ker\varphi \cap N'$, llavors existeix $y \in \operatorname{im}\varphi$ tal que $x = \psi(y)$ i que $\varphi(x) = 0$; però llavors és $y = \varphi\big(\psi(y)\big) = \varphi(x) = 0$, de manera que $x = \psi(y) = \psi(0) = 0$. Això demostra que $\ker\varphi \cap N' = \{0\}$, D'ltra banda, si $x \in L$, llavors $\varphi(x) \in \operatorname{im}\varphi$ i $\psi\big(\varphi(x)\big) \in \operatorname{im}\psi = N'$; com que $\varphi\Big(x - \psi\big(\varphi(x)\big)\Big) = \varphi(x) - (\varphi \circ \psi \circ \varphi)(x) = 0$, també és $x - \psi\big(\varphi(x)\big) \in \ker\varphi$. Per tant, $x = \Big(x - \psi\big(\varphi(x)\big)\Big) + \psi\big(\varphi(x)\big) \in \ker\varphi + \operatorname{im}\psi$, com volíem veure. □

Proposició 7.5.4. *Siguin K un domini d'ideals principals, M un K-mòdul lliure de dimensió m, $B_M := \{x_1, \ldots, x_m\}$ una K-base de M, $N \subseteq M$ un K-submòdul de M, i $G_N := \{y_1, \ldots, y_t\}$ un conjunt (finit) generador de N. Anomenem R la matriu dels vectors columna $\{y_1, \ldots, y_t\}$ expressats en la base B_M, $K\,d_1 \supseteq K\,d_2 \supseteq \cdots \supseteq K\,d_n$ els factors invariants de N en M (incloent-hi els elements invertibles), D' la matriu quadrada $D' = \operatorname{diag}(d_1, \ldots, d_n) \in \mathbf{M}(n, K)$, i $D \in \mathbf{M}(m, n, K)$ la matriu $\begin{bmatrix} D' & 0_1 \\ 0_2 & 0_3 \end{bmatrix} \in \mathbf{M}(m, t, K)$, formada per les caixes D', i les matrius $0_1 = 0 \in \mathbf{M}(n, t-n, K)$, $0_2 = 0 \in \mathbf{M}(m-n, n, K)$, i $0_3 = 0 \in \mathbf{M}(m-n, t-n, K)$. Notem que és $n \leq m$ i $n \leq t$. Llavors, existeixen matrius invertibles $P \in \mathbf{GL}(m, K)$ i $Q \in \mathbf{GL}(t, K)$ tals que $D = P\,R\,Q$.*

Demostració: Considerem un K-mòdul lliure, L, de dimensió t i base $\{z_1, \ldots, z_t\}$, i sigui $\varphi : L \longrightarrow N \subseteq M$ l'aplicació K-lineal determinada per les assignacions $\varphi(z_j) := y_j$, per a $1 \leq j \leq t$; notem que $\operatorname{im}\varphi = \varphi(L) = N$.

El teorema **7.2.1** ens permet assegurar l'existència d'una K-base $\{e_1, \ldots, e_m\}$ de M i d'elements $d_i \in K$, $1 \leq i \leq n$, tals que d_i divideix d_{i+1}, per a $1 \leq i \leq n-1$, i que $\{d_1\,e_1, \ldots, d_n\,e_n\}$ és una K-base de N (això defineix els elements d_i de l'enunciat, inclosos els invertibles). Siguin $v_i \in L$, $1 \leq i \leq n$, elements tals que $\varphi(v_i) = d_i\,e_i$, i sigui $N' \subseteq L$ el K-submòdul generat per $\{v_1, \ldots, v_n\}$. La proposició anterior, **7.5.2**, ens permet dir que $L = \ker\varphi \oplus N'$ ($\cong \ker\varphi \oplus N$) i, en particular, que $\{v_1, \ldots, v_n\}$ és una K-base de N.

Com que $\ker\varphi \subseteq L$, que és lliure i de dimensió finita sobre un domini d'ideals principals, podem considerar una K-base $\{w_{n+1}, \ldots, w_t\}$ de $\ker\varphi$ (notem que la suma de dimensions de $\ker\varphi$ i de N ha de ser la dimensió, t, de L) i, llavors, $\{v_1, \ldots, v_n, w_{n+1}, \ldots, w_t\}$ és una K-base de L.

Disposem, doncs, de les dades següents:

- una aplicació K-lineal $\varphi : L \longrightarrow M$;
- dues K-bases de M; $\{x_1, \ldots, x_m\}$ i $\{e_1, \ldots, e_m\}$;
- dues K-bases de L; $\{z_1, \ldots, z_t\}$ i $\{v_1, \ldots, v_n, w_{n+1}, \ldots, w_t\}$; i
- la matriu R dels vectors columna $y_j := \varphi(z_j)$, expressats en la K-base $\{x_1, \ldots, x_m\}$; és a dir, la matriu de l'aplicació K-lineal φ en les K-bases $\{z_1, \ldots, z_t\}$ i $\{x_1, \ldots, x_m\}$.

Anomenem $P \in \mathbf{GL}(m, K)$ la matriu de $\{x_1, \ldots, x_m\}$ expressats en la base $\{e_1, \ldots, e_m\}$, i $Q \in \mathbf{GL}(t, K)$ la matriu de $\{z_1, \ldots, z_t\}$ expressats en la base $\{v_1, \ldots, v_n, w_{n+1}, \ldots, w_t\}$. Llavors, $P\,R\,Q$ és la matriu de φ en les bases $\{v_1, \ldots, v_n, w_{n+1}, \ldots, w_t\}$ i $\{e_1, \ldots, e_m\}$. Però resulta que $\varphi(v_i) = d_i\,e_i$, per a $1 \leq i \leq n$, i que $\varphi(w_j) = 0$, per a $n+1 \leq j \leq t$, ja que $w_j \in \ker\varphi$, Per tant, la matriu de φ en aquestes bases és la matriu D, d'on la igualtat que volíem provar, $P\,R\,Q = D$. □

Observació 7.5.5. Si coneixem un K-mòdul donat per una presentació finita, és a dir, un conjunt finit de generadors, $\{x_1, \ldots, x_m\}$, i un conjunt finit de relacions entre aquests generadors, posem $\{y_1, \ldots, y_t\}$, expressats en la base anterior, llavors estem en la situació de la proposició **7.5.4**, ja que coneixem la matriu R. La pregunta és, podem realitzar el càlcul efectiu del rang, dels factors invariants d_i, $1 \leq i \leq n$, i de les bases descrites? I, en cas afirmatiu, com?

Lema 7.5.6. *Siguin K un domini d'ideals principals, $P \in \mathbf{GL}(m, K)$ una matriu invertible, i $R \in \mathbf{M}(m, t, K)$ una matriu qualsevol. Per a $1 \leq n \leq \min(m, t)$, siguin $d_n \in K$*

el màxim comú divisor dels menors d'ordre n de la matriu R, i $e_n \in K$ el màxim comú divisor dels menors d'ordre n de la matriu $P\,R$. Llavors, $K\,d_n = K\,e_n$.

DEMOSTRACIÓ: Posem $S := P\,R$, $P = [p_{i,j}]_{1\leq i,j\leq m}$, $R = [r_{j,k}]_{1\leq j\leq m,\,1\leq k\leq t}$, i $S = [s_{i,k}]_{1\leq i\leq m,\,1\leq k\leq t}$, de manera que, per a $1 \leq i \leq m$, $1 \leq k \leq t$, és $s_{i,k} = \sum_{j=1}^{m} p_{i,j}\,r_{j,k}$.

Calculem el menor d'ordre n de S que correspon a prendre les files $i_1, \ldots, i_n$ i les columnes $k_1, \ldots, k_n$,

$$S_{i_1,\ldots,i_n;k_1,\ldots,j_n} = \begin{vmatrix} s_{i_1,k_1} & s_{i_1,k_2} & \cdots & s_{i_1,k_n} \\ s_{i_2,k_1} & s_{i_2,k_2} & \cdots & s_{i_2,k_n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{i_n,k_1} & s_{i_n,k_2} & \cdots & s_{i_n,k_n} \end{vmatrix} = \sum_{\sigma\in S_n} \varepsilon(\sigma) s_{i_1,k_{\sigma(1)}} \cdots s_{i_n,k_{\sigma(n)}} =$$

$$= \sum_{\sigma\in S_n} \varepsilon(\sigma) \sum_{j_1=1}^{m} p_{i_1,j_1} r_{j_1,k_{\sigma(1)}} \cdots \sum_{j_n=1}^{m} p_{i_n,j_n} r_{j_n,k_{\sigma(n)}} =$$

$$= \sum_{j_1,\ldots,j_n} p_{i_1,j_1} \cdots p_{i_n,j_n} \sum_{\sigma\in S_n} \varepsilon(\sigma) r_{j_1,k_{\sigma(1)}} \cdots r_{j_n,k_{\sigma(n)}} =$$

$$= \sum_{j_1,\ldots,j_n} p_{i_1,j_1} \cdots p_{i_n,j_n}\, R_{j_1,\ldots,j_n;k_1,\ldots,k_n};$$

és a dir, tot menor d'ordre n de S és combinació lineal, de coeficients en K, de (alguns) menors d'ordre n de R. Per tant, tenim que d_n, que és el màxim comú divisor de tots els menors d'ordre n de R, divideix el màxim comú divisor dels menors d'ordre n de R que es fan servir, i aquest divideix el menor considerat d'ordre n de S; per tant, d_n divideix tots els menors d'ordre n de S, de manera que divideix e_n.

Ara, si apliquem això que ja hem demostrat a les matrius S i $R = P^{-1}\,S$, obtenim que e_n divideix d_n. Per tant, e_n i d_n són elements associats de K, com calia demostrar. □

Corol·lari 7.5.7. *Amb les notacions anteriors, sigui R la matriu de relacions. Llavors, per als factors invariants $d_1, \ldots, d_n$, se satisfan les propietats:*

(a) $d_1 = \mathrm{mcd}\{r_{i,j} : 1 \leq i \leq m,\, 1 \leq j \leq t\}$, *on* $R = [r_{i,j}]_{1\leq i\leq m,\,1\leq j\leq t}$;

(b) $d_1 \cdots d_k = \mathrm{mcd}\{$*menors d'ordre k de R*$\}$, *per a* $1 \leq k \leq n$; *i*

(c) $0 = \mathrm{mcd}\{$*menors d'ordre k de R*$\}$, *si* $n < k \leq \min(m, t)$.

DEMOSTRACIÓ: Exercici. □

Observació 7.5.8. Notem que això soluciona el càlcul de la matriu D. També podem calcular les matrius P i Q de manera explícita. Tot i que el procediment següent no és òptim, sí que és molt entenedor.

Sigui $R = [r_{i,j}]_{1\leq i\leq m,1\leq j\leq t} \in \mathbf{M}(m, t, K)$, $r_{i,j} \in K$, la matriu de relacions. A fi de fer més senzilla l'exposició, notem que podem afegir, si convé, columnes de zeros a la matriu R i, d'aquesta manera, podem suposar que $t \geq m$.

• D'altra banda, si la matriu R és la matriu 0, llavors no hi ha relacions no trivials i el mòdul en qüestió és lliure de dimensió m, amb base $\{x_1, \ldots, x_m\}$.

• Suposem, doncs, que és $R \neq 0$: Si multipliquem a esquerra i dreta per matrius invertibles elementals (que podem triar de determinant 1), podem dur a la posició $(1,1)$ un element no nul; així, podem suposar que $r_{1,1} \neq 0$.

• Posem, momentàniament, $d := \mathrm{mcd}(r_{1,1}, r_{1,2}) \neq 0$.

• Calculem $\lambda_1, \lambda_2 \in K$ tals que $d = \lambda_1 r_{1,1} + \lambda_2 r_{1,2}$, i escrivim $r_{1,1} = d\, r'_{1,1}$, $r_{1,2} = d\, r'_{1,2}$, amb $r'_{1,1}$, $r'_{1,2} \in K$. Llavors, tenim que $1 = \lambda_1 r'_{1,1} + \lambda_2 r'_{1,2}$, i $\mathrm{mcd}(\lambda_1, \lambda_2) = 1$. A més a més,

$$\begin{bmatrix} \lambda_1 & -r'_{1,2} \\ \lambda_2 & r'_{1,1} \end{bmatrix} \in \mathbf{SL}(2,K), \qquad \begin{bmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \end{bmatrix} \begin{bmatrix} \lambda_1 & -r'_{1,2} \\ \lambda_2 & r'_{1,1} \end{bmatrix} = \begin{bmatrix} d & 0 \\ * & * \end{bmatrix}.$$

Notem que si K és euclidià, podem fer aquest càlcul amb l'algoritme d'Euclides. Si només sabem que K és domini d'ideals principals, caldrà calcular d i la igualtat de Bézout a partir de generadors d'ideals i d'expressions d'elements concrets d'ideals en funció de generadors d'aquests. En qualsevol cas, l'existència és garantida.

• La reiteració del procediment anterior, ara per a d i $r_{1,3}$, i després, successivament per a tots els elements de la primera fila, permet obtenir una matriu $Q_1 \in \mathbf{SL}(t,K)$ tal que

$$R\,Q_1 = \begin{bmatrix} d'_1 & 0 & \dots & 0 \\ * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \dots & * \end{bmatrix}, \qquad d'_1 = \mathrm{mcd}(r_{1,1}, \dots, r_{1,t}) \in K.$$

• Si repetim inductivament el procediment per a les altres files, podem obtenir una matriu de la forma

$$R\,Q_1 \cdots Q_m = \begin{bmatrix} d'_1 & 0 & 0 & \dots & 0 & \dots & 0 \\ b_2 & d'_2 & 0 & \dots & 0 & \dots & 0 \\ b_3 & * & d'_3 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \dots & \vdots \\ b_m & * & \dots & * & d'_m & \dots & 0 \end{bmatrix}, \qquad d'_1, \dots, d'_m \in K.$$

• Ara es poden donar dues situacions: o bé d'_1 divideix tots els elements de la primera columna, o bé, contràriament, el màxim comú divisor dels elements de la primera columna és un divisor propi de d'_1. En el primer cas, és fàcil restar a cada fila un múltiple adequat de la primera i obtenir una matriu de la forma

$$P_1\,R\,Q_1 \cdots Q_m = \begin{bmatrix} d'_1 & 0 & 0 & \dots & 0 & \dots & 0 \\ 0 & d'_2 & 0 & \dots & 0 & \dots & 0 \\ 0 & * & d'_3 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \dots & \vdots \\ 0 & * & \dots & * & d'_m & \dots & 0 \end{bmatrix}, \qquad d'_1, \dots, d'_m \in K.$$

• En l'altre cas, posem $d''_1 := \mathrm{mcd}(d'_1, b_2, \dots, b_m)$; tenim que d''_1 és un divisor propi de d'_1, i podem repetir el procediment inicial, però per files en lloc de per columnes, per a obtenir una matriu de la forma

$$P_1\,R\,Q_1 \cdots Q_m = \begin{bmatrix} d''_1 & * & * & \dots & * & \dots & * \\ 0 & d''_2 & * & \dots & * & \dots & * \\ \vdots & \vdots & \ddots & \ddots & \dots & \dots & \vdots \\ 0 & 0 & \dots & d''_m & * & \dots & * \end{bmatrix}, \qquad d''_1, \dots, d''_m \in K.$$

• Com que el nombre de divisors propis (llevat d'associats) de d_1 és finit, en repetir alternadament els passos anteriors, obtindrem una matriu de la forma

$$P'\,R\,Q' = \begin{bmatrix} d_0' & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \dots & * \end{bmatrix}, \qquad d_0' \in K.$$

• Ara, recursivament, obtenim matrius $\overline{P} \in \mathbf{SL}(m,K)$, $\overline{Q} \in \mathbf{SL}(t,K)$ tals que

$$\overline{P}\,R\,\overline{Q} = \begin{bmatrix} \overline{d}_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & \overline{d}_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \dots & \overline{d}_m & \dots & 0 \end{bmatrix}, \qquad \overline{d}_1, \dots, \overline{d}_m \in K.$$

• Cal ajustar, encara, les propietats de divisibilitat. Però això és senzill. Mostrarem com passar d'una matriu $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ a la matriu $\begin{bmatrix} d & 0 \\ 0 & d' \end{bmatrix}$, on $d = \mathrm{mcd}(a,b)$, i $d' = \mathrm{mcm}(a,b) = \dfrac{a\,b}{d}$. Això es pot fer amb la successió de canvis

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \to \begin{bmatrix} a & b \\ 0 & b \end{bmatrix} \to \begin{bmatrix} a & b \\ 0 & b \end{bmatrix} \begin{bmatrix} \lambda & -\dfrac{b}{d} \\ \mu & \dfrac{a}{d} \end{bmatrix} = \begin{bmatrix} d & 0 \\ b\,\mu & \dfrac{a\,b}{d} \end{bmatrix} \to \begin{bmatrix} d & 0 \\ 0 & \dfrac{a\,b}{d} \end{bmatrix},$$

on $d = \lambda\,a + \mu\,b = \mathrm{mcd}(a,b)$, el darrer pas, ja que d divideix $b\,\mu$.

• Per inducció, podem canviar $\overline{d}_1$, per $\mathrm{mcd}(\overline{d}_1, \dots, \overline{d}_m)$.

• I finalment, recursivament, obtenim els factors invariants i les matrius de canvi de base. Notem que podem triar totes aquestes matrius de determinant igual a 1; és a dir, de $\mathbf{SL}(m,K)$ i $\mathbf{SL}(t,K)$, respectivament.

7.6 Grups abelians finitament generats

El teorema de classificació s'aplica al cas de l'anell $\mathbb{Z}$ dels nombres enters. En destaquem els resultats i, a continuació, presentem un exemple explícit.

Teorema 7.6.1. *Sigui G un grup abelià finitament generat. Existeix un nombre enter $r \geq 0$, i existeixen nombres naturals $d_1, \dots, d_s > 1$ tals que $G \cong \mathbb{Z}^r \oplus \dfrac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \dfrac{\mathbb{Z}}{d_s\mathbb{Z}}$ i que d_i divideix d_{i+1}, per a $1 \leq i \leq s-1$.* □

En tenir en compte les p-torsions per als diferents nombres primes p, podem enunciar el teorema de classificació en la forma equivalent següent.

Teorema 7.6.2. *Siguin G un grup abelià finitament generat i $\mathbb{P}$ el conjunt dels nombres naturals primers. Existeixen un nombre enter $r \geq 0$, un subconjunt finit $F \subseteq \mathbb{P}$, i, per a cada element $p \in F$, una successió finita de nombres enters $1 \leq e_{p,1} \leq \cdots \leq e_{p,r_p}$, tals que G és isomorf al grup abelià additiu*

$$\mathbb{Z}^r \oplus \bigoplus_{p \in F} \bigoplus_{j=1}^{r_p} \frac{\mathbb{Z}}{\mathbb{Z}/p^{e_{p,j}}\mathbb{Z}}.$$ □

Exemple 7.6.3. Es tracta de determinar el rang i els factors invariants d'un grup abelià donat per la presentació $G := \langle a, b, c; u := 3a + 9b + 9c, v := 9a - 3b + 9c\rangle$.

Posem $R := \begin{bmatrix} 3 & 9 \\ 9 & -3 \\ 9 & 9 \end{bmatrix}$, la matriu de les relacions. Si només volem esbrinar el tipus de grup abelià, és suficient calcular els màxims comuns divisors dels menors d'ordres 1 i 2 de la matriu R: el càlcul proporciona 3 i 18; per tant, els factors invariants són 3, i $\frac{18}{3} = 6$, als quals cal afegir un zero, perquè hi ha tres generadors lliures. Això ens diu que el grup abelià G és isomorf a $\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Oblidem-nos d'això i fem el càlcul, també, de les noves bases. Tenim que

$$R \cdot \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 9 & -30 \\ 9 & -18 \end{bmatrix}.$$

Ara, 3 divideix tots els elements de la primera columna; per tant,

$$\begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \cdot R \cdot \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & -30 \\ 0 & -18 \end{bmatrix}.$$

Ara, $\mathrm{mcd}(-30, -18) = 6 = (-30) \cdot 1 + (-18) \cdot (-2)$; per tant,

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \cdot R \cdot \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 6 \\ 0 & -18 \end{bmatrix}.$$

I, com que 6 divideix -18:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \cdot R \cdot \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 6 \\ 0 & 0 \end{bmatrix}.$$

Això ens diu que el grup abelia G és isomorf al grup $\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

A més a més, el càlcul dels productes de matrius ens diu que, per a les matrius

$$P := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & -2 \\ 6 & 3 & -5 \end{bmatrix}, \qquad Q := \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix},$$

és $P \cdot R \cdot Q = D := \begin{bmatrix} 3 & 0 \\ 0 & 6 \\ 0 & 0 \end{bmatrix}$; així, per a la nova base $\{e_1, e_2, e_3\}$ és $a = e_1 + 3e_2 + 6e_3$, $b = e_2 + 3e_3$, $c = -2e_2 - 5e_3$; i es té que les relacions s'han convertit en $3e_1 = u$, i $6e_2 = -3u + v$.

7.7 Endomorfismes dels espais vectorials de dimensió finita

En aquesta secció, es tracta de recuperar la forma canònica dels endomorfismes dels espais vectorials de dimensió finita. Ens posarem, doncs, en la situació que tenim un cos K, un K-espai vectorial E de dimensió finita, $n := \dim_K E$, i un K-endomorfisme $\varphi : E \longrightarrow E$.

7.7.1 (El polinomi mínim)**.** Considerem l'anell de polinomis $K[X]$, i l'únic morfisme de K-àlgebres $K[X] \longrightarrow K[\varphi] \subseteq \mathrm{End}_K(E)$ tal que $X \mapsto \varphi$ (és a dir, el morfisme d'avaluació en φ).

Notem que $\dim_K \mathrm{End}_K(E)$ és finita (de fet, és n^2), mentre que $\dim_K K[X]$ no ho és; per tant, el morfisme lineal té nucli no nul. A més a més, com que és un morfisme de K-àlgebres, el nucli és un ideal no nul de $K[X]$; i, com que $K[X]$ és un domini d'ideals principals, existeix un únic polinomi mònic, $m_\varphi(X) \in K[X]$ tal que el nucli és l'ideal $m_\varphi(X)\,K[X]$. Aquest polinomi és, doncs, el polinomi mònic de grau mínim que anul·la l'endomorfisme φ; s'anomena el polinomi mínim de φ. Notem, també, que la imatge del morfisme d'avaluació en φ és la K-subàlgebra (commutativa) $K[\varphi] \cong \dfrac{K[X]}{m_\varphi(X)\,K[X]}$.

7.7.2 (Estructura de $K[X]$-mòdul de E)**.** Podem considerar l'acció de $K[X]$ en el grup abelià additiu E donada per $f(X)\,v := f(\varphi)(v)$, per a tot $f(X) \in K[X]$ i tot $v \in E$ (notem que $f(\varphi)$ és la imatge de $f(X)$ pel morfisme d'avaluació en φ). És un exercici immediat comprovar que aquesta acció determina en E una estructura de $K[X]$-mòdul en E, estructura que estén l'estructura de K-espai vectorial de E. A més a més, l'anul·lador del $K[X]$-mòdul E és exactament l'ideal $m_\varphi(X)\,K[X]$, de manera que, si volem, podem considerar E com un $K[\varphi]$-mòdul. D'altra banda, els $K[X]$-submòduls de E són, exactament, els K-subespais vectorials de E que són invariants per φ. Notem, també, que E és finitament generat com a $K[X]$-mòdul (perquè ho és com a K-mòdul), i de torsió (és anul·lat per $m_\varphi(X)$). En particular, podem considerar la seva estructura com a $K[X]$-mòdul de torsió. Considerem la descomposició del polinomi mínim $m_\varphi(X)$ com a producte

$$m_\varphi(X) = \prod_{i=1}^{s} p_i(X)^{v_i}, \qquad v_i \geq 1, \quad 1 \leq i \leq s,$$

amb els polinomis $p_i(X) \in K[X]$, $1 \leq i \leq s$, mònics, irreductibles, i diferents dos a dos. Llavors, existeixen nombres enters $1 \leq e_{i,1} \leq e_{i,2} \leq \cdots \leq e_{i,r_i} = v_i$ de manera que

$$E \cong \bigoplus_{i=1}^{s} \left(\bigoplus_{j=1}^{r_i} \frac{K[X]}{p_i(X)^{e_{i,j}}\,K[X]} \right).$$

Notem que això no és res més que dir que $E = T(E) = \bigoplus_{i=1}^{s} T_{p_i(X)}(E)$ i que $T_{p_i(X)}(E) \cong \bigoplus_{j=1}^{r_i} \dfrac{K[X]}{p_i(X)^{e_{i,j}}\,K[X]}$.

7.7.3 (La forma canònica)**.** Notem que els $K[X]$-mòduls $\dfrac{K[X]}{p_i(X)^{e_{i,j}}\,K[X]}$ són monògens i generats per la classe de l'element 1. I, com a K-espais vectorials, admeten com a K-base el conjunt de classes dels polinomis de la successió

$$\begin{array}{llll}
1, & X, & \ldots, & X^{m_i-1} \\
p_i(X), & X\,p_i(X), & \ldots, & X^{m_i-1}\,p_i(X), \\
p_i^2(X), & X\,p_i^2(X), & \ldots, & X^{m_i-1}\,p_i^2(X), \\
\ldots & \ldots & \ldots & \ldots \\
p_i^{e_{i,j}-1}(X), & X\,p_i^{e_{i,j}-1}(X), & \ldots, & X^{m_i-1}\,p_i^{e_{i,j}-1}(X),
\end{array}$$

on $m_i := \mathrm{gr}\big(p_i(X)\big)$ és el grau del polinomi irreductible $p_i(X)$. Per tant, això diu que existeix un vector $w \in E$ tal que

$$\begin{array}{llll} w, & \varphi(w), & \dots, & \varphi^{m_i-1}(w) \\ p_i(\varphi)(w), & \varphi\, p_i(\varphi)(w), & \dots, & \varphi^{m_i-1}\, p_i(\varphi)(w), \\ p_i^2(\varphi)(w), & \varphi\, p_i^2(\varphi)(w), & \dots, & \varphi^{m_i-1}\, p_i^2(\varphi)(w), \\ \dots & \dots & \dots & \dots \\ p_i^{e_{i,j}-1}(\varphi)(w), & \varphi\, p_i^{e_{i,j}-1}(\varphi)(w), & \dots, & \varphi^{m_i-1}\, p_i^{e_{i,j}-1}(\varphi)(w) \end{array}$$

és una K-base del subespai invariant corresponent. La matriu de (la restricció de) φ en aquesta base és de la forma

$$A_{i,e_{i,j}} = \begin{bmatrix} B_i & 0 & 0 & \cdots & 0 & 0 \\ U_i & B_i & 0 & \cdots & 0 & 0 \\ 0 & U_i & B_i & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & B_i & 0 \\ 0 & 0 & 0 & \cdots & U_i & B_i \end{bmatrix} \in \mathbf{M}(e_{i,j}\, m_i, e_{i,j}\, m_i, K),$$

on les matrius B_i i U_i són de la forma

$$B_i = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_{i,0} \\ 1 & 0 & 0 & \cdots & 0 & -a_{i,1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{i,2} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_{i,m_i-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{i,m_i-1} \end{bmatrix}, \quad U_i = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{bmatrix} \in \mathbf{M}(m_i, m_i, K),$$

de manera que $p_i(X) = a_{i,0} + a_{i,1}\, x + \cdots + a_{i,m_i-1}\, x^{m_i-1} + x^{m_i} \in K[x]$ i les matrius U_i només apareixen si $e_{i,j} > 1$.

Finalment, per reunió de K-bases d'aquests subespais invariants, s'obté una K-base de E de manera que la matriu de φ és formada per caixes com aquestes $A_{i,e_{i,j}}$ a la diagonal; notem que hi ha una caixa per a cada parella (i,j), $1 \le i \le s$, i $1 \le j \le r_i$.

7.7.4 (Nombre de caixes de cada tipus)**.** Observem que per a cada factor irreductible $p_i(X)$ del polinomi mínim $m_\varphi(X)$, l'anell quocient $\dfrac{K[X]}{p_i(X)\, K[X]}$ és un cos i, per a tot nombre enter $k \ge 1$, el $K[X]$-mòdul quocient $\dfrac{p_i^{k-1}(X)\, E}{p_i^k(X)\, E}$ és un $\dfrac{K[X]}{p_i(X)\, K[X]}$-espai vectorial de dimensió finita. D'acord amb la demostració de la unicitat de la descomposició de la torsió, la quantitat, $n_{i,k}$ de mòduls monògens isomorfs a $\dfrac{K[X]}{p_i(X)^k\, K[X]}$, per a $1 \le k \le v_i$, és donada per la diferència entre les dimensions de $\dfrac{p_i^{k-1}(X)\, E}{p_i^k(X)\, E}$ i $\dfrac{p_i^k(X)\, E}{p_i^{k+1}(X)\, E}$ com a $\dfrac{K[X]}{p_i(X)\, K[X]}$-espai vectorial.

Ara, notem que $\dfrac{K[X]}{p_i(X)\, K[X]}$ és un K-espai vectorial de dimensió igual al grau, m_i, del polinomi irreductible $p_i(X)$, Això fa que la dimensió del quocient $\dfrac{p_i^{k-1}(X)\, E}{p_i^k(X)\, E}$, però

considerat com a K-espai vectorial, siguin el producte per m_i de la dimensió com a $\dfrac{K[X]}{p_i(X)\,K[X]}$-espai vectorial. Per tant, podem calcular els nombres $n_{i,k}$ en dividir per m_i la diferència de les dimensions, com a K-espais vectorials, de $\dfrac{p_i^{k-1}(X)\,E}{p_i^k(X)\,E}$ i $\dfrac{p_i^k(X)\,E}{p_i^{k+1}(X)\,E}$.

Finalment, notem que $p_i^k(X)\,E$ és la imatge de l'endomorfisme $p_i^k(\varphi)$; per tant, obtenim la fórmula

$$n_{i,k} = \frac{\operatorname{rang}\left(p_i^{k-1}(\varphi)\right) + \operatorname{rang}\left(p_i^{k+1}(\varphi)\right) - 2\operatorname{rang}\left(p_i^k(\varphi)\right)}{m_i}.$$

I, si tenim en compte que per a tot endomorfisme g de E és $n = \operatorname{rang}(g) + \dim_K \ker g$, recuperem la fórmula habitual,

$$n_{i,k} = \frac{2\dim_K \ker\left(p_i^k(\varphi)\right) - \dim_K \ker\left(p_i^{k-1}(\varphi)\right) - \dim_K \ker\left(p_i^{k+1}(\varphi)\right)}{m_i},$$

per als nombres de caixes de cada tipus associades a cada factor irreductible $p_i(X)$ del polinomi mínim de φ.

Apèndix A

El lema de Zorn

Els axiomes usuals de la teoria de conjunts, els axiomes de Zermelo-Fraenkel, no són suficients per a explicar totes les propietats interessants d'algunes teories matemàtiques. Cal afegir, doncs, altres axiomes, i un dels més habituals és l'axioma de l'elecció. En aquest apèndix en donem l'enunciat, en comentem algunes equivalències (sense demostració) i n'establim algunes conseqüències. Un desenvolupament més complet que inclou demostracions dels resultats que aquí no es demostren es pot consultar en el llibre [Halmos 1960].

A.1 L'axioma de l'elecció

L'axioma de l'elecció predica una propietat que sembla tan evident que, molt sovint, el seu ús podria passar desapercebut. Una de les maneres equivalents de formular-lo és la següent.

A.1.1. Axioma de l'elecció. El producte cartesià d'una família no buida de conjunts no buits és un conjunt no buit.

Formulat d'aquesta manera, sembla que l'axioma de l'elecció es podria acceptar sense discussió. Estem segurs que no l'hem usat implícitament alguna vegada? Anem a estudiar un mica més de prop aquesta formulació.

Definició A.1.2. Sigui $\{A_i\}_{i\in I}$ una família no buida de conjunts no buits. Una funció d'elecció per a la família $\{A_i\}_{i\in I}$ és una aplicació $f : I \longrightarrow \bigcup_{i\in I} A_i$ tal que per a tot $i \in I$ és $f(i) \in A_i$.

A.1.3. Notem, doncs, que el producte cartesià de la família de conjunts $\{A_i\}_{i\in I}$ és exactament el conjunt de les funcions d'elecció per a la família. I dir que el producte cartesià és no buit és dir que existeix alguna funció d'elecció.

Observació A.1.4. Suposem que en un conjunt no buit, C, hi ha definida una relació d'equivalència, R. Llavors, podem considerar el conjunt quocient, C/R, que és el subconjunt del conjunt $\mathcal{P}(C)$, de parts de C, format per les classes d'equivalència. Fins aquí, no hi ha cap necessitat de l'axioma de l'elecció, perquè el conjunt quocient es pot definir explícitament. Per exemple, podem fer-ho en la forma següent:

$$C/R := \{A \in \mathcal{P}(C) : A \neq \varnothing \text{ i per a tot } x, y \in A \text{ és } xRy\}.$$

Ara bé, podem parlar d'un conjunt de representants de les classes d'equivalència?

Notem que, per definició de C/R, tenim que $C = \bigcup_{A \in C/R} A$, de manera que tot conjunt de representants de les classes d'equivalència és la imatge d'una funció d'elecció per a la família $\{A\}_{A \in C/R}$.

A.2 El teorema de Zermelo

En contrapunt a l'axioma de l'elecció, que sembla acceptable de manera evident, l'enunciat següent ho sembla molt menys; de fet, intuïtivament pot semblar no acceptable.

A.2.1. Teorema de Zermelo. Sigui C un conjunt no buit qualsevol. Existeix una relació de bon ordre en C.

Anem a aclarir els termes de la formulació de l'enunciat anterior.

Definició A.2.2. Donat un conjunt qualsevol, C, una relació d'ordre $\leq$ en C és una relació reflexiva, transitiva i antisimètrica; un conjunt C on hi ha un ordre s'anomena un conjunt ordenat. Es diu que un ordre és un bon ordre si tot subconjunt no buit de C té un primer element; és a dir, si per a tot subconjunt $D \subseteq C$, $D \neq \varnothing$, existeix un element $a \in D$ tal que $a \leq b$, per a tot $b \in D$. També es diu que C és un conjunt ben ordenat. Notem que un conjunt ben ordenat és automàticament totalment ordenat; és a dir, l'ordre de C és total; això vol dir que per a tot $a, b \in C$ és $a \leq b$ o bé $b \leq a$.

A.2.3. A primer cop d'ull, la formulació del teorema de Zermelo també pot semblar evident, perquè podem pensar que posem els elements del conjunt l'un darrere l'altre. Això és clar si el conjunt és finit o bé numerable, perquè el podem ben ordenar a partir d'una bijecció amb el conjunt dels nombres naturals, l'ordre del qual és un bon ordre.

Però, com es pot fer això si un conjunt és infinit no numerable? Donat un conjunt infinit no numerable C, sigui $\leq$ un bon ordre en C. Siguin $a_1 \in C$ el primer element de $C_1 := C$ i $C_2 := C - \{a_1\}$. A continuació, prenem a_2 el primer element de C_2 i sigui $C_3 := C_2 - \{a_2\}$. I així, successivament. Podríem procedir d'aquesta manera i formar una successió (numerable) d'elements de C. Ara bé, què succeeix amb els elements que "continuen" després de la successió? Com els podem veure ordenats? Quin és el primer element "després" de la successió? Ja no sembla tan clar.

Observació A.2.4. Les preguntes anteriors es poden contestar de manera satisfactòria amb la teoria dels ordinals i dels cardinals, i l'ús de l'axioma de l'elecció! No és el nostre objectiu provar, en aquest curs, l'equivalència de l'axioma de l'elecció i el teorema de Zermelo.

A.3 El lema de Zorn

Tampoc no és objectiu del curs provar l'equivalència de l'axioma de l'elecció ni del teorema de Zermelo amb el lema de Zorn. De fet, aquesta serà la formulació equivalent de l'axioma de l'elecció que més s'utilitza en el curs. Comencem amb algunes definicions prèvies.

Definició A.3.1. Sigui C un conjunt ordenat per una relació d'ordre $\leq$. Es diu que l'ordre de C és inductiu si tot subconjunt totalment ordenat $D \subseteq C$ té una fita superior (en C); és a dir, si per a tot subconjunt totalment ordenat $D \subseteq C$ existeix un element $c \in C$ tal que $a \leq c$, per a tot $a \in D$.

Definició A.3.2. Sigui C un conjunt ordenat per una relació d'ordre $\leq$. Un element $a \in C$ s'anomena un element maximal per a l'ordre $\leq$ si per a tot $b \in C$ tal que $a \leq b$ és $a = b$; és a dir, si no existeix cap element $b \in C$ tal que $b > a$. Un element $a \in C$ s'anomena un màxim per a l'ordre $\leq$ si per a tot $b \in C$ és $b \leq a$.

Observacions A.3.3. • En els conjunts ordenats $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ (amb els ordres usuals) no hi ha elements maximals.

• Òbviament, tot element màxim és maximal.

• D'altra banda, si C és un conjunt amb més d'un element, podem considerar el conjunt $\mathcal{C}$ format per tots els subconjunts $A \subseteq C$, tals que $A \neq \varnothing$ i $A \neq C$ (o sigui, $\mathcal{C} = \mathcal{P}(C) - \{\varnothing, C\}$). I podem definir un ordre en $\mathcal{C}$ per $A \leq B$ si, i només si, $A \subseteq B$. Llavors, els elements maximals de $\mathcal{C}$ són els complementaris dels subconjunts de C formats per un sol element. Però en $\mathcal{C}$ no hi ha màxim.

La formulació que es fa servir més habitualment del lema de Zorn és la següent.

A.3.4. Lema de Zorn. Sigui C un conjunt ordenat per un ordre $\leq$. Si l'ordre de C és inductiu, C conté elements maximals.

A.3.5. Conseqüències importants del lema de Zorn (moltes d'elles, de fet, són enunciats equivalents al lema de Zorn) són, entre d'altres, les següents.

• (Teorema de Tychonov) Sigui $\{X_i\}_{i \in I}$ una família no buida d'espais topològics compactes. Llavors, l'espai topològic producte és compacte (i no buit).

• Tot espai vectorial té una base.

• Tot anell commutatiu té un ideal maximal.

• Tot anell té un ideal maximal per l'esquerra, un ideal maximal per la dreta, i un ideal maximal.

• Tot cos és subcòs d'un cos algebraicament tancat.

• Tot cos admet una clausura algebraica; és a dir, tot cos k és subcòs d'un cos algebraicament tancat k^a tal que l'extensió $k^a|k$ és algebraica.

A fi de veure com se sol aplicar el lema de Zorn, demostrarem un parell dels resultats anteriors.

Teorema A.3.6. *Sigui K un cos. Tot K-espai vectorial admet una base. De fet, encara més, suposem que E és un K-espai vectorial i que $S \subseteq E$ és qualsevol subconjunt linealment independent. Llavors, existeix una base B de E que conté S.*

Observem que aquest resultat es pot llegir en la forma "tot conjunt linealment independent d'un espai vectorial es pot completar a una base".

Demostració: Siguin K un cos qualsevol, E un K-espai vectorial no nul, i $S \subseteq E$ un subconjunt linealment independent de E. Considerem el conjunt $\mathcal{C}$ format per tots els

subconjunts de E que són K-linealment independents i contenen S, i, en $\mathcal{C}$, la relació d'ordre donada per la inclusió de subconjunts; és a dir, donats dos subconjunts $A, B \subseteq E$ que siguin K-linealment independents i continguin S, direm que $A \leq B$ si, i només si, $A \subseteq B$. Notem que $S \in \mathcal{C}$, de manera que $\mathcal{C}$ és no buit.

Provem que l'ordre de $\mathcal{C}$ és inductiu. Sigui, doncs, $\mathcal{D} \subseteq \mathcal{C}$ un subconjunt no buit de $\mathcal{C}$ i totalment ordenat. Posem T la reunió de tots els elements de $\mathcal{D}$ (que són subconjunts de E, K-linealment independents, i que contenen S). Clarament, T conté com a subconjunts tots els elements de $\mathcal{D}$, de manera que, si T és K-linealment independent i conté S, llavors és $T \in \mathcal{C}$ i, com a conseqüència, $\mathcal{D}$ té una fita superior en $\mathcal{C}$, com cal demostrar. Ara bé, qualsevol combinació lineal no trivial entre elements de T contindria una quantitat finita de vectors de E; aquests vectors estarien, cadascun, en algun element del conjunt $\mathcal{D}$; la finitut de la quantitat d'aquests vectors i el fet que $\mathcal{D}$ és totalment ordenat ens permeten assegurar que tots ells pertanyerien a un mateix conjunt de $\mathcal{D}$, de manera que $\mathcal{D}$ contindria un conjunt K-linealment dependent, contra la definició de $\mathcal{D}$ com a subconjunt de $\mathcal{C}$. Per tant, T és un conjunt K-linalment independent que conté S i l'ordre de $\mathcal{C}$ és inductiu.

Apliquem, ara, el lema de Zorn. Obtenim que $\mathcal{C}$ té un element maximal. Sigui $B \in \mathcal{C}$ un element maximal de $\mathcal{C}$. Si veiem que B és un conjunt de generadors de E com a K-espai vectorial, obtindrem que B és una base de E, de manera que el resultat estarà provat, perquè B conté S. Ara bé, si B no generés E com a K-espai vectorial, existiria un vector $v \in E$ que no seria combinació lineal d'elements de B, de manera que $B' := B \cup \{v\}$ seria un subconjunt K-linealment independent de E; però això contradiria la maximalitat de B en $\mathcal{C}$, ja que seria $B' \in \mathcal{C}$ i $B < B'$. Per tant, B és una base de E i conté S. □

El segon exemple toca més directament el temari del curs. Tot i això, enunciarem i demostrarem un resultat més general. Recordem que un ideal propi per l'esquerra de A és un ideal per l'esquerra de A que sigui diferent de A. I que un ideal per l'esquerra és maximal si és diferent del total i no està inclòs en cap altre ideal propi per l'esquerra.

Teorema A.3.7. *Siguin A un anell, no necessàriament commutatiu, i $\mathfrak{a} \subseteq A$ un ideal propi per l'esquerra de A. Llavors, $\mathfrak{a}$ està inclos en un ideal maximal (propi) per l'esquerra de A.*

Demostració: Sigui $\mathcal{C}$ el subconjunt format per tots els ideals propis per l'esquerra de A que contenen $\mathfrak{a}$. Clarament $\mathfrak{a} \in \mathcal{C}$, de manera que el conjunt $\mathcal{C}$ és no buit. Ordenem $\mathcal{C}$ per inclusió i considerem $\mathcal{D} \subseteq \mathcal{C}$ un subconjunt totalment ordenat. Com que $\mathcal{D}$ és totalment ordenat, $\bigcup_{\mathfrak{b} \in \mathcal{D}} \mathfrak{b}$ és un ideal per l'esquerra de A, i conté $\mathfrak{a}$, i és propi perquè $1 \notin \mathfrak{b}$ per a cap $\mathfrak{b} \in \mathcal{D}$, de manera que $1 \notin \bigcup_{\mathfrak{b} \in \mathcal{D}} \mathfrak{b}$. A més a més, aquesta reunió pertany a $\mathcal{C}$ i és una fita superior per a $\mathcal{D}$, i això demostra que l'ordre de $\mathcal{C}$ és inductiu.

Apliquem el lema de Zorn; trobem que existeix un element maximal $\mathfrak{m} \in \mathcal{C}$. Però, llavors, $\mathfrak{m}$ és un ideal propi per l'esquerra de A; i és maximal per l'esquerra i conté $\mathfrak{a}$. □

Referències

[Artin 1991] Artin, Michael: *Algebra*. Prentice Hall, New Jersey, USA, 1991. ISBN: 0-13-004763-5.

[Atiyah-Macdonald 1973] Atiyah, Michael Francis; Macdonald, Ian Grant: *Introducción al álgebra conmutativa*. Ed. Reverté, Barcelona, 1973. Traducció: Griselda Pascual Xufré. ISBN: 84-291-5008-0. Versió original, *Introduction to commutative Algebra*. Addison-Wesley Pub. Comp., Massachussets, USA, 1969.

[Barnes-Mack 1978] Barnes, Donald W.; Mack, John Michael: *Una Introducción algebraica a la lógica matemática*. EUNIBAR, Barcelona, 1978. Traducció: Sebastià Xambó Descamps. ISBN: 84-85257-13-8. Versió original: *An Algebraic Introduction to Mathematical Logic*. Springer-Verlag, New York, USA, 1975.

[Bourbaki 1970] Bourbaki, Nicolas: *Éléments de Mathématique. Algèbre*, chap. 1 à 3. Hermann, París, 1970.

[Godement 1978] Godement, Roger: *Álgebra*, tercera reimpressió de la primera edició. Editorial Tecnos, Madrid, 1978. Traducció: Mario Meléndez Rolla. ISBN: 84-309-0526-X. Versió original: *Cours d'algèbre*, Hermann, Paris, 1964.

[Halmos 1960] Halmos, Paul Richard: *Naive Set Theory*. UTM, Springer-Verlag. New York, USA, 1974. ISBN: 0-387-90092-6. Versió original publicada per Litton Educational Publishing, Inc., 1960.

[Jacobson 1974] Jacobson, Nathan: *Basic Algebra, I*. W. H. Freeman and Company, San Francisco, California, USA, 1974. ISBN: 0-7167-0453-6.

[Jacobson 1980] Jacobson, Nathan: *Basic Algebra, II*. W. H. Freeman and Company, San Francisco, California, USA, 1980. ISBN: 0-7167-1079-X.

[Kelley 1975] Kelley, John Leroy: *Topología general*. EUDEBA, Buenos Aires, segona edició, 1975. Traducció: Óscar Alberto Varsavsky. Versió original, *General Topology*. D. van Nostrand, New York, USA, 1955.

[Lang 1971] Lang, Serge: *Álgebra*. Aguilar, Madrid, 1971. Traducció: Milagros Ancochea. ISBN: 84-03-20216-4. Versió original, *Algebra* (second printing). Addison Wesley Publishing Company, Reading, Massachussets, USA, 1965.

[Lang 1984] Lang, Serge: *Algebra*, Second Edition. Addison Wesley Publishing Company, Reading, Massachussets, USA, 1984. ISBN: 0-201-05487-6.

[Malitz 1979] Malitz, Jerome Irving: *Introduction to Mathematical Logic*. Springer Verlag, UTM, New York, USA, 1979 . ISBN: 0-387-90346-1.

[Mendelson 1979] Mendelson, Elliott: *Introduction to Mathematical Logic*, second edition. Van Nostrand, New York, USA, 1979. ISBN: 0-442-25307-9.

[Monk 1976] Monk, James Donald: *Mathematical Logic*. Springer Verlag, GTM, **37**, New York, USA, 1976. ISBN: 0-387-90170-1.

[Pla 1993] Pla Carrera, Josep: *Axiomes alternatius de la teoria de conjunts i llur influència en matemàtiques*. IEC-SC, Arxius de la secció de ciències, **107**, Barcelona, 1993. ISBN: 84-7283-256-2.

[Pla 2006] Pla Carrera, Josep: *Introducció a la Metodologia de la Matemàtica*. Publicacions i Edicions de la Universitat de Barcelona, col·lecció Universitat, **20**, Barcelona, 2006. ISBN: 84-4753-065-5.

[Queysanne 1971] Queysanne, Michel: *Àlgebra básica*. Ed. Vicens Vives, Barcelona, 1971. Traducció: José Luis Viviente. ISBN: 84-316-1360-2. Versió original, *Algèbre*. Librairie Armand Colin, París, 1964.

[Samuel 1972] Samuel, Pierre: *Teoría algebraica de números*. Ed. Omega, Col. Métodos, Barcelona, 1972. Traducció: Manuel Udina Abelló, María José Castello Esnal. Versió original, *Théorie algébrique des nombres*. Hermann, París, 1967.

[Travesa 1992] Travesa Grau, Artur: *Teoria de Nombres*. Text accessible en format pdf a la pàgina `https://travesa.cat/notes.html`. Barcelona, 1992.

[Travesa 1998] Travesa Grau, Artur: *Aritmètica*. Edicions de la Universitat de Barcelona, col·lecció UB, **25**, Barcelona, 1998. ISBN: 84-8338-031-5.

[Travesa 2020] Travesa Grau, Artur: *Equacions algebraiques*. Text accessible en format pdf a la pàgina `https://travesa.cat/notes.html`. Barcelona, 2020.

Índex de diagrames

Índex terminològic