Universitat de Barcelona

Facultat de Matemàtiques i Enginyeria Informàtica

Apunts

Grau en Matemàtiques

Curs 2022-2023 | Cinquè Semestre

Estructures Algebraiques (EA)

Autor:
Mario Vilar

Professor/a:
Dra. Teresa Crespo

Presentació de l'assignatura

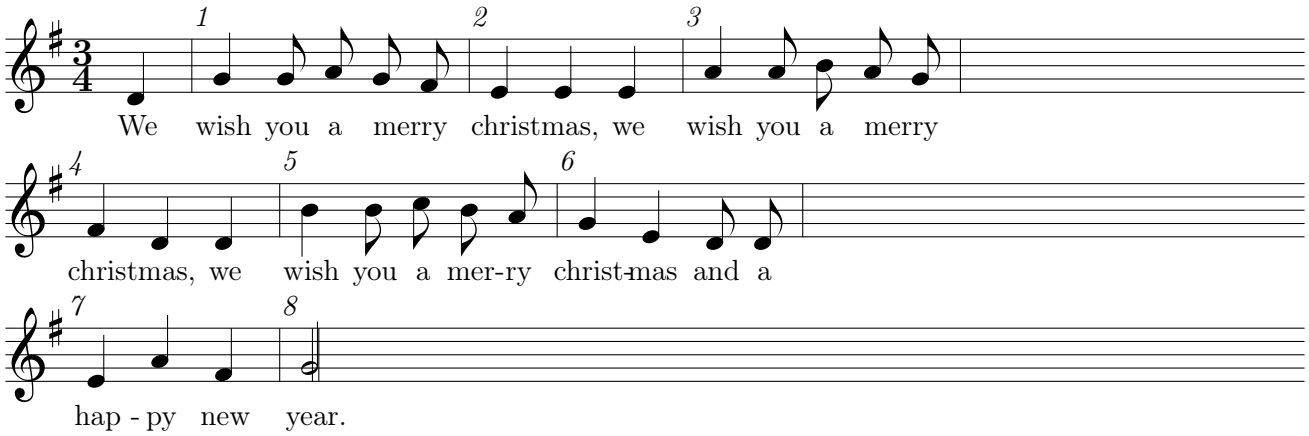
Els objectius d'aquesta assignatura són de dos tipus: assolir formació en àlgebra bàsica i assolir coneixements i destreses per a manipular objectes abstractes. Les estructures algebraiques són interessants perquè permeten abstreure propietats importants i ens ajuden a saber manipular exemples que poden ser de natura molt diferent.

Universitat de Barcelona

Classificació AMS (2020): 00-01, 08-01, 08Axx, 20-01, 97H40.

Índex

Introducció



Primer de tot, trobareu que hi ha un índex, on hi distingim els diferents apartats ordenats seguint el meu propi criteri i, de tant en tant, seguint l'ordre cronològic del curs. Hi ha capítols, seccions, subseccions (i fins i tot subsubseccions). Us faig cinc cèntims de com he organitzat els encapçalaments de cada pàgina:

1. el número de l'últim capítol/secció/subsecció, depèn de la profunditat que hi hagi definida en aquell moment, figurarà en cada cantonada superior de pàgina parella (per exemple, *1.2*);
2. el nom del capítol es trobarà a la part dreta de la capçalera de les pàgines parelles (per exemple, «Divisibilitat i nombres primers»);
3. el nom de l'última secció/subsecció de la pàgina, a la cantonada dreta superior de les pàgines parelles (per exemple, «Polinomis: algorisme d'Euclides»);
4. el número de l'últim teorema, definició... de la pàgina en qüestió es trobarà a les pàgines senars, a la cantonada superior dreta, destacat en el seu color corresponent (per exemple, **1.2.3**).

A més, hi ha una taula, la taula de contingut, en què es veu fàcilment que s'ha seguit una mena de *sorting-by-color* per poder treballar de manera més eficient amb els diferents tipus d'enunciats matemàtics. D'aquesta manera, si busqueu una definició, un teorema... podreu trobar-los molt ràpidament.

Per últim, m'estalviaré de comentar l'índex terminològic perquè el seu propòsit és clar i, en efecte, paral·lel al de l'organització d'aquest document: poder facilitar-vos al màxim la feina per localitzar qualsevol concepte que desitgeu. Espero que us serveixin d'alguna cosa aquests apunts, els he fet amb tot l'amor del món. Sort!

Teorema de prova. *Aquest és un teorema de prova. Els teoremes, les proposicions, els lemes, els corol·laris, les propietats, les conjectures i els processos tindran aquest format.*

Definició de prova. Aquesta és una definició de prova. Les definicions, els exemples i les notacions tindran aquest format.

Remarca de prova. Aquesta és una remarca de prova. Les remarques tindran aquest format.

Figura 1: Els diferents formats d'enunciats.

Mario Vilar
Sitges, Barcelona
2 de gener de 2023

Taula de continguts

Part

I

Grups

I

Grups

1.1 Definicions

Definició 1.1.1 (Operació interna)**.** Si A és un conjunt no buit, una *operació interna* a A és una aplicació d'$A \times A$ en A. Indiquem la imatge d'(a, b) per aquesta aplicació per $a \circledcirc b$. Tenim:

$$\begin{array}{rccc} \circledcirc : & A \times A & \longrightarrow & A \\ & (a, b) & \longmapsto & f(a, b) = a \circledcirc b \end{array} \tag{1.1.1}$$

A la llarga farem un abús de notació i no posarem aquest signe.

Sigui $\circledcirc$ una operació interna definida en el conjunt A:

1. Diem que $\circledcirc$ és **associativa** si $(a \circledcirc b) \circledcirc c = a \circledcirc (b \circledcirc c)$, per a a, b, c elements d'A, qualssevol.
2. Diem que $\circledcirc$ és **commutativa** si $a \circledcirc b = b \circledcirc a$, per a $a, b \in A$.
3. Diem que $e \in A$ és **element neutre** per $\circledcirc$ si $a \circledcirc e = e \circledcirc a = a$ per a qualsevol element $a \in A$.
4. Si e és element neutre per $\circledcirc$ i a és un element d'A, diem que un element b d'A és **simètric** d'a per $\circledcirc$ si $a \circledcirc b = b \circledcirc a = e$.

Definició 1.1.2 (Suma)**.** Sigui $a \in A$. Definim la suma com una operació interna amb element neutre 0, amb oposat l'element simètric $-a$.

Definició 1.1.3 (Producte)**.** Amb element neutre 1, i diem invers d'a l'element simètric a^{-1}.

Si A és un conjunt dotat d'una operació interna $\circledcirc$ i B és un subconjunt d'A, diem que B és estable per $\circledcirc$ si es compleix

$$a, b \in B \implies a \circledcirc b \in B. \tag{1.1.2}$$

Definició 1.1.4 (Grup)**.** És un conjunt G no buit dotat d'una operació interna associativa, amb element neutre i tal que tot element té simètric. Si, a més, l'operació és commutativa, diem que el grup és *abelià*:

1. per a tots $x, y, z \in G$, $(x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z)$, la propietat associativa;
2. existeix $e \in G$ tal que $e \circledcirc x = x \circledcirc e = x$, per a tot $x \in G$ (e és l'element neutre de G).
3. per a tot $x \in G$, existeix $x' \in G$ tal que $x' \circledcirc x = x \circledcirc x' = e$ (x' és l'element simètric de x);

Definició 1.1.5 (Grup abelià)**.** Diem que G és abelià si l'operació de G és commutativa, és a dir, si $x \circledcirc y = y \circledcirc x$ per a tots $x, y \in G$.

Notació 1.1.6. Si l'operació de G és un producte, es posa 1 l'element neutre, el simètric x' de x es diu invers i s'indica per x^{-1}. Si l'operació és una suma, es posa com a 0 l'element neutre, el simètric x' de x es diu oposat i s'indica per $-x$. Habitualment, una operació denotada com a suma és commutativa (i, per tant, abeliana).

Exemple 1.1.7.

- $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ són grups abelians per la suma;
- $(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},\cdot),(\mathbb{C}\setminus\{0\},\cdot),(\mathbb{Z}/m\mathbb{Z},\cdot),((\mathbb{Z}/m\mathbb{Z})^*,\cdot)$ són grups abelians per la multiplicació;
- Definit $GL(n,\mathbb{R})=\{M\in\mathcal{M}_{n\times n}(\mathbb{R}) \mid \det(M)\neq 0\}$, tenim que $(GL(n,\mathbb{R}),\cdot)$ és un grup per al producte de matrius, no abelià per a tot $n\geq 2$.

Proposició 1.1.8. *L'element neutre d'un grup és únic i l'element simètric d'un element x d'un grup és únic.*

Demostració. En efecte, si $e,e'\in G$ compleixen la propietat de ser neutre, tenim $e=e\circledcirc e'=e'$. Pel que fa a la segona part, en efecte, si $x',x''\in G$ compleixen la propietat de ser simètrics de x, tenim:

$$x''=e\circledcirc x''=(x'\circledcirc x)\circledcirc x''=x'\circledcirc(x\circledcirc x'')=x'\circledcirc e=x'. \tag{1.1.3}$$

■

Propietat 1.1.9. *De la definició de grup es dedueixen fàcilment les propietats següents d'un grup G:*

1. *Llei de simplificació: donats $a,x,y\in G$,*

$$\begin{aligned} ax=ay &\implies x=y\\ xa=ya &\implies x=y \end{aligned} \tag{1.1.4}$$

   En particular, $xx=x\implies x=e$.
2. *Donats $x,y\in G$, $(xy)^{-1}=y^{-1}x^{-1}$.*

Demostració. Ho farem solament per a la primera implicació. La segona es fa de manera totalment anàloga:

$$x=xe=x(zz^{-1})=(xz)z^{-1}=(yz)z^{-1}=y(zz^{-1})=ye=y. \tag{1.1.5}$$

En particular, podem aplicar-ho al cas $xx=x$ i ens surt de manera directa que $x=e$. Pel que fa al segon apartat, ens hem de limitar a comprovar que $y^{-1}x^{-1}$ és, en efecte, l'invers de xy:

$$\begin{aligned} (xy)(y^{-1}x^{-1})=x(yy^{-1})x^{-1}=xex^{-1}=xx^{-1}=e,\\ (y^{-1}x^{-1})(xy)=y^{-1}(x^{-1}x)y=y^{-1}ey=y^{-1}y=e. \end{aligned} \tag{1.1.6}$$

■

Definició 1.1.10 (Subgrup)**.** Un subgrup d'un grup G és un subconjunt no buit H de G tal que:

1. $x, y \in H \implies xy \in H$ (H és tancat respecte de l'operació de G).
2. H és grup amb l'operació de G.

Proposició 1.1.11. *Siguin G un grup i $H \subset G$ un subconjunt no buit. Els tres enunciats següents són equivalents:*

1. *H és subgrup de G.*
2. *H satisfà les següents propietats:*
   1. *$e \in H$,*
   2. *per a tot $x \in H$ es compleix $x^{-1} \in H$,*
   3. *per a tot $x, y \in H$ es compleix $xy \in H$.*
3. *Per a tot $x, y \in H$ es compleix $xy^{-1} \in H$.*

Demostració.

1. ⇒ 2. Aquesta resulta de la unicitat de l'element neutre i l'element simètric. En més detall, si H és un grup, existeix un neutre $e' \in H$. Com H és un subgrup, el neutre de G funciona com a neutre a H, tal que $e \in H$ i, per la unicitat del neutre, $e = e'$. Anàlogament, si H és subgrup, qualsevol $x \in H$ té invers; per la unicitat de l'invers, l'invers x^{-1} de x a G compleix que $x^{-1} \in G$ és l'invers de x a H. Per últim, la segona propietat del segon apartat és directa.

2. ⇒ 3. Per a $x, y \in H$, tenim $y \in H \implies y^{-1} \in H$ per la segona propietat del segon apartat; ara, $x, y^{-1} \in H$ implica que $xy^{-1} \in H$ per la tercera.

3. ⇒ 1. Com H és no buit existeix $x \in H$ i, segons el tercer apartat, $x, x \in H$ implica $xx^{-1} = e \in H$. Aplicant el mateix, per a qualsevol $y \in H$, obtenim $y^{-1} = ey^{-1} \in H$; finalment, per a $x, y \in H$ ens queda en particular que $y^{-1} \in H$ i $xy = x(y^{-1})^{-1} \in H$.

Una operació associativa a G implica una operació associativa a H. ■

Proposició 1.1.12. *Siguin H_1, H_2 subgrups de G. Aleshores, $H_1 \cap H_2$ és un subgrup de G.*

Demostració. Siguin $e \in H_1$ i $e \in H_2$ els respectius elements neutres (iguals per la unicitat de l'element neutre). Aleshores, $e \in H_1 \cap H_2$ i, per tant, aquesta intersecció no és buida. Suposem ara $x, y \in H_1 \cap H_2$:

$$\left.\begin{array}{l} x, y \in H_1 \implies xy^{-1} \in H_1 \\ x, y \in H_2 \implies xy^{-1} \in H_2 \end{array}\right\} \implies xy^{-1} \in H_1 \cap H_2 \tag{1.1.7}$$

Generalitzant aquest raonament, podem agafar H_i, $i \in I$ subgrups de G i tindrem que $\bigcap_{i \in I} H_i$ és subgrup de G. ■

Exemple 1.1.13.

- Sigui G un grup. G és subgrup d'ell mateix, el *subgrup total*.
- Anàlogament, podem considerar el subgrup $\{e\} \in G$, el *subgrup trivial*.
- En aquest sentit, recordem $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Els seus únics subgrups són el trivial i el total.

- Els ideals, $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$, són un subgrup de $(\mathbb{Z}, +)$.
  1. $0 \in m\mathbb{Z} \implies m\mathbb{Z} \neq \emptyset$.
  2. $\forall n_1, n_2 \in m\mathbb{Z}$, tenim que $n_1 - n_2 \in m\mathbb{Z}$. Aleshores:

$$\left.\begin{array}{l} n_1 = m \cdot a_1 \\ n_2 = ma_2 \end{array}\right\} \implies n_1 - n_2 = m(a_1 - a_2) \in m\mathbb{Z}. \tag{1.1.8}$$

Proposició 1.1.14. *Tot subgrup de $(\mathbb{Z}, +)$ és igual a $m\mathbb{Z}$ per a algun enter natural $m \geq 0$.*

Demostració. Sigui H un subgrup de $(\mathbb{Z}, +)$. Si $H = \{0\}$, de manera que tenim el subgrup trivial $H = m\mathbb{Z}$ amb $m = 0$. Si $H \neq \{0\}$ i $H \neq \emptyset$, $\exists n \in H, n \neq 0$. Més concretament, podem afirmar que $-n \in H$ (existència de l'element oposat). Això mateix ens diu que H conté elements estrictament positius. Sigui $m = \min\{n \in H \mid n > 0\} \in H$, volem veure que $H = m\mathbb{Z}$.

$m\mathbb{Z} \subset H$ Pel fet que m és l'enter estrictament positiu més petit contingut a H.

$m\mathbb{Z} \supset H$ Sigui $a \in H$. Podem posar, per la divisió euclidiana, $a = mq + r$, amb $0 \leq r < m$ i $r = a - mq \in H$. Per l'elecció de m, ha de ser $r = 0$ (no pot ser més petit que l'enter estrictament positiu més petit) i, en conseqüència, $a = mq \in m\mathbb{Z}$.

■

1.2 Permutacions

1.2.1 Permutacions i transposicions

Definició 1.2.1 (Permutacions)**.** Una permutació de n elements és una bijecció de $\{1, \ldots, n\}$ en $\{1, \ldots, n\}$, és a dir, $\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$. Per tant, cada enter $i \in \{1, \ldots, n\}$ té una imatge $\sigma(i)$ per σ i tenim $\sigma(i) \neq \sigma(j)$ si $i \neq j$ i tot enter de $\{1, \ldots, n\}$ és $\sigma(i)$ per a un únic i.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \tag{1.2.1}$$

Definició 1.2.2 (Composició de permutacions)**.** Siguin σ, τ dues permutacions de n elements. La composició és la seva composició com a aplicacions: $\sigma \circ \tau$ compleix $(\sigma \circ \tau)(i) = \sigma(\tau(i))$ per a $i \in \{1, 2, \ldots, n\}$. La imatge d'un enter i per $\sigma\tau$ s'obté, doncs, fent la imatge de i per τ i després la imatge de $\tau(i)$ per σ.

Proposició 1.2.3.

1. *Si σ, τ, ρ són permutacions de n elements, es compleix $(\sigma\tau)\rho = \sigma(\tau\rho)$ (associativitat).*
2. *Considerem la permutació identitat Id definida per per $Id(i) = i$, per a tot $i \in \{1, \ldots, n\}$. Si σ és qualsevol permutació de n elements, es compleix $Id\sigma = \sigma Id = \sigma$ (existència d'element neutre).*
3. *Per a tota permutació σ de n elements, existeix una permutació de n elements, que denotem per σ^{-1} i diem inversa de σ que compleix $\sigma\sigma^{-1} = \sigma^{-1}\sigma = Id$ (existència d'element invers).*

Demostració.

1. Per a $i \in \{1, \ldots, n\}$ qualsevol, tenim:
$$\begin{array}{c}((\sigma\tau)\rho)(i) = (\sigma\tau)(\rho(i)) = \sigma(\tau(\rho(i))),\\ (\sigma(\tau\rho))(i) = \sigma(\tau \circ \rho(i)) = \sigma(\tau\rho(i)).\end{array} \tag{1.2.2}$$
2. Per a $i \in \{1, \ldots, n\}$ qualsevol, tenim $Id(\sigma)(i)Id(\sigma(i)) = \sigma(i)$ i $(\sigma Id)(i) = \sigma(Id(i)) = \sigma(i)$.
3. Com cada $i \in \{1, \ldots, n\}$ és igual a $\sigma(j)$ per a exactament un enter j de $\{1, \ldots, n\}$, podem definir σ^{-1} per $\sigma^{-1}(i) = j$ si, i només si, $i = \sigma(j)$ i es compleix clarament que $\sigma\sigma^{-1} = \sigma^{-1}\sigma = Id$.

■

Proposició 1.2.4. *Si σ, τ són permutacions de n elements, es compleix $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.*

Demostració. Fem el producte tant per l'esquerra com per la dreta i arribem el mateix resultat, la identitat.
$$\begin{array}{c}(\sigma\tau)(\tau^{-1}\sigma^{-1}) = \sigma(\tau\tau^{-1})\sigma^{-1} = \sigma Id\sigma^{-1} = \sigma\sigma^{-1} = Id,\\ (\tau^{-1}\sigma^{-1})(\sigma\tau) = Id.\end{array} \tag{1.2.3}$$
És a dir, un és l'invers de l'altre i viceversa. ■

Definició 1.2.5 (Transposició)**.** Una transposició és una permutació que deixa fixos tots els elements de $\{1, \ldots, n\}$ excepte dos, que es corresponen l'un amb l'altre per la transposició. Si aquests dos són i, j, denotem la transposició per (i, j) o (j, i) indistintament. Suposant $i < j$:
$$(i,j) = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix} \tag{1.2.4}$$
Clarament, $(i, j)^2 = Id$. Per tant, l'inversa d'una transposició és ella mateixa.

Lema 1.2.6. *Si $a, b, c \in \{1, 2, \ldots, n\}$ són tots tres diferents, tenim, a S_n, la igualtat $(a, b)(b, c) = (a, c)(a, b)$.*

Demostració. En efecte, tenim $(a, b)(b, c) = (a, b, c)$ i $(a, c)(a, b) = (a, b, c)$. ■

Proposició 1.2.7. *La identitat no és igual al producte d'un nombre senar de transposicions.*

Demostració. **Incorrecta**. Raonem per reducció a l'absurd. Sigui $Id = \tau_1, \ldots, \tau_k$ tal que $\tau_i = (a_i, b_i), a_i < b_i$. Si $a_i = 1$, $(a_i, b_i) = (1, a_i)(1, b_i)(1, a_i)$ (el nombre de transposicions és senar). D'altra banda, $Id = (1, c_1)(1, c_2) \cdots (1, c_\ell)$ amb ℓ de la mateixa paritat que k.
$$\begin{array}{rcl} c_i & \longmapsto & c_i \text{ per } (1, c_j), \quad c_j \neq c_i; \\ c_i & \longmapsto & 1 \text{ per } (1, c_i). \end{array} \tag{1.2.5}$$
En altres paraules, com la transposició $(1, c_i)$ envia c_i a 1 i $(1, c_j)$ envia 1 a c_j, hi ha d'haver al producte (1.2.5) un nombre parell de factors $(1, c_i)$ per tal que la imatge de c_i pel producte sigui, en efecte, c_i. Com el producte de transposicions de (1.2.5) és igual a la identitat, la imatge de c_i ha de ser c_i, per a tot $i = 1, \ldots, \ell$. És a dir, si el nombre de factors $(1, c_i)$ és parell, aleshores el nombre de factors és parell (arribem a contradicció). ■

Demostració. **Corregida**. Volem veure que la identitat no és producte de $2k+1$ transposicions, per a k enter ≥ 0, per inducció sobre k.

1. Per a $k=0$, és clar que Id no és una transposició.
2. Suposem que la identitat no és producte de $2k-1$ transposicions i provem que tampoc no ho és de $2k+1$ transposicions.

Posem $Id = t_1 t_2 \dots t_{2k+1}$, per a t_i transposicions, $1 \leq i \leq 2k+1$, i $t_{2k+1} = (a, x)$. Com el producte de totes les t_i' ha de ser Id, ha d'haver algun factor de la forma (a, y). Per 1.2.6, podem suposar $t_{2k} = (a, y)$. Si fos $x = y$, Id seria producte de $2k-1$ transposicions, que no pot ser per hipòtesi d'inducció. Per tant, $x \neq y$. Ara, y té imatge a pel producte $t_{2k} t_{2k+1}$, de manera que un dels altres factors ha de ser de la forma (a, z). Per 1.2.6 un altre cop, podem suposar $t_{2k-1} = (a, z)$ i, per la hipòtesi d'inducció, ha de ser $z \neq y$ i $z \neq x$. Reiterant aquest raonament arribaríem a què totes les t_i són de la forma (a, v), amb tots els v' diferents i per tant el seu producte no pot donar Id. ■

Corol·lari 1.2.8. *Si $t_1, \dots, t_r, \tau_1, \dots, \tau_s$ són transposicions i $t_1 t_2 \cdots t_r \neq \tau_1 \cdots \tau_s$, aleshores r i s tenen la mateixa paritat.*

Demostració. Definim la signatura d'una permutació σ de S_n com $\varepsilon(\sigma) = 1$ si σ és producte d'un nombre parell de transposicions, i com $\varepsilon(\sigma) = -1$ si σ és producte d'un nombre senar de transposicions. Siguin σ, τ permutacions:

$$\varepsilon(Id) = 1,\ \varepsilon(\sigma^{-1}) = \varepsilon(\sigma). \tag{1.2.6}$$

■

1.2.2 Grups de permutacions i cicles

Definició 1.2.9 (Grup simètric)**.** Posem S_n el conjunt de les permutacions de n elements amb el producte de permutacions. És un grup que es diu *grup simètric*. A S_n tenim $n!$ permutacions.

$$\begin{aligned} S_2 &= \left\{ Id, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}, \\ S_3 &= \left\{ Id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \end{aligned} \tag{1.2.7}$$

Suposem l'i-èsim element de S_3 com S_3^i; observem que $S_3^2 S_3^3 = S_3^5$ i $S_3^3 S_3^2 = S_3^6$; com la operació no commuta, S_3 no és abelià. A S_n, amb $n > 3$, podem considerar dues permutacions que donin la mateixa imatge per a $1, 2, 3$ que t_1 i t_2, respectivament, i enviïn els nombres $4, \dots, n$ a ells mateixos. Com aquestes dues permutacions no commuten entre elles, podem dir que S_n és un grup no abelià per a $n \geq 3$.

Proposició 1.2.10 (Grup alternat)**.** *El conjunt de permutacions parelles de S_n és un subgrup de S_n. Es diu grup alternat i es denota per A_n.*

Demostració. Per 1.2.7, $\varepsilon(Id) = 1$; per tant, $Id \in A_n$. Siguin ara $\sigma, \tau \in A_n$; aleshores, $\sigma\tau \in A_n$. Si $\sigma \in A_n$, $\sigma^{-1} \in A_n$. ■

Definició 1.2.11 (r-cicle)**.** Siguin $k_1, \ldots, k_r$ índexs diferents 2 a 2 de $\{1, \ldots, m\}$. Definim

$$\begin{array}{c} \sigma(k_1) = k_2 \\ \vdots \\ \sigma(k_{r-1}) = k_r \\ \sigma(k_r) = k_1 \end{array} \tag{1.2.8}$$

i $\sigma(i) = i$ per a $i \in \{1, \ldots, n\} \setminus \{k_1, \ldots, k_r\}$. σ s'anomena l'r-cicle i el denotem per $(k_1, \ldots, k_r)$.

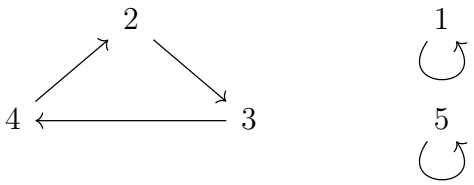


Figura 1.1: Exemple amb $(2, 3, 4) \in S_5$

Exemple 1.2.12. Podem posar el 2-cicle i el 3-cicle:

$$\begin{aligned} S_2 &= \{Id, (1,2)\}; \\ S_3 &= \{Id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}; \\ S_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ no és un cicle.} \end{aligned} \tag{1.2.9}$$

Definició 1.2.13 (Cicles disjunts)**.** Siguin $(k_1, \ldots, k_r)$ i $(l_1, \ldots, l_s)$ dos cicles. Són disjunts si els conjunts $\{k_1, \ldots, k_r\}$ i $\{l_1, \ldots, l_s\}$ són disjunts. El producte de cicles disjunts commuta.

Exemple 1.2.14. Per exemple, a S_5 ho són $(1, 4, 5)$ i $(2, 3)$. En general, la forma de representar un cicle no és pas única.

Proposició 1.2.15. *Tota permutació és producte de cicles disjunts 2 a 2, únicament determinats tret de l'ordre.*

Demostració. Sigui $\sigma \in S_n$, diferent de la identitat. Tenim, al menys, un enter $k \in \{1, \ldots, n\}$ tal que $\sigma(k) \neq k$. Considerem $k, \sigma(k), \sigma^2(k), \ldots$ Com $\{1, 2, \ldots, n\}$ és finit, ha d'existir algun r natural tal que $\sigma^r)k = k$. Prenem l'r més petit amb aquesta condició. Aleshores, els enters $k, \sigma(k), \ldots, \sigma^{r-1}(k)$ són tots diferents.
Considerem el cicle $c_1 = (k, \sigma(k), \ldots, \sigma^{r-1}(k))$. Si per a tot $i \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k)\}$ és $\sigma(i) = i$, tenim que $\sigma = c_1$. En cas contrari, sigui $l \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k)\}$ tal que $\sigma(l) \neq l$ i sigui s l'enter més petit tal que $\sigma^s(l) = l$.
Posem c_2 el cicle $(l, \sigma(l), \ldots, \sigma^{s-1}(l))$. Observem que els conjunts

$$\{k, \sigma(k), \ldots, \sigma^{r-1}(k)\} \text{ i } \{l, \sigma(l), \ldots, \sigma^{s-l}(l)\} \tag{1.2.10}$$

han de ser necessàriament disjunts. Si per a tot

$$i \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k), l, \sigma(l), \ldots, \sigma^{s-1}(l)\} \tag{1.2.11}$$

és $\sigma(i) = i$, tenim que $\sigma = c_1 c_2$. Si no, continuaríem iterativament el procés fins acabar, fet garantit donada la finitud del conjunt.
Observem que si F és el conjunt d'enters que queden fixos per σ, aleshores $F \cup \{k, \sigma(k), \sigma^{r-1}(k)\}$ és el conjunt d'enters que queden fixos per $c_1^{-1}\sigma$. Anàlogament,

$$F \cup \{k, \sigma(k), \sigma^{r-1}(k)\} \cup \{l, \sigma(l), \ldots, \sigma^{s-l}(l)\} \tag{1.2.12}$$

és el conjunt d'enters que queden fixos per $c_2^{-1}c_1^{-1}\sigma$. I així, recursivament i en un nombre finit de passos, arribem a una descomposició de σ com a producte de cicles. Els factors són únics ja que per a cada $i \in \{1, 2, \ldots, n\} \setminus F$ hi ha un únic factor tal que $c(i) \neq i$ i, per aquest, $c(i) = \sigma(i)$. ■

Corol·lari 1.2.16. *Tota permutació és producte de transposicions (una transposició és un 2-cicle).*

Demostració. N'hi ha prou amb veure que tot cicle és producte de transposicions. Ara tenim $(k_1, \ldots, k_r) = (k_1, k_2)(k_2, k_3) \cdots (k_{r-1}, k_r)$. Cadascuna d'aquestes transposicions, des de la dreta, va enviant un element al seu anterior, fins arribar al k_1. ■

Observació 1.2.17. Posem una permutació qualsevol:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 5 & 7 & 1 & 4 & 10 & 3 & 11 & 6 & 8 & 12 & 9 \end{pmatrix} = (1, 2, 5, 4)(3, 7)(6, 10, 8, 11, 12, 9). \tag{1.2.13}$$

De fet, podem escriure les permutacions com a producte de transposicions:

$$(1, 2)(2, 5)(5, 4)(3, 7)(6, 10)(10, 8)(8, 11)(11, 12)(12, 9). \tag{1.2.14}$$

1.3 Morfismes de grups

Definició 1.3.1 (Morfisme). Si G, G' són grups, una aplicació $f : G \longrightarrow G'$ és un morfisme de grups si $f(xy) = f(x)f(y)$, per a tot $x, y \in G$.

Exemple 1.3.2. L'aplicació signatura n'és un bon exemple. $\varepsilon : S_n \longrightarrow \{\pm 1\}$, $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Un altre bon exemple és el determinant pel grup lineal n (el de les matrius invertibles de dimensió n):

$$\begin{array}{rccc} \det : & GL(n, \mathbb{R}) & \longrightarrow & \mathbb{R} \setminus \{0\} \\ & M & \longrightarrow & \det(M). \end{array} \tag{1.3.1}$$

Proposició 1.3.3. *Si G i G' són grups, e l'element neutre de G, e' el de G' i $f : G \longrightarrow G'$ és un morfisme de grups, es compleix:*

1. $f(e) = e'$,

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

Demostració. Per al primer apartat, sabem que $e = ee$ per definició i prenem $f(e)$. $f(e) = f(ee) = f(e)f(e) \implies f(e) = e'$; hem usat les propietats de l'element neutre en la primera igualtat, la definició de morfisme en la segona i la llei de simplificació en la tercera.
Per al segon, ens quedem amb el producte $f(x^{-1})f(x)$. En efecte, $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$. Podem demostrar el mateix per la dreta, de manera totalment anàloga. D'aquesta manera, $f(x^{-1}) = f(x)^{-1}$. ■

Proposició 1.3.4. *Si G, G', G'' són grups, $f : G \longrightarrow G', g : G' \longrightarrow G''$ són morfismes de grups, aleshores $g \circ f : G \longrightarrow G''$ és un morfisme de grups.*

Demostració. Si $x, y \in G$, tenim $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$, on a la segona igualtat usem que f és morfisme i a la tercera que ho és g. ■

Definició 1.3.5 (Nucli i imatge d'un grup)**.** Siguin G, G' grups. Per a un morfisme de grups $f : G \longrightarrow G'$ definim el nucli de f com $\ker(f) = \{x \in G \mid f(x) = e'\}$ (els elements del conjunt inicial que s'envien per f al neutre del conjunt d'arribada) i definim la imatge de f com $\mathrm{im}(f) = \{f(x) \mid x \in G\}$ (el conjunt d'imatges per f).

Proposició 1.3.6. *Si $f : G \longrightarrow G'$ és morfisme de grups, $\ker(f)$ és subgrup de G i $\mathrm{im}(f)$ és subgrup de G'.*

Demostració. Com $f(e) = e'$, es dona que $e \in \ker(f)$; per tant, $\ker(f) \neq \emptyset$. Si $x, y \in \ker(f)$, tenim $f(xy^{-1}) = f(x)f(y)^{-1} = e$, on usem la definició de morfisme en la primera igualtat i, a la segona, que x, y són elements de $\ker(f)$. Resulta, doncs, que $\ker(f)$ és subgrup de G.
Com $f(e) = e'$, $e' \in \mathrm{im}(f)$; per tant, $\mathrm{im}(f) \neq \emptyset$. Si $x', y' \in \mathrm{im}(f)$, tenim que $x' = f(x), y' = f(y)$ per a certs $x, y \in G$. Ara:

$$x'(y')^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in \mathrm{im}(f) \implies \mathrm{im}(f) \text{ subgrup de } G'. \quad (1.3.2)$$

A la tercera igualtat hem de notar que $xy^{-1} \in \ker(f)$. ■

Definició 1.3.7 (Tipus de morfismes)**.** Suposem dos grups G, G' i f una aplicació $f : G \longrightarrow G'$.

1. Un *monomorfisme* de grups és un morfisme de grups injectiu, és a dir, $\ker(f) = \{e\}$.
2. Un *epimorfisme* de grups és un morfisme de grups exhaustiu, és a dir, $\mathrm{im}(f) = G'$.
3. Un *isomorfisme* de grups és un morfisme de grups bijectiu. Diem que dos grups G, G' són isomorfs i posem $G \simeq G'$ si existeix un isomorfisme de grups $f : G \longrightarrow G'$. Clarament, la relació de ser isomorfs és una relació d'equivalència.
4. Un *endomorfisme* d'un grup G és un morfisme de grups de G en G.
5. Un *automorfisme* de G és un endomorfisme de G bijectiu.

Proposició 1.3.8. *Sigui $f : G \longrightarrow G'$ un morfisme de grups. f és un morfisme injectiu si, i només si,* $\ker(f) = \{e\}$.

Demostració.

$\Rightarrow$ Suposem f injectiu i sigui $x \in \ker(f)$. Tenim $f(x) = e' = f(e) \implies x = e$, a causa de la definició d'injectivitat. Per tant, $\ker(f) = \{e\}$.

$\Leftarrow$ Suposem ara $\ker(f) = \{e\}$ i siguin $x, y \in G$ tals que $f(x) = f(y)$. Tenim $f(x) = f(y) \implies e' = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$. Per tant, $xy^{-1} \in \ker(f)$. Notem que totes les implicacions que hem fet resulten ser equivalències. Així, fem servir la hipòtesi que $\ker(f) = \{e\}$. Aleshores, $xy^{-1} = e$; equivalentment, $x = y$.

■

Proposició 1.3.9. *Si $f : G \longrightarrow G'$ és un morfisme de grups bijectiu, aleshores $f^{-1} : G' \longrightarrow G$ també és morfisme de grups.*

Demostració. $f^{-1}(x') = x \iff f(x) = x'$. Hem de veure que $f^{-1}(x'y') = f^{-1}(x')f^{-1}(y')$. Això és equivalent a la igualtat que ens queda si apliquem f a les dues bandes:

$$f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(x')f^{-1}(y'). \tag{1.3.3}$$

on hem usat que f és morfisme de grups pel terme de la dreta de la igualtat. ■

Definició 1.3.10 (Grups isomorfs)**.** Diem que G i G' són isomorfs si existeix $f : G \longrightarrow G'$ tal que f és un isomorfisme de grups. La relació d'isomorfia és, de fet, una relació d'equivalència.

Exemple 1.3.11. Sigui G un grup, amb $x \in G$. Aleshores el següent morfisme de grups és un isomorfisme de grups:

$$\begin{array}{rccc} \varphi_x : & G & \longrightarrow & G \\ & y & \longmapsto & xyx^{-1} \end{array} \tag{1.3.4}$$

Siguin $y_1, y_2 \in G$. Aleshores, $\varphi_x(y_1y_2) = xy_1y_2x^{-1} = (xy_1x^{-1})(xy_2x^{-1}) = \varphi_x(y_1)\varphi_x(y_2)$. $\varphi_{x^{-1}}$ és l'aplicació inversa de φ_x (φ_x és bijectiva). φ_x és un automorfisme de conjugació per x.

Proposició 1.3.12. *Sigui $f : G \longrightarrow G'$ un morfisme de grups:*

1. *Si H és un subgrup de G, $f(H) = \{f(H) \mid x \in H\}$ és subgrup de G'.*
2. *Si H' és subgrup de G', $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ és subgrup de G.*

Demostració. Agafem l'element neutre $e \in H$. Aleshores, $e' = f(e) \in f(H)$, de manera que la imatge per f d'H és no buida ($f(H) \neq \emptyset$).

$$\begin{gathered} x', y' \in f(H) \iff x' = f(x), y' = f(y), \quad x, y \in H. \\ x'y'^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in f(H) \implies x'y'^{-1} \in f(H), \end{gathered} \tag{1.3.5}$$

on $xy^{-1} \in H$. Pel que fa al segon apartat, $e' \in H'$ i $f(e) = e'$, de manera que $e \in f^{-1}(H')$. Aleshores, la inversa per H' és no buida ($f^{-1}(H') \neq \emptyset$). Prenem ara $x, y \in f^{-1}(H')$.

$$f(xy^{-1}) = f(x)f(y)^{-1} \in H' \implies xy^{-1} \in f^{-1}(H'). \tag{1.3.6}$$

Hem usat que un subconjunt és subgrup si, i només si, per a tot x, y, xy^{-1} és tancada. ■

Observació 1.3.13. Convendria no confondre f^{-1} aplicació inversa (f és necessàriament bijectiva) i f^{-1} imatge inversa (funciona per a subconjunts propis de l'espai d'arribada). Un recordatori de teoria de conjunts: si A i A' són conjunts, $f : A \longrightarrow A'$ una aplicació, B' un subconjunt d'A', definim la imatge inversa de B' per f per:

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}. \tag{1.3.7}$$

1.4 Teorema de Lagrange

Definició 1.4.1 (Ordre d'un grup)**.** Donat un grup G, diem que G és finit si el conjunt G és finit i, en aquest cas, diem ordre de G i indiquem per $|G|$ el cardinal del conjunt G.

Definició 1.4.2 (Relacions per la dreta i per l'esquerra)**.** Donats un grup G i un subgrup H de G, definim a G les relacions D i E per:

$$xDy \iff x^{-1}y \in H,\ xEy \iff yx^{-1} \in H. \tag{1.4.1}$$

Proposició 1.4.3. *Les relacions D i E són relacions d'equivalència.*

Demostració. Es prova per les dues relacions de forma anàloga. Ho provarem, sense pèrdua de generalitat, per E.

1. Per a $x \in G$, tenim que xEx, ja que $xx^{-1} = e \in H$ (reflexivitat).
2. Per a $x, y \in G$, $xEy \iff yx^{-1} \in H \iff (yx^{-1})^{-1} = xy^{-1} \in H \iff yEx$ (commutativitat).
3. Per a $x, y, z \in G$, provem la transitivitat:

$$\left.\begin{matrix} xEy \\ yEz \end{matrix}\right\} \implies \left.\begin{matrix} yx^{-1} \in H \\ zy^{-1} \in H \end{matrix}\right\} \implies zx^{-1} = (zy^{-1})(yx^{-1}) \in H \implies xEz. \tag{1.4.2}$$

Per la dreta, sigui x fixat. $xDy \iff x^{-1}y = h \in H \iff y = xh$. En més detall ara. ■

Considerem ara les classes d'equivalència per les relacions D i E. Tenim:

$$xDy \iff x^{-1}y \in H \iff y = xh \text{ per a algun } h \in H. \tag{1.4.3}$$

Tenim, doncs, que la classe d'equivalència de $x \in G$ per la relació D és el conjunt $\{xh \mid h \in H\}$. Escrivim aquest conjunt com xH i diem que és la classe de x per la dreta mòdul H. Posem G/D el conjunt quocient de G per la relació D. Anàlogament, tenim:

$$xEy \iff yx^{-1} \in H \iff y = hx \text{ per a algun } h \in H. \tag{1.4.4}$$

Tenim, doncs, que la classe d'equivalència de $x \in G$ per a la relació E és el conjunt $\{hx \mid h \in H\}$. Escrivim aquest conjunt com Hx i diem que és la classe de x per l'esquerra mòdul H. Posem G/E el conjunt quocient de G per la relació E.

Observació 1.4.4. Observem que les aplicacions:

$$\begin{array}{cc} H \longrightarrow xH & H \longrightarrow Hx \\ h \longmapsto xh & h \longmapsto hx \end{array} \quad \left\{ \begin{array}{c} \text{enviem l'element a la classe per la dreta (esquerra)} \\ \text{podem construir la inversa} \end{array} \right. \tag{1.4.5}$$

són bijectives; per tant, totes les classes d'equivalència tant per D com per E tenen el mateix cardinal que H. Ara, per a $x, y \in G$ tenim $y \in xH \iff y^{-1} \in Hx^{-1}$; per tant, $y \longmapsto y^{-1}$ indueix una bijecció de G/D en G/E. Ara:

$$\begin{array}{ccc} G/E & \longrightarrow & G/D \\ xH & \longmapsto & H\varphi(x), \end{array} \quad \varphi : x \longmapsto x^{-1}. \tag{1.4.6}$$

Anàlogament, és clara una bijecció de G/E en G/D.

Exemple 1.4.5.

- Si G és abelià, es dona evidentment que $D = E$ (hi ha la mateixa relació tant per la dreta com per l'esquerra a causa de la commutativitat).
- Per a $G = \mathbb{Z}, H = m\mathbb{Z}$, es dona $D = E$ i és una congruència mòdul m.
- Determinem ara els conjunts quocients G/D i G/E per a $G = S_3 = \{Id, t_1, t_2, t_3, s_1, s_2\}, H = \{Id, t_1\}$.

$$\begin{array}{c} \mathbb{I}H = H,\ t_2H = \{t_2, t_2t_1 = s_2\}, t_3H = \{t_3, t_3t_1 = s_1\} \text{ (classes per l'esquerra).} \\ H\mathbb{I} = H,\ Ht_2 = \{t_2, t_1t_2 = s_1\}, Ht_3 = \{t_3, t_1t_3 = s_2\} \text{ (classes per la dreta).} \end{array} \tag{1.4.7}$$

  Hem indicat $\mathbb{I}$ per denotar la identitat. Tenim, doncs, que G/D i G/E són diferents.

Definició 1.4.6 (Índex de grup)**.** Donats un grup G i un subgrup H de G, posem $[G : H]$ i diem índex de G en H el cardinal de G/D (que hem vist és igual al de G/E). En altres paraules, és el nombre de classes d'equivalència que existeix, tant per la dreta com per l'esquerra.

Teorema 1.4.7 (Teorema de Lagrange)**.** *Donats un grup G i un subgrup H de G, el grup G és finit si, o només si, H i $[G : H]$ són finits. En aquest cas,*

$$|G| = |H| \cdot [G : H]. \tag{1.4.8}$$

En particular, $|H|$ i $[G : H]$ són divisors de $|G|$.

Demostració. Suposem G finit. Com que H és subgrup (i, en particular, subconjunt) de G, H és finit i com les classes d'equivalència per D formen una partició de G, és a dir, G és reunió disjunta de les classes d'equivalència, $[G : H]$ és finit.

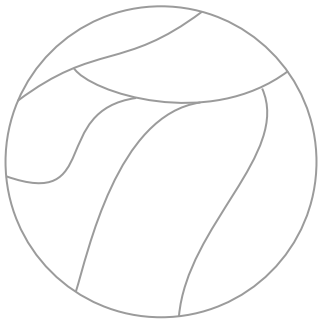


Figura 1.2: Divisió d'un grup en classes d'equivalència

Suposem ara H i $[G:H]$ finits. Com G és reunió disjunta de les classes d'equivalència per D, hi ha $[G:H]$, i a cada classe d'equivalència, hi ha tants elements com a H, tenim $|G| = |H| \cdot [G:H]$. ■

1.5

Subgrups normals. Grup quocient

Volem ara definir una estructura de grup en el conjunt quocient d'un grup G per la relació D associada a un subgrup H. Considerem el cas $G = S_3, H = \{Id, t_1\}$. Intentem fer el producte de les classes $[t_2]$ de t_2 i $[t_3]$ de t_3. Posem $[t_2][t_3] = [t_2t_3] = [s_1]$. Però $s_2 \in [t_2]$ i $s_1 \in [t_3]$ i, en canvi, $s_2s_1 = Id \notin [s_1]$. El producte depèn del representant; per tant, no estaria ben definit. Veiem ara que si podem definir un producte de classes que no depengui del representant escollit a cada classe, aleshores el conjunt quocient té estructura de grup.

Definició 1.5.1 (Relació compatible)**.** Sigui T una relació d'equivalència definida en un grup G. Diem que T és compatible amb l'operació de G si per qualssevol $x, y, x', y' \in G$ es compleix:

$$\left.\begin{matrix} xTx' \\ yTy' \end{matrix}\right\} \implies xyTx'y'. \tag{1.5.1}$$

Proposició 1.5.2. *Si T és una relació definida en un grup G, compatible amb l'operació de G, aleshores G/T és grup amb l'operació definida per $[x][y] = [xy]$.*

Demostració. Clarament l'operació està ben definida, és associativa, l'element neutre és $[e]$ en G/T i $[x]^{-1} = [x^{-1}]$ en G/T. ■

Proposició 1.5.3. *Sigui G un grup, H un subgrup de G, D i E les relacions definides a partir d'H. Els enunciats següents són equivalents:*

- *$xH = Hx$, per a tot $x \in G$;*
- *$xHx^{-1} = \{xhx^{-1} \mid h \in H\} = H$, per a tot $x \in G$;*
- *$xHx^{-1} \subset H$, per a tot $x \in G$;*
- *D és compatible amb l'operació de G;*
- *E és compatible amb l'operació de G.*

Demostració.

$1 \Rightarrow 2$ Suposat $xH = Hx$ per a tot $x \in G$ volem provar que $xHx^{-1} = H$, per a tot $x \in G$ un altre cop. Siguin $x \in G$ i $h \in H$. Posem $xh \in xH = Hx$. Per tant, existeix un $h' \in H$ tal que $xh = h'x$.

$$(xh)x^{-1} = (h'x)x^{-1} = h'(xx^{-1}) = h' \in H. \tag{1.5.2}$$

Hem vist que $xHx^{-1} \subset H$ per a tot $x \in G$. $x^{-1}Hx \subset H \iff H \subset xHx^{-1}$ i, per tant, $x^{-1}hx = h' \iff xh'x^{-1} = h$.

$2 \Rightarrow 3$ Una igualtat és una doble inclusió. Simplement cal usar la inclusió cap a la dreta.

$2 \Rightarrow 1$ Ara prenem com a hipòtesi $xHx^{-1} = H$ per a tot $x \in G$. En particular, tenim que $xHx^{-1} \subset H$ per a tot $x \in G$; per tant, $xH = Hx$ per a tot $x \in G$. Existeix $h' \in H$ tal que $xhx^{-1} = h'$ i això implica que $xh = h'x \in Hx$, és a dir, $xH \subset Hx$. Podem obtenir la inclusió contrària anàlogament, $x^{-1}Hx \subset H$ per a tot $x \in G$; per tant, existeix $h' \in H$ tal que $x^{-1}hx = h'$ i això implica que $xh = h'x \in xH$.

$1 \Rightarrow 4$ D resulta ser compatible amb el producte de G.

$$\left.\begin{matrix} x' = xh \\ y' = yh' \end{matrix}\right\} \implies x'y' = x(hy)h' = x(yh'')h' = xy(h''h') \implies \left.\begin{matrix} xDx' \\ yDy' \end{matrix}\right\} \implies xyDx'y'. \tag{1.5.3}$$

$3 \Leftarrow 4$ Ara suposem que D és compatible. Volem demostrar que $xHx^{-1} \subset H$, per a tot $x \in G$. Volem veure $x \in G$ i $h \in H$ implica que $xhx^{-1} \in H$.

$$\left.\begin{matrix} xhDx \\ x^{-1}Dx^{-1} \end{matrix}\right\} \implies xhx^{-1}Dxx^{-1} = e \implies xhx^{-1} \in H. \tag{1.5.4}$$

$1 \Rightarrow 5$ Ara volem provar que si $xH = Hx$ per a tot $x \in G$, E és compatible amb el producte de G. Posem $x' = hx$ i $y' = h'y$. Aleshores, $x'y' = h(xh')y = (hh'')xy$, on a la segona igualtat hem usat que $xh' = h''x$ per a algun $h'' \in H$. Per tant, $(x'y')E(xy)$ i ja hem acabat.

$3 \Leftarrow 5$ Suposant que E és compatible, volem trobar que $xHx^{-1} \subset H$ per a tot $x \in G$. Prenem $x \in G$ i $h \in H$. Per hipòtesi, xEx i $hx^{-1}Ex^{-1}$; així, $xhx^{-1}Exx^{-1} = e \implies xhx^{-1} \in H$.

■

Definició 1.5.4 (Morfisme de pas al quocient)**.** El definim per $\pi : G \longrightarrow G/H$ i envia cada element de G a la seva classe en G/H. És epimorfisme de grups amb nucli H.

Definició 1.5.5 (Grup normal)**.** Un subgrup H de G es diu normal si es compleix alguna (i, per conseqüència, totes) de les condicions de 1.5.3. En aquest cas, $G/D = G/E$ i l'escrivim G/H o $H \lhd G$. En particular, anomenem $x \longmapsto [x]$ com morfisme de pas al quocient.

Definició 1.5.6 (Grup quocient)**.** Sigui H un subgrup de G. Si H és normal, G/H té estructura de grup. En efecte, $[x][y] = [xy]$ i es diu grup quocient de G en H.

Proposició 1.5.7. *Si T és relació d'equivalència compatible amb l'operació del grup G, $H := \{x \in G \mid xTe\}$ és subgrup normal de G i la relació d'equivalència associada a H coincideix amb T.*

Demostració. Veiem primer que H és subgrup normal de G. Per a $x \in G$ i $h \in H$, hem de veure que $xhx^{-1} \in H$; equivalentment, per a $x, h \in G$, hem de veure $hTe \implies xhx^{-1}Te$. Com T és relació d'equivalència, tenim xTx i $x^{-1}Tx^{-1}$ i, com T és compatible amb l'operació de G, $xTx, hTe, x^{-1}Tx^{-1}$ impliquen

$$xhx^{-1}Txex^{-1} = xx^{-1} = e. \tag{1.5.5}$$

Com H és normal en G, les relacions D i E definides a partir d'H són iguals. Vegem que D coincideix amb T. Per a $x, y \in G$, hem de veure $xTy \iff xDy$. Per definició de D i H, tenim

$xDy \iff x^{-1}y \in H \iff x^{-1}yTe$. Ens cal veure:

$$xTy \iff x^{-1}yTe. \tag{1.5.6}$$

Si xTy, com T és relació d'equivalència, tenim yTx i $x^{-1}Tx^{-1}$ i, com T és compatible amb l'operació de G, $x^{-1}yTx^{-1}x = e$. Recíprocament, si $x^{-1}yTe$, com T és reflexiva, tenim xTx i, com T és compatible amb l'operació de G, $y = x(x^{-1}y)Txe = x$, que implica xTy, per ser T simètrica. ■

Proposició 1.5.8. *Si $f : G \longrightarrow G'$ és un morfisme de grups,* $\ker(f)$ *és subgrup normal de G.*

Demostració. Per a $x \in G$, $h \in \ker(f)$, tenim

$$f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)e'f(x)^{-1} = f(x)f(x)^{-1} = f(xx^{-1}) = f(e) = e'. \tag{1.5.7}$$

Per tant, $xhx^{-1} \in \ker(f)$. ■

Proposició 1.5.9. *Sigui $f : G \longrightarrow G'$ un morfisme de grups.*

1. *Si H és un subgrup de G, aleshores $f(H)$ és subgrup de G'.*
2. *Si H' és subgrup de G', aleshores $f^{-1}(H')$ és subgrup de G. A més, si H' és subgrup normal de G', aleshores $f^{-1}(H')$ és subgrup normal de G.*

Demostració.

1. Siguin $x', y' \in f(H)$. Tenim $x' = f(x), y' = f(y)$, per a certs $x, y \in H$ i, per ser f morfisme, $x'y'^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$. Ara, per ser H subgrup de G, $xy^{-1} \in H$ i, per tant, $x'y'^{-1} \in f(H)$.
2. Sigui H' un subgrup de G' i $x, y \in f^{-1}(H')$. Volem veure $xy^{-1} \in f^{-1}(H')$, que equival a $f(xy^{-1}) \in H'$. Ara, per ser f morfisme, $f(xy^{-1}) = f(x)f(y)^{-1}$. Com $x \in f^{-1}(H')$, clarament $f(x) \in H'$; anàlogament, $f(y) \in H'$ i es té $f(y)^{-1} \in H'$ per ser H' subgrup de G'. De nou, per ser H' subgrup de G':

   $$f(x) \in H',\ f(y)^{-1} \in H' \implies f(xy^{-1}) = f(x)f(y)^{-1} \in H'. \tag{1.5.8}$$

   Suposem ara que H' és normal en G. Donats $x \in G$ i $h \in f^{-1}(H')$, volem veure $xhx^{-1} \in f^{-1}(H')$. Ara tenim $f(xhx^{-1}) = f(x)f(h)f(x)^{-1} \in H'$, per ser $f(h) \in H'$ i H' normal en G'.

■

Corol·lari 1.5.10. *Si $\varphi : G \longrightarrow G'$ és un morfisme de grups i H' és subgrup normal de G', aleshores $\varphi^{-1}(H')$ és subgrup normal de G. En particular,* $\ker(\varphi) = \varphi^{-1}(\{e'\})$ *és subgrup normal de G.*

Demostració. És conseqüència directa de les dues proposicions anteriors. Sigui $x \in G$ i $h \in \varphi^{-1}(H')$, volem veure que $xhx^{-1} \in \varphi^{-1}(H')$. Equivalentment, $\varphi(xhx^{-1}) \in H'$:

$$\varphi(xhx^{-1}) = \varphi(x)\varphi(h)\varphi(x)^{-1} \in H', \tag{1.5.9}$$

on $\varphi(h) \in H'$, $\varphi(x)^{-1} \in H$. ■

Exemple 1.5.11. Sigui $i : \{Id, t_1\} \longrightarrow S_3$ una inclusió, que envia $Id \longmapsto Id$ i $t_1 \longmapsto t_1$. $\{Id, t_1\}$ és subgrup normal de $\{Id, t_1\}$, però $i(\{Id, t_1\}) = \{Id, t_1\}$ no és subgrup normal de S_3.

Exercici 1.5.12. *Siguin $f : G_1 \longrightarrow G_2$ un morfisme de grups i H_1 un subgrup de G_1. Demostreu que si H_1 és normal en G_1, llavors $f(H_1)$ és un subgrup normal de $f(G_1)$. Proveu amb un contraexemple que $f(H_1)$ no és necessàriament normal en G_2.*

Resolució. Si H_1 és normal en G_1, podem agafar $g \in G_1$ tal que $gH_1g^{-1} = H_1 \iff ghg^{-1} \in H_1, \forall h \in H_1$. Per tant, utilitzant que f és morfisme de grups:

$$f(ghg^{-1}) \in f(H_1) \iff f(g)f(h)f(g)^{-1} \in f(H_1). \tag{1.5.10}$$

Per demostrar que $f(H_1)$ és normal en $f(G_1)$, siguin $g' = f(g) \in f(G_1)$ i $h' = f(h) \in f(H_1)$. Aplicant la definició de subgrup normal, hauríem d'obtenir que $g'h(g')^{-1} \in f(H_1)$ per a tot h'. Com que l'expressió anterior és coincident amb (1.5.10), ha quedat demostrat. En principi, per provar el que se'ns demana hem de suposar que f no és epimorfisme i triar un $g \in G_2 \setminus f(G_1)$ de manera que no es complirà la condició de subgrup normal. ■

Proposició 1.5.13. *Si G és abelià, aleshores cada subgrup H de G és normal. Si $[G : H] = 2$, aleshores H és normal en G.*

Demostració. Si G és abelià, aleshores $xH = Hx$ per a tot $x \in G$. Pel que fa al segon que se'ns demana, recordem que si $[G : H] = 2$, H té exactament dos *cosets* en G: un d'aquests és H mateix, i l'altre ha de ser $G \setminus H$. Aquest últim conté tant les classes per la dreta com per l'esquerra i, per tant, han de ser iguals. ■

1.6 Teoremes d'isomorfia

Definició 1.6.1 (f factoritza a través de G/H). Siguin G, G' grups i sigui $f : G \longrightarrow G'$ un morfisme de grups i sigui H un subgrup normal de G. Diem que f factoritza a través de G/H si existeix un morfisme de grups $\overline{f} : G/H \longrightarrow G'$ tal que $f = \overline{f} \circ \pi$, on $\pi : G \longrightarrow G/H$ és el morfisme de pas a quocient, és a dir, si existeix un morfisme de grups $\overline{f} : G/H \longrightarrow G'$ que faci commutatiu el diagrama:

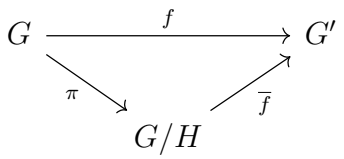


Figura 1.3: El diagrama commuta si, i només si, $f = \overline{f} \circ \pi$.

Proposició 1.6.2. *Siguin G, G' grups i sigui $f : G \longrightarrow G'$ un morfisme de grups i sigui H un subgrup normal de G. Aleshores, f factoritza a través de G/H si, i només si, $H \subset \ker(f)$.*

Demostració.

$\Rightarrow$ Si f factoritza a través de G/H i $h \in H$, tenint en compte la definició de π i que $\overline{f}$ és morfisme, obtenim $f(h) = \overline{f}(\pi(h)) = \overline{f}([h]) = \overline{f}(\overline{e}) = e'$, on en la tercera igualtat $[h] = \overline{e}$ per la sel·lecció d'h. $\overline{e}$ indica l'element neutre de G/H i e' el del de G'. Per tant, $H \subset \ker(f)$.

$\Leftarrow$ Si $H \subset \ker(f)$, definim $\overline{f} : G/H \longrightarrow G'$ per $\overline{f}([x]) = f(x)$, on $[x]$ indica la classe a G/H d'un element x de G. Hem de veure que la definició no depèn del representant de la classe, és a dir, que $[x] = [y] \implies f(x) = f(y)$. Si $y \in [x]$ tenim que $y = xh$, amb $h \in H$. Per tant,

$$f(y) = f(xh) = f(x)f(h) = f(x)e' = f(x), \tag{1.6.1}$$

ja que $h \in H \subset \ker(f)$. Ara, cal veure si $\overline{f}$ és morfisme de grups. Si $x, y \in G$, tenim:

$$\overline{f}([x][y]) = \overline{f}([xy]) = f(xy) = f(x)f(y) = \overline{f}([x])\overline{f}([y]), \tag{1.6.2}$$

per la definició d'operació al grup quocient G/H (el producte de classes), el fet que f és morfisme de grups i la definició de $\overline{f}$. Finalment, és clar que $f = \overline{f} \circ \pi$ (així doncs, f factoritza a través de G/H per definició).

■

Teorema 1.6.3 (Primer teorema d'isomorfia). *Si G, G' són grups i $f : G \longrightarrow G'$ és un morfisme de grups, aleshores f factoritza a través de $G/\ker(f)$ i tenim $f = i \circ \tilde{f} \circ \pi$, amb $\tilde{f}$ isomorfisme de grups $G/\ker(f)$ en $\mathrm{im}(f)$, on $\pi : G \longrightarrow G/\ker(f)$ és el morfisme de pas al quocient i $i : \mathrm{im}(f) \longrightarrow G'$ la inclusió. Tenim, doncs, un diagrama commutatiu:*

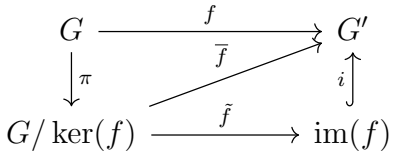


Figura 1.4: Primer teorema d'isomorfia.

Demostració. Per 1.6.2, existeix un morfisme $\overline{f} : G/\ker(f) \longrightarrow G'$, que envia $[x] \longmapsto f(x)$, tal que $f = \overline{f} \circ \pi$. Clarament, $\overline{f}$ és injectiu i $\overline{f} = i \circ \tilde{f}$, amb $\tilde{f}$ isomorfisme de $G/\ker(f)$ en $\mathrm{im}(\overline{f})$. Com $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$, per la definició de $\overline{f}$ obtenim el resultat desitjat.

$$\overline{f} = i \circ \tilde{f}, \quad \tilde{f} : \begin{array}{ccc} G/\ker(f) & \longrightarrow & \mathrm{im}(\overline{f}) \\ [x] & \longmapsto & f(x) \end{array} \quad f = i \circ \tilde{f} \circ \pi, \ \tilde{f} \text{ és injectiva.} \tag{1.6.3}$$

$\tilde{f}$ és injectiva ja que, donada una classe $[x] \in G/\ker(f)$, $\tilde{f}([x]) = f(x) = e'$, de manera que $x \in \ker(f)$ i, per tant, $[x] = [e]$; de fet, $\ker(\tilde{f}) = \{[e]\}$ i, en efecte, $\tilde{f}$ és injectiva. Com que $\overline{f}$ és un morfisme, $\tilde{f}$ és un morfisme també. ■

Teorema 1.6.4 (Segon teorema d'isomorfia). *Sigui $\varphi : G \longrightarrow G'$ un epimorfisme de grups. Sigui H' un subgrup normal de G' i $H = \varphi^{-1}(H')$. Aleshores, φ indueix un isomorfisme de G/H en $G'H'$.*

Demostració. Considerem la composició $\pi' \circ \varphi : G \longrightarrow G'/H'$, on $\pi' : G' \longrightarrow G'/H'$ és el morfisme de pas al quocient. Tenim $\pi' \circ \varphi$ exhaustiu i $\ker(\pi' \circ \varphi) = H$. Aplicant 1.6.3, obtenim que existeix un isomorfisme $\tilde{\varphi} : G/H \longrightarrow G'/H'$ tal que $\pi' \circ \varphi = \tilde{\varphi} \circ \pi$, on $\pi : G \longrightarrow G/H$ és el morfisme de pas al quocient. ■

Corol·lari 1.6.5. *Si G és un grup i F i H són subgrups normals de G amb $F \subset H$, aleshores H/F és subgrup normal de G/F i el morfisme de pas al quocient $G \longrightarrow G/F$ indueix un isomorfisme de G/H en $(G/F)/(H/F)$.*

Demostració. Si $[h] \in H/F$ i $[x] \in G/F$, tenim $xhx^{-1} \in H$ per ser H normal en G. Per tant, $[x][h][x]^{-1} = [xhx^{-1}] \in H/F$. Tenim, doncs, que H/F és subgrup normal de G/F. Considerem ara $\varphi : G \longrightarrow G/F$ el morfisme de pas al quocient. Aleshores, $\varphi^{-1}(H/F) = H$ i, aplicant 1.6.4, obtenim que G/H és isomorf a $(G/F)/(H/F)$. ■

Teorema 1.6.6 (Tercer teorema d'isomorfia)**.** *Sigui G un grup, H i F subgrups de G, amb H normal en G. Posem $HF := \{hf \mid h \in H, f \in F\}$. Aleshores, HF és un subgrup de G, $F \cap H$ és un subgrup normal de F i H és un subgrup normal d'HF. A més, la inclusió d'F en HF indueix un isomorfisme de $F/(F \cap H)$ en HF/H.*

Demostració. Provem primer que HF és un subgrup de G. Clarament, $e \in HF$. Sigui hf un element d'HF amb $h \in H$ i $f \in F$. Es compleix que $(hf)^{-1} = f^{-1}h^{-1} = (f^{-1}h^{-1}f)f^{-1}$. Com H és normal a G, sabem que $fhf^{-1} \in H \iff (fhf^{-1})^{-1} \in H \iff f^{-1}h^{-1}f \in H$, de manera que $(hf)^{-1} \in HF$. Siguin h_1f_1 i h_2f_2 elements d'HF, amb $h_1, h_2 \in H$ i $f_1, f_2 \in F$. Es dona que $(h_1f_1)(h_2f_2) = h_1(f_1h_2f_1^{-1})f_1f_2$. Com H és normal a G, $h_3 = f_1h_2f_1^{-1} \in H$; ens queda $(h_1h_3)(f_1f_2) \in HF$ i, per tant, $(h_1f_1)(h_2f_2) \in HF$.
Provem ara que $F \cap H$ és un subgrup normal de F. Sigui $x \in F \cap H$, amb $f \in F$. Com que H és normal en G, $fxf^{-1} \in H$ (en particular, $x \in H$); a més, per ser F subgrup de G obtenim que $fxf^{-1} \in F$ (en particular, $x \in F$). Per tant, $fxf^{-1} \in F \cap H$.
Ara, com H és subgrup normal de G per hipòtesi, HF és subgrup de G, $H \subset HF$ i H és subgrup normal d'HF.
Considerem ara la composició de la inclusió i de F en HF amb el morfisme de pas al quocient π de HF en $(HF)/H$. La composició $\pi \circ i$ s'escriu com: $\pi \circ i : F \xrightarrow{i} HF \xrightarrow{\pi} (HF)/H$.

1. Veiem, primer, que $\pi \circ i$ és epimorfisme. Si tenim $h \in H$ i $f \in F$, aleshores $(hf)f^{-1} = h \in H$ implica la igualtat $[hf] = [f]$ a $(HF)/H$, on $hf \in HF$ i $f^{-1} \in F$. Per tant,
$$[hf] = \pi(hf) = \pi(f) = (\pi \circ i)(f), \tag{1.6.4}$$
és a dir, tot element de $(HF)/H$ està a la imatge de $\pi \circ i$.
2. Amb aquesta informació, podem inferir l'existència de l'isomorfisme desitjat a partir del primer teorema d'isomorfia 1.6.3.
$$\ker(\pi \circ i) = F \cap \ker(\pi) = F \cap H \xrightarrow{1.6.3} F/(F \cap H) \simeq (HF)/H. \tag{1.6.5}$$

Amb tot, ja hem demostrat el que volíem. ■

1.7

Ordre d'un element d'un grup

Definició 1.7.1 (Subgrup de G generat per x). Si x és un element d'un grup G i n un enter, posem:

$$x^n : \begin{cases} \overbrace{x \cdots x}^{n} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ \overbrace{x^{-1} \cdots x^{-1}}^{n} & \text{si } n < 0 \end{cases} \tag{1.7.1}$$

Definim:

$$\begin{array}{rccc} f_x : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & x^n \end{array} \tag{1.7.2}$$

Clarament, f_x és un morfisme de $(\mathbb{Z}, +)$ en G. La imatge de f_x és un subgrup de G. L'escrivim $\langle x \rangle = \operatorname{im}(f_x)$ i diem que és el subgrup de G generat per x.

Definició 1.7.2 (Ordre d'un element). El subgrup $\langle x \rangle$ és el conjunt dels elements de G que són iguals a x^n per a algun $n \in \mathbb{Z}$. En particular, $\ker(f_x) = m\mathbb{Z}$ és subgrup de $\mathbb{Z}$. Per 1.1.14, tenim $\langle x \rangle \simeq \mathbb{Z}/m\mathbb{Z}$. Si $m > 0$, diem que m és l'ordre de x i posem $\operatorname{ord}(x)$. En cas que $m = 0$, diem que x té ordre infinit. *L'ordre de l'element és l'ordre del subgrup que genera.* En particular, l'ordre de x divideix l'ordre de G, $|G|$.

Observació 1.7.3. *L'ordre de l'element no és el mateix que l'ordre del grup.* Quan l'ordre és finit, quan considerem el subgrup de G generat per x $\langle x \rangle$, com m és generador del nucli, $x^m = e$. En aquest cas, $\langle x \rangle = \{e, x, x^2, \ldots, x^{m-1}\}$. Si $\operatorname{ord} x = \infty$, $\langle x \rangle \simeq \mathbb{Z}$: quan definim aquest morfisme, hem d'assumir que m és l'enter més petit tal que la potència m-èsima ens dona el neutre i, per tant, $\langle x \rangle = \mathbb{Z}$.

Exemple 1.7.4.

- Un r-cicle $(a_1, \ldots, a_r)$ té ordre r.
- Si agafem $z \in \mathbb{Z} \setminus \{0\}$ té ordre infinit (suposant que $\mathbb{Z}$ és un grup amb la suma, si agafem un element qualsevol i el sumem amb ell mateix tantes vegades com vulguem mai no ens donarà zero).
- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$ té ordre infinit, ja que la potència n-èsima de la matriu és $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$. En canvi, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ té ordre 2.

Exercici 1.7.5. *Sigui G un grup no trivial. Proveu que, si els únics subgrups de G són el trivial i el total, aleshores G és un grup finit i el seu ordre és primer.*

Resolució. G és un grup no trivial, de manera que és diferent del buit i d'$\{e\}$ (en aquest segon cas, l'exercici resulta trivial). En efecte, tot element de G diferent de l'element neutre pertany al subgrup total, i a cap subgrup més. Consegüentment, $G = \langle x \rangle$ i, per tant, és un grup finit. A més, si $n = k\ell$, $\langle x^k \rangle$ seria un subgrup propi de G, però l'únic subgrup no trivial és el total. Així, n ha de ser necessàriament primer. ∎

Exercici 1.7.6. *Siguin a, b dos elements d'un grup G. Proveu que* $\operatorname{ord}(bab^{-1}) = \operatorname{ord}(a)$. *És cert que* $\operatorname{ord}(ab) = \operatorname{ord}(ba)$*?*

Resolució. Sigui $n = \operatorname{ord}(bab^{-1})$. Fixem-nos que $bab^{-1} \in G$ pel fet de ser G un grup. Per definició d'ordre d'un element de grup, $(bab^{-1})^n = e \iff (bab^{-1}) \cdots (bab^{-1}) = e \iff ba^n = b \iff a^n = e$. Per tant, $\operatorname{ord}(bab^{-1}) = \operatorname{ord}(a)$. Pel que fa a la segona part de l'enunciat,

$$\begin{aligned} \operatorname{ord}(ab) = n \iff ab\overbrace{\cdots}^{n}ab = e \iff a^{-1}aba\overbrace{\cdots}^{n}bb^{-1} = a^{-1}b^{-1} \\ \iff ba\underbrace{\cdots}_{n-1}ba = (ba)^{-1} \iff (ba)^n = e. \end{aligned} \tag{1.7.3}$$

Per tant, tot i que *a priori* sembla que no, també es compleix la segona propietat. ■

Exercici 1.7.7. *Sigui M el conjunt de matrius de la forma:*

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a, b \in \mathbb{R}, a \neq 0. \tag{1.7.4}$$

Proveu que M és grup amb el producte usual de matrius i que M té infinits elements d'ordre 2.

Resolució. La primera part del problema és rutinària: per provar que $(M, \cdot)$ és grup provem que donats $A, B \in M$, es compleixen les següents condicions.

- L'associativitat és evident.
- Existència d'element neutre: efectivament, si $a = 1$ i $b = 0$ l'element neutre és la identitat.
- Existència d'element invers:

$$M \ni \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 & 0 & 1 \end{array}\right), \tag{1.7.5}$$

  que està definit ja que $a \neq 0$ per hipòtesi.
- L'operació és clarament tancada (tota multiplicació de matrius d'aquesta forma cau dins d'M).

Per demostrar que M té infinits elements d'ordre 2, agafem un element qualsevol del conjunt i fem la multiplicació corresponent:

$$A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} a^2 & ab+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff a = -1. \tag{1.7.6}$$

Podem escriure b en funció d'a: per a $a = -1$, $b - b = 0$ per a tot $b \in \mathbb{R}$. Per tant, solament ens cal fixar $a = -1$ i b queda lliure en $\mathbb{R}$. ■

1.8 Grups cíclics

Definició 1.8.1 (Grup cíclic)**.** Un grup G es diu cíclic si existeix $x \in G$ tal que $G = \langle x \rangle$ (és a dir, que està generat per un únic element). Diem que G està generat per x. Denotem per C_n el grup cíclic d'ordre n i aquest és isomorf a $\mathbb{Z}/n\mathbb{Z}$ (ho veurem a 1.8.4).

Teorema 1.8.2. *Sigui $G = \langle x \rangle$ un grup cíclic. Si x té un ordre infinit, totes les seves potències són diferents. Si $|x| = n \ll \infty$, aleshores els elements de G són justament $e, x, x^2, \ldots, x^{n-1}$. En particular, $|x| = |\langle x \rangle|$.*

Exemple 1.8.3.

- $\mathbb{Z}^* = \langle 1 \rangle$ és un grup cíclic infinit.
- $(\mathbb{Z}/m\mathbb{Z}, +) = \langle \overline{1} \rangle$ és un grup cíclic d'ordre m.

Proposició 1.8.4. *Tot grup cíclic és isomorf a $\mathbb{Z}$ o bé a $\mathbb{Z}/m\mathbb{Z}$, per a un enter $m > 0$. Per tant, dos grups cíclics del mateix ordre són isomorfs entre ells.*

Demostració. Sigui $G = \langle x \rangle$. Podem establir f_x exhaustiu definit de la següent manera:

$$\begin{array}{rccc} f_x : & \mathbb{Z} & \longrightarrow & G = \langle x \rangle \\ & n & \longmapsto & x^n \end{array} \tag{1.8.1}$$

Pel primer teorema d'isomorfia, $\mathbb{Z}/m\mathbb{Z} \simeq G$ si el grup G té ordre finit i $\ker(f_x) = m\mathbb{Z}$ amb $m \geq 0$. En canvi, si G té ordre infinit tenim $\mathbb{Z} \simeq G$. ■

Observació 1.8.5. Per a cada ordre podem considerar que hi ha un únic grup cíclic, tret d'isomorfismes. És a dir, si dos grups cíclics tenen el mateix ordre ha d'existir necessàriament un isomorfisme entre ells.

Corol·lari 1.8.6. *Si G és finit, G és cíclic si, i només si, existeix $x \in G$ tal que $\operatorname{ord} x = |G|$.*

Demostració. És conseqüència directa de la definició de grup cíclic: existeix un element x de G tal que $\langle x \rangle = G \implies |\langle x \rangle| = |G|$. L'ordre de x és l'enter natural més petit m tal que $x^m = e$ i $\langle x \rangle = \{e, x, x^2, \ldots, x^n\}$. ■

Exemple 1.8.7.

- S_3 no és cíclic: no té cap element d'ordre 6.
- Tot grup d'ordre p, amb p primer, és cíclic: sigui $x \in G$ tal que $x \neq e$. Aleshores, $\operatorname{ord} x > 1$ i, en particular, $\operatorname{ord} x$ divideix l'ordre de G, $|G| = p$. Per tant, $\operatorname{ord} x = p$ i $\langle x \rangle = G$.
- $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$. També, $(\mathbb{Z}/7\mathbb{Z})^* = \langle [5] \rangle$, ja que 3 i 5 són arrels primitives mòdul 7. Es pot comprovar elevant terme a terme a la tercera potència i la cinquena, respectivament.
- En canvi, $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ no és cíclic donat que $[3], [5], [7]$ tenen ordre 2.

Teorema 1.8.8. *Tot grup cíclic és abelià.*

Demostració. Sigui a un element de G tal que $G = \langle a \rangle$. Si $b, c \in G$, aleshores $b = a^m$ i $c = a^n$, per a certs $m, n \in \mathbb{Z}$. Aleshores, $bc = a^m a^n = a^{m+n}$, però $cb = a^n a^m = a^{n+m} = a^{m+n}$ també. ■

Lema 1.8.9. *Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n per a tot enter $k > 0$, es compleix:*

$$\operatorname{ord}(x^k) = \frac{n}{\operatorname{mcd}(n, k)}. \tag{1.8.2}$$

Demostració. Sigui $\ell \in \mathbb{Z}$ més gran que 0. Si $(x^k)^\ell = e$, aleshores $x^{k\ell} = e$. Per tant, $n \mid k\ell$. Ara, sigui $d = \text{mcd}(n,k)$. Podem escriure n i k com a producte de factors: $n = dn_1$ i $k = dk_1$, amb n_1 i k_1 primers entre ells. Així, $dn_1 \mid dk_1\ell \implies n_1 \mid k_1\ell$, de manera que $n_1 \mid \ell$.

$$(x^k)^{n_1} = x^{kn_1} = x^{nk_1} = (x^n)^{k_1} = e^{k_1} = e \implies \text{ord}(x^k) = n_1 = \frac{n}{\text{mcd}(n,k)} = \frac{n}{d}. \tag{1.8.3}$$

Notem que hem usat que $nk_1 = dn_1k_1 = kn_1$, ja que hem escrit $k = dk_1$. ■

Corol·lari 1.8.10. *Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n. Aleshores, x^k genera G si, i només si,* $\text{mcd}(n,k) = 1$.

Demostració. Tenim que x^k és generador de G si, i només si, x^k té ordre n. Per 1.8.9, x^k té ordre n si, i només si, $\text{mcd}(n,k) = 1$. Per tant, ja hem acabat. ■

Observació 1.8.11. Si prenem $G = (\mathbb{Z}/m\mathbb{Z})^*$ (que és el conjunt dels invertibles) amb m tal que existeixen arrels primitives mòdul m, totes les potències primitives cauen en classes diferents i per tant generen G. En concret, d'*Aritmètica* sabem que $a \in (\mathbb{Z}/m\mathbb{Z})^* \iff \text{mcd}(a,m) = 1$.

Proposició 1.8.12. *Tot subgrup d'un grup cíclic és cíclic.*

Demostració. Si $G = \langle x \rangle$ i H és el subgrup trivial, el resultat és trivial: $H = \{e\} = \langle e \rangle$. Si H és subgrup no trivial de G, sigui m l'enter estrictament positiu més petit tal que $x^m \in H$. Volem veure $H = \langle x^m \rangle$. Clarament, $\langle x^m \rangle \subset H$ (tota potència d'$x \in H$ es troba en H perquè l'operació és tancada). Sigui ara $x^\ell \in H$; hem de veure que $x^\ell \in \langle x^m \rangle$, per demostrar l'inclusió. Fem la divisió entera $x^\ell = x^{mq+r} = (x^m)^q + x^r$ que implica $x^r = x^l(x^m)^{-q} \in H$. Per l'elecció de m (l'element *més petit* tal que $x^m \in H$), ha de ser $r = 0$ i, per tant:

$$x^\ell = (x^m)^q \in \langle x^m \rangle. \tag{1.8.4}$$

Hem obtingut, doncs, $H = \langle x^m \rangle$; en particular, que H és cíclic. ■

Proposició 1.8.13. *Si G és un grup cíclic d'ordre n, per a cada divisor d de n existeix un únic subgrup de G d'ordre d.*

Demostració. Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n ($|G| = n$) i d un divisor de n. Un subgrup d'un grup cíclic G és cíclic, 1.8.12, i és d'ordre d si està generat per un element d'ordre d. Per 1.8.9, $x^{\frac{n}{d}}$ té ordre d i $\langle x^{\frac{n}{d}} \rangle$ és subgrup de G d'ordre d. De nou per 1.8.9, els elements de G que tenen ordre d són els x^k amb $\frac{n}{\text{mcd}(n,k)} = d$, és a dir, són els x^k amb k múltiple d'$\frac{n}{d}$ ($k = \ell\frac{n}{d}$ per algun ℓ). Per tant,

$$x^k = (x^{\frac{n}{k}})^\ell \in \langle x^{\frac{n}{d}} \rangle. \tag{1.8.5}$$

Com hem vist, tots aquests elements estan continguts en el subgrup $\langle x^{\frac{n}{d}} \rangle$. Per tant, aquest subgrup és l'únic d'ordre d. ■

Proposició 1.8.14. *Un grup d'ordre parell ha de contenir un element d'ordre 2.*

Demostració. Prenem qualsevol grup G d'ordre n i intentem emparellar els elements de G amb les seves inverses. Suposem que podem formar m parelles, és a dir, alliberem $2m$ elements. Els elements restants són de la forma $g = g^{-1}$ o $g^2 = e$; aquests inclouen el neutre i tots els elements d'ordre 2. Aleshores, hi ha d'haver $n - 2m - 1$ elements d'ordre 2. Si n és parell, $n - 2m - 1$ és senar i no pot ser zero: hi ha un element d'ordre 2 en G. ■

1.9 Subgrup generat per un conjunt

Definició 1.9.1 (Subgrup generat per S). Sigui G un grup, S un subconjunt de G. Definim el subgrup de G generat per S, que indicarem per $\langle S\rangle$, com la intersecció de tots els subgrups de G que contenen S. Si H és subgrup de G i $H = \langle S\rangle$, direm que S és un conjunt (o sistema) de generadors de H. Clarament $\langle\emptyset\rangle = \{e\}$.

Proposició 1.9.2. *El subgrup de G generat per un subconjunt no buit S de G és el conjunt de tots els elements de la forma*

$$x_1^{n_1} \dots x_r^{n_r}, \tag{1.9.1}$$

on r és un enter positiu, $x_1, \dots, x_r$ són elements de S i $n_1, \dots, n_r \in \mathbb{Z}$.

Demostració. Tot subgrup de G que contingui S ha de contenir els elements de la forma $x_1^{n_1} \cdots x_r^{n_r}$ i el conjunt de tots els elements $\{x_1^{n_1} \cdots x_r^{n_r}\}$ és, en efecte, subgrup de G. ■

Definició 1.9.3 (Subgrup finitament generat). Si S és conjunt finit, $S = \{x_1, \dots, x_r\}$, posarem $\langle x_1, \dots, x_r\rangle$ en comptes de $\langle\{x_1, \dots, x_r\}\rangle$ i direm que $\langle x_1, \dots, x_r\rangle$ és el subgrup de G generat per $x_1, \dots, x_r$. Direm que un grup G és finitament generat si existeix un subconjunt finit S de G tal que $\langle S\rangle = G$.

Exemple 1.9.4. $\langle t_i\rangle = \{\mathrm{Id}, t_i\}$, per a $i = 1, 2, 3$; $\langle s_1\rangle = \langle s_2\rangle = \{\mathrm{Id}, s_1, s_2\}$; $\langle t_1, s_1\rangle = S_3$.

Observació 1.9.5. Clarament, un grup finit és finitament generat però no recíprocament. Per exemple, $\mathbb{Z}$ és infinit i finitament generat.

Proposició 1.9.6. *Si S és un subconjunt d'un grup G i es compleix $ySy^{-1} \subset \langle S\rangle$, per a tot $y \in G$, aleshores $\langle S\rangle$ és subgrup normal de G.*

Demostració. Qualsevol element de $\langle S\rangle$ és de la forma $x_1^{n_1} \dots x_r^{n_r}$, amb $x_1, \dots, x_r$ elements de S. Tenim

$$y\,(x_1^{n_1} \dots x_r^{n_r})\,y^{-1} = \left(yx_1y^{-1}\right)^{n_1} \cdots \left(yx_ry^{-1}\right)^{n_r} \tag{1.9.2}$$

i, per hipòtesi, $yx_1y^{-1}, \dots, yx_ry^{-1}$ són elements de $\langle S\rangle$. Per tant, el seu producte també i obtenim $y\langle S\rangle y^{-1} \subset \langle S\rangle$, per a tot y de G, que dóna que $\langle S\rangle$ és subgrup normal de G. ■

Exercici 1.9.7. *Demostreu que S_n admet els sistemes de generadors següents:*

1. $(1,2), (1,3), \dots, (1,n)$.

2. $(1,2),(2,3),\ldots,(n-1,n)$.
3. $(1,\ldots,n),(1,2)$.

Demostració.

- Assignem $A=(1,2),(1,3),\ldots,(1,n)$. Els elements de la forma (i,j) generen S_n i podem escriure (i,j) com a $(1,i)(1,j)(1,i)$.
- Podem escriure un n-cicle $(1,\ldots,n)$ com a producte d'n transposicions, $(1,2),(2,3),\ldots,(n-1,n)$. També, $(1,j)=(1,j-1)(j-1,j)(1,j-1)$.
- El procés inductiu en aquest cas, és el següent: $(j,j+1)=(1,\ldots,n)^{n-k}(1,2)(1,\ldots,n)^k$ i $k=n-j-1$. Anem substituint aquí, progressivament, fins a obtenir la igualtat.

■

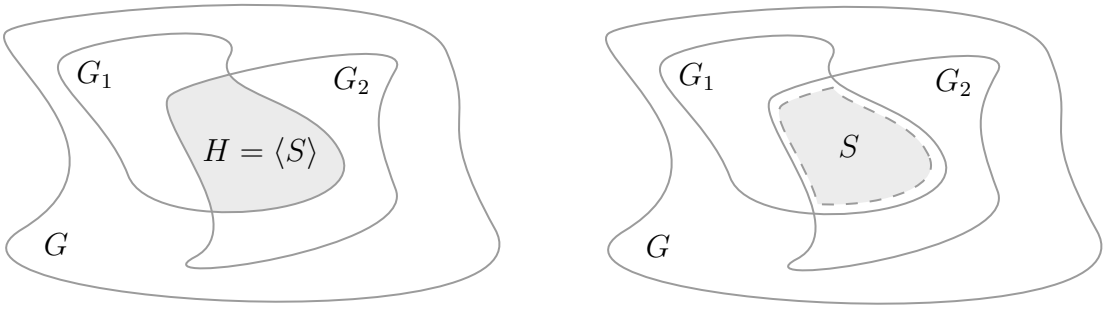


Figura 1.5: Representació d'un subgrup generat per un subconjunt

1.10 Producte directe de grups

Si G_1 i G_2 són grups, en el producte cartesià $G_1\times G_2$, podem definir una operació binària interna, component a component, per:

$$(x_1,x_2)\,(y_1,y_2)=(x_1y_1,x_2y_2)\,. \tag{1.10.1}$$

És immediat veure que $G_1\times G_2$ amb aquesta operació és grup, l'element neutre és (e_1,e_2) (on e_1 és l'element neutre de G_1 i e_2 el de G_2) i $(x_1,x_2)^{-1}=\left(x_1^{-1},x_2^{-1}\right)$. Diem que $G_1\times G_2$ amb aquesta operació és el producte directe de G_1 i G_2. Les aplicacions

$$\begin{array}{rccc} i_1: & G_1 & \longrightarrow & G_1\times G_2 \\ & x_1 & \longmapsto & (x_1,e_2) \end{array} \qquad \begin{array}{rccc} i_2: & G_2 & \longrightarrow & G_1\times G_2 \\ & x_2 & \longmapsto & (e_1,x_2) \end{array} \tag{1.10.2}$$

són monomorfismes de grup i les aplicacions:

$$\begin{array}{rccc} \pi_1: & G_1\times G_2 & \longrightarrow & G_1 \\ & (x_1,x_2) & \longmapsto & x_1 \end{array} \qquad \begin{array}{rccc} \pi_2: & G_1\times G_2 & \longrightarrow & G_2 \\ & (x_1,x_2) & \longmapsto & x_2 \end{array} \tag{1.10.3}$$

són epimorfismes de grups, i $\ker(\pi_1)=\{(e_1,x_2)\mid x_2\in G_2\}=\{e_1\}\times G_1$ i $\ker(\pi_2)=\{(x_1,e_2)\mid x_2\in G_1\}=G_1\times\{e_2\}$, respectivament. Clarament, si G_1 i G_2 són abelians, $G_1\times G_2$ també ho és.

Observació 1.10.1. En el cas de les aplicacions i_1 i i_2, $\mathrm{im}(i_1) = \{(x_1, e_2) \mid x_1 \in G_1\}$ i $\mathrm{im}(i_2) = \{(e_1, x_2) \mid x_2 \in G_2\}$. A més, $\mathrm{im}(i_1) \simeq G_1$ i $\mathrm{im}(i_2) \simeq G_2$.

Proposició 1.10.2. *Siguin G_1 i G_2 grups cíclics d'ordres n_1 i n_2, respectivament. El producte directe $G_1 \times G_2$ és cíclic si i només si n_1 i n_2 són primers entre ells. En aquest cas, si x_1 és un generador de G_1 i x_2 és un generador de G_2, $\langle (x_1, x_2) \rangle$ és un generador de $G_1 \times G_2$.*

Demostració. Per a $(x_1, x_2) \in G_1 \times G_2$, es compleix

$$\mathrm{ord}\,(x_1, x_2) = \mathrm{mcm}\,(\mathrm{ord}\,x_1, \mathrm{ord}\,x_2)\,, \tag{1.10.4}$$

ja que, per a un enter natural n, $(x_1, x_2)^n = (x_1^n, x_2^n) = (e_1, e_2) \iff x_1^n = e_1$ i $x_2^n = e_2 \implies \mathrm{ord}\,x_1 \mid n$ i $\mathrm{ord}\,x_2 \mid n$.

$$(x_1, x_2)^{\mathrm{mcm}(\mathrm{ord}(x_1), \mathrm{ord}(x_2))} = (e_1, e_2). \tag{1.10.5}$$

Definim $n_1 = \mathrm{ord}(x_1)$ i $n_2 = \mathrm{ord}(x_2)$. Per tant, si $\mathrm{mcd}\,(n_1, n_2) = 1$ i $G_1 = \langle x_1 \rangle, G_2 = \langle x_2 \rangle$, aleshores (x_1, x_2) és un element de $G_1 \times G_2$ que té ordre $n_1 n_2 = |G_1 \times G_2|$ i $G_1 \times G_2$ és cíclic. En aquest cas, $G_1 \times G_2 = \langle (x_1, x_2) \rangle$. Si $\mathrm{mcd}\,(n_1, n_2) \neq 1, G_1 \times G_2$ no pot tenir cap element d'ordre igual a $n_1 n_2$. ■

Definició 1.10.3 (Producte directe de $G_1 \times \cdots \times G_r$). Generalitzant, si $G_1, \ldots, G_r$ grups en el producte cartesià $G_1 \times \cdots \times G_r$ definim la operació binària interna per $(x_1, \ldots, x_r)(y_1, \ldots, y_r) = (x_1 y_1, \ldots, x_r y_r)$. $G_1 \times \cdots \times G_r$ és grup:

1. l'element neutre és $(e_1, \ldots, e_r)$ (on e_i és l'element neutre de G_i, $1 \leq i \leq r$),
2. existeix l'element invers $(x_1, \ldots, x_r)^{-1}$ definit per $(x_1^{-1}, \ldots, x_r^{-1})$.

Diem que $G_1 \times \cdots \times G_r$ és el producte directe de $G_1, \ldots, G_r$.

Donats un grup G i dos subgrups H_1, H_2 de G:

$$\begin{array}{rccc} f: & H_1 \times H_2 & \longrightarrow & G \\ & (h_1, h_2) & \longmapsto & h_1 h_2 \end{array} \tag{1.10.6}$$

1. $\mathrm{im}(f) = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\} = H_1 H_2$. f és exhaustiva si, i només si, $H_1 H_2 = G$.
2. Per comprovar que f és morfisme, siguin (h_1, h_2) i $(h_1', h_2') \in H_1 \times H_2$. Aleshores:

$$\left.\begin{array}{c} f((h_1 h_2)(h_1' h_2')) = f(h_1 h_1', h_2 h_2') = h_1 h_1' h_2 h_2' \\ f(h_1 h_2) f(h_1' h_2') = h_1 h_2 h_1' h_2' \end{array}\right\} \iff h_1' h_2 = h_2 h_1',\ \forall h_1' \in H_1, h_2 \in H_2. \tag{1.10.7}$$

   Per tant, f és morfisme si, i només si, tot element de H_1 commuta amb tot element d'H_2.
3. Si f és morfisme, $\ker(f) = \{(h_1, h_2) \in H_1 \times H_2 \mid h_1 h_2 = e\}$. Si $h_1 h_2 = e$, podem posar que $h_1 = h_2^{-1} \in H_1$ i $h_2 = h_1^{-1} \in H_2$ i reescriure el conjunt com $\{(h, h^{-1}) \mid h \in H_1 \cap H_2\}$. Per tant, f és injectiva si, i només si, $H_1 \cap H_2 = \{e\}$.

Definició 1.10.4 (Producte directe intern). Si f està definida com (1.10.6) i és isomorfisme, diem que G és producte directe intern de $H_1 \cap H_2$. Equivalentment, si es compleixen les tres condicions següents:

1. $G = H_1H_2$ (és morfisme exhaustiu);
2. per a tot $h_1 \in H_1$ i tot $h_2 \in H_2$ es compleix que $h_1h_2 = h_2h_1$ (és morfisme);
3. $H_1 \cap H_2 = \{e\}$ (és morfisme injectiu).

Si G és producte directe intern dels subgrups H_1 i H_2, aleshores H_1 i H_2:

$$\begin{array}{l} H_1 \simeq \{(h_1, e_2) \mid h_1 \in H_1\} \text{ subgrup normal d'} H_1 \times H_2, \\ H_2 \simeq \{(e_1, h_2) \mid h_2 \in H_2\} \text{ subgrup normal d'} H_1 \times H_2; \end{array} \tag{1.10.8}$$

en altres paraules, H_1, H_2 són normals en G ja que $H_1 \times \{e_2\}$ i $\{e_1\} \times H_2$ són normals en $H_1 \times H_2$ i H_1 i H_2 són les imatges de $H_1 \times \{e_2\}$ i $\{e_1\} \times H_2$ per l'isomorfisme f de $H_1 \times H_2$ en G.

1.11 Grups definits per generadors i relacions

En aquesta secció presentem el concepte de grup definit per generadors i relacions. Una presentació totalment rigorosa d'aquest concepte exigeix el coneixement de grups lliures generats per un conjunt. L'estudiant interessat pot consultar l'apèndix.

Definició 1.11.1 (Relació entre elements)**.** Sigui G un grup generat per un conjunt finit $S = \{x_1, \ldots, x_n\}$, és a dir, $G = \langle x_1, \ldots, x_n \rangle$. Una relació entre els elements de S és una igualtat del tipus

$$x_1^{k_1} \ldots x_n^{k_n} = e, \text{ on } k_1, \ldots, k_n \in \mathbb{Z}. \tag{1.11.1}$$

Exemple 1.11.2. Considerem el grup S_3 i el sistema de generadors $\{t_1, s_1\}$, on $t_1 = (2,3), s_1 = (1,2,3)$. Aleshores $t_1^2 = \mathrm{Id}, s_1^3 = \mathrm{Id}, t_1s_1t_1s_1 = \mathrm{Id}$ són relacions entre els generadors t_1, s_1 de S_3.

Definició 1.11.3 (Grup definit pels generadors)**.** Si G és un grup i S és un sistema de generadors d'un grup finit G i R és un conjunt de relacions entre els elements de S, direm que G està definit pel conjunt de generadors S i les relacions R si totes les relacions entre els elements de S es dedueixen de les del conjunt R. Si G és un grup finit definit pel conjunt de generadors S i el conjunt de relacions R, aleshores, tenint en compte les relacions de R, podem fixar una única manera d'escriure cada element de G en funció dels generadors i podem escriure també el producte de dos elements de G a partir de les relacions de R.
En altres paraules, en aquest cas, si G és un grup finit definit pel conjunt de generadors S i el conjunt de relacions R a partir de R i S podem escriure els elements de G i la taula del producte de G.

$$G = \langle S \mid R \rangle. \tag{1.11.2}$$

Exemple 1.11.4. El grup S_3 és el grup definit pels generadors t_1, s_1 i les relacions $t_1^2 = e, s_1^3 = e, t_1s_1t_1s_1 = e$. En efecte a partir d'aquestes relacions, tenim $t_1s_1 = s_1^{-1}t_1^{-1} = s_1^2t_1$ i, per tant, els elements del grup són $e, t_1, s_1, s_1t_1, s_1^2, s_1^2t_1$. Ara, les relacions ens donen també com s'operen els elements. Per exemple, $(s_1t_1)(s_1^2t_1) = s_1(t_1s_1)s_1t_1 = s_1(s_1^2t_1)s_1t_1 = s_1^3t_1s_1t_1 = (t_1s_1)t_1 = (s_1^2t_1)t_1 = s_1^2t_1^2 = s_1^2$. Posem $S_3 = \langle t_1, s_1 / t_1^2 = e, s_1^3 = e, t_1s_1t_1s_1 = e \rangle$ per indicar que S_3 està definit pels generadors t_1, s_1 i les relacions $t_1^2 = e, s_1^3 = e, t_1s_1t_1s_1 = e$.

Exemple 1.11.5. El grup cíclic $C_n = \langle x \mid x^n = e \rangle$ és un grup definit pels generadors. Al seu torn, si agafem $C_2 = \langle a \mid a^2 = e \rangle = \langle b \mid b^2 = e \rangle$:

$$G = \langle a, b \mid a^2 = e, b^2 = e, ab = ba \rangle = C_2 \times C_2 = \{e, a, ab\} \iff (ab)^2 = a(ba)b = a^2b^2 = e. \tag{1.11.3}$$

També tenim que:

$$G = \langle a, b \mid a^4 = e, b^2 = e, bab = a^3 \rangle = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\} \quad \begin{cases} ab = ba^3 \\ a^2b = a(ab) = aba^3 = ba^6 = ba^2 \end{cases} \tag{1.11.4}$$

1.12

Grups resolubles

Definició 1.12.1 (Grup resoluble)**.** Un grup G és resoluble si existeix una cadena finita de subgrups de G de la següent forma: comença amb el trivial i cadascun està inclòs en el següent i cadascun d'ells compleix que cadascun és normal amb el següent i els quocients són abelians:

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,\ i = 0 \div n - 1. \tag{1.12.1}$$

1. G_i és normal en G_{i+1},
2. G_{i+1}/G_i és abelià.

Una successió de grups es diu que és una *torre normal* si compleix la primera propietat i és una *torre abeliana* si compleix la segona propietat. És *resoluble* si és una torre abeliana l'últim subgrup de la qual és el neutre (és a dir, que $G_0 = \{e\}$, el subgrup trivial de G).

Exemple 1.12.2.

1. G és abelià implica que G és resoluble. Els quocients de grups abelians és abelià i cada G_i és normal en G_{i+1}, ja que tot subgrup d'un grup abelià és normal.
2. S_3 és resoluble: $\{e\} \subset A_3 \subset S_3$. En aquest cas, els dos quocients són cíclics i, en particular, abelians.
3. S_4 és resoluble. $S_4/A_4 \simeq C_2$ i prenem el grup de Klein $V_4 = \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ i es pot veure que és normal a S_4. En particular, podem fer el conjugat de cadascun d'aquests elements per una permutació qualsevol de manera que les seves imatges per aquesta permutació (una bijecció) són tots diferents i ens torna a caure en V_4:

   $$\sigma(1,2)(3,4)\sigma^{-1} = (\sigma(1), \sigma(2))(\sigma(3), \sigma(4)) \in V_4. \tag{1.12.2}$$

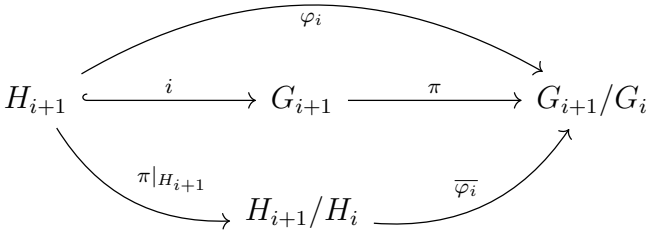
   A més, aquest V_4 és abelià (i no cíclic): tots els elements excepte el neutre tenen ordre 2. Calculant l'ordre del quocient A_4/S_4, és a dir, $|A_4/S_4| = \frac{|A_4|}{|V_4|} = \frac{12}{4} = 3$. Com que 3 és primer, hi ha només un subgrup d'ordre 3 (concretament la identitat), així que C_3 és isomorf a A_4/V_4.

Proposició 1.12.3.

1. *Tot subgrup d'un grup resoluble és resoluble.*
2. *Tot quocient d'un grup resoluble per un subgrup normal és resoluble.*
3. *Si G és grup i H subgrup normal de G tal que H i G/H són grups resolubles, aleshores G és resoluble.*

Demostració.

1. Si G és resoluble, per definició $\exists G_0 = \{e\} \subset G_1 \subset \cdots \subset G_n = G$ amb G_i normal a G_{i+1} i G_{i+1}/G_i, aleshores sigui H subgrup de G. Posem $H_i = G_i \cap H$, amb $H_i \subset H_{i+1}$. Considerem el següent diagrama:



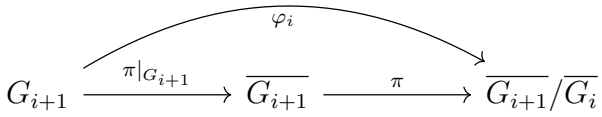
$$\begin{aligned} \ker(\varphi_i) = H_{i+1} \cap G_i = (H \cap G_{i+1}) \cap G_i = H \cap G_i = H_i \implies H_i \lhd H_{i+1} \\ \varphi_i \text{ factoritza a través de } H_{i+1}/H_i \text{ i } \overline{\varphi_2} : H_{i+1}/H_i \longrightarrow G_i/G_{i+1}. \end{aligned} \tag{1.12.3}$$

   - Per 1.5.8, $\ker(\varphi_i) \lhd H_{i+1}$; així doncs, $H_i \lhd H_{i+1}$.
   - $\overline{\varphi_i}$ és injectiu pel teorema d'isomorfia: sigui $[x] \in H_{i+1}/H_i$ tal que, en concret, $[x] \in \ker(\overline{\varphi_i})$. Aleshores, $\overline{\varphi_i}([x]) = \varphi_i(x) = \overline{e}$, on $\overline{e}$ és el neutre en G_{i+1}/G_i. Prenent $x \in \ker(\varphi_i) = H_i$, $[x]$ és la classe del neutre en H_{i+1}/H_i: $\overline{\varphi_i}([x]) = \varphi_i(x) = \overline{e}$.
   - Així, H_{i+1}/H_i és isomorf a $\operatorname{im}(\overline{\varphi_i}) \subset G_{i+1}/G_i$ abelià (ja que G és resoluble per hipòtesi), de manera que H_{i+1}/H_i és també abelià.

2. Sigui $\overline{G}$ el quocient de G per un subgrup normal, $\pi : G \longrightarrow \overline{G}$ és un morfisme de pas al quocient. $\overline{G_i} = \pi(G_i)$, amb $\overline{G_i} \subset \overline{G_{i+1}}$ i $\overline{G_n} = \overline{G}$.

$$\overline{G_i} \lhd \overline{G_{i+1}} \;\Big|\; \forall x \in G_i, \forall y \in G_{i+1}, G_i \lhd G_{i+1}, yxy^{-1} \in G_i \implies \overline{y}\;\overline{x}\;\overline{y}^{-1} \in \overline{G_i} \tag{1.12.4}$$

   Per tant, considerem el següent diagrama un altre cop:



   Per tant, $G_i \subset \ker(\varphi_i)$; en particular, $G_{i+1}/\ker(\varphi_i)$ és isomorf a $\overline{G_{i+1}}/\overline{G_i}$. Així doncs, $G_i \subset \ker(\varphi_i) \subset G_{i+1}$ implica, per 1.6.5:

$$\begin{aligned} G_{i+1}/\ker(\varphi_i) \simeq \frac{G_{i+1}/G_i}{\ker(\varphi_i)/G_i} \text{ és abelià } (G_{i+1}/G_i \text{ abelià, } G \text{ és resoluble}) \\ \implies G_{i+1}/\ker(\varphi_i) \text{ abelià} \implies \overline{G_{i+1}}/\overline{G_i} \text{ abelià.} \end{aligned} \tag{1.12.5}$$

3. Sigui G un grup, H un subgrup normal de G tal que H i G/H són resolubles. Posem $\overline{G} = G/H$. Sigui

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = H \tag{1.12.6}$$

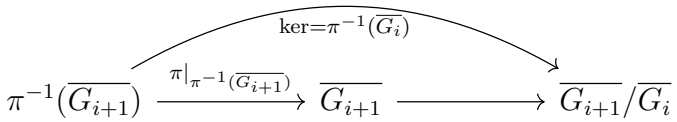
una torre abeliana de H i

$$\{\overline{e}\} = \overline{G}_0 \subset \overline{G}_1 \subset \cdots \subset \overline{G}_n = \overline{G} \tag{1.12.7}$$

una torre abeliana de $\overline{G}$. Sigui $\pi : G \longrightarrow \overline{G}$ el morfisme de pas al quocient. Considerem la torre de G. Sabem que $G_i = \pi^{-1}(\overline{G_i})$ és subgrup de G, $G_{i+1} = \pi^{-1}(\overline{G_{i+1}})$ és subgrup de G_{i+1}, $\pi^{-1}(\overline{G_0}) = \pi^{-1}(\overline{e}) = \ker(\pi) = H$ i $\pi^{-1}(\overline{G}) = G$:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = H = \pi^{-1}\left(\overline{G}_0\right) \subset \pi^{-1}\left(\overline{G}_1\right) \subset \cdots \subset \pi^{-1}\left(\overline{G}_n\right) = G. \tag{1.12.8}$$

Tenim $\overline{G}_i \lhd \overline{G}_{i+1}$ implica $\pi^{-1}\left(\overline{G}_i\right) \lhd \pi^{-1}\left(\overline{G}_{i+1}\right)$ i $\pi^{-1}\left(\overline{G}_i\right)$ és el nucli de la composició de $\pi : \pi^{-1}\left(\overline{G}_{i+1}\right) \longrightarrow \overline{G}_{i+1}$ amb el morfisme de pas al quocient $\overline{G}_{i+1} \longrightarrow \overline{G}_{i+1}/\overline{G}_i$.



Per tant pel primer teorema d'isomorfia, $\pi^{-1}\left(\overline{G}_{i+1}\right)/\pi^{-1}\left(\overline{G}_i\right) \simeq \overline{G}_{i+1}/\overline{G}_i$ és abelià. Hem provat doncs que $\overline{G_{i+1}}/\overline{G_i}$ és una torre abeliana de G i per tant G és resoluble.

■

1.13 Grups simples

Definició 1.13.1 (Grup simple)**.** Un grup G es diu simple si no té subgrups normals propis no trivials, és a dir, diferents de $\{e\}$ i G. Els grups S_3, A_4, S_4, D_{2n} no són simples.

Proposició 1.13.2. *Un grup no trivial és simple i resoluble si, i només si, és cíclic d'ordre primer.*

Demostració. Si G és simple i resoluble, l'única torre abeliana possible és $\{e\} \subset G$. Aleshores, G ha de ser abelià i, per tant tots els seus subgrups són normals. Com G és simple, $\{e\}$ i G són els seus únics subgrups. Com G és no trivial, G té un element x diferent de $\{e\}$ i ha de ser $\langle x\rangle = G$ (ja que el subgrup que genera ha de ser diferent del subgrup trivial, al ser un element diferent del neutre). Per veure que G és cíclic, si $\text{ord}(G) = \infty$, aleshores $\langle x^2\rangle \neq G$, però això no pot ser. Ara sabem que un grup cíclic d'ordre n té un subgrup d'ordre d per a cada divisor d de n. Per tant $|G|$ ha de ser primer, ja que solament té dos subgrups. Ara si G és cíclic d'ordre primer és clarament simple i $\{e\} \subset G$ és torre abeliana de G, per tant G és resoluble. ■

Hem vist que el grup alternat A_4 no és simple. El grup alternat A_3 és cíclic d'ordre 3, per tant simple. Volem veure ara que el grup alternat A_n és simple per a $n \geq 5$.

Proposició 1.13.3. *Sigui $n \geq 5$ un enter i sigui N un subgrup normal del grup alternat A_n. Si N conté un 3-cicle, aleshores $N = A_n$.*

Demostració. Si N conté un 3-cicle, podem suposar que és el cicle $(1,2,3)$. La relació

$$(3,2,j)(1,2,3)^2(3,2,j)^{-1} = (1,2,j), \quad 3 < j \leq n, \tag{1.13.1}$$

prova que N conté tots els 3 -cicles de la forma $(1,2,j)$, amb $j \geq 3$. Ara tenim

$$\begin{aligned} (1,i,j) &= (1,2,j)(1,2,i)^2, \quad i \neq j; i,j > 1 \\ (i,j,k) &= (1,i,j)(1,j,k), \quad i,j,k \text{ diferents i } > 1. \end{aligned} \tag{1.13.2}$$

■

Proposició 1.13.4. *El grup alternat A_n és simple si i només si $n \neq 4$.*

Demostració. En paraules textuals, *no és una demostració interessant.* Ja hem vist que A_3 és simple i A_4 no és simple. Hem de veure que A_n és simple per a $n \geq 5$. Sigui N un subgrup normal de $A_n, N \neq \{Id\}$. Per la proposició 1.13.3, n'hi ha prou amb veure que N conté un 3-cicle. Sigui x un element de $N, x \neq Id$. Aleshores, per a tot $t \in A_n$, tenim $z := txt^{-1}x^{-1} \in N$. Considerem la descomposició de x com a producte de cicles disjunts i raonem per casos.

1. Si en la descomposició de x com a producte de cicles disjunts hi ha només transposicions, n'hi ha d'haver al menys dues. Podem suposar $x = (1,2)(3,4)x'$, on x' és un producte de transposicions disjuntes de $(1,2)$ i $(3,4)$. Prenent $t = (2,3,4)$, obtenim $z = (1,4)(2,3) \in N$ i, després, si $u = (1,4,5)$, obtenim $uzu^{-1}z = (1,5,4) \in N$.
2. Si en la descomposició de x com a producte de cicles disjunts hi ha un únic 3-cicle, a més d'un cert nombre de transposicions, podem suposar $x = (1,2,3)x'$, amb x' producte de transposicions disjuntes de $(1,2,3)$. En aquest cas, $x^2 = (1,2,3)^2 = (1,3,2) \in N$.
3. Si en la descomposició de x com a producte de cicles disjunts hi ha al menys dos 3-cicles, podem suposar que $x = (1,2,3)(4,5,6)x'$, on x' és un producte de cicles disjunts de $(1,2,3)$ i de $(4,5,6)$. En aquest cas, prenent $t = (2,3,4)$, trobem $z = (1,4,2,3,5) \in N$, per tant N conté un 5-cicle. Per acabar, només cal veure que si en la descomposició de x com a producte de cicles disjunts hi ha un cicle d'ordre $n \geq 4$, aleshores N conté un 3-cicle.
4. Suposem $x = (1,2,\ldots,r)x'$, amb $r \geq 4$ i x' producte de cicles disjunts amb $(1,2,\ldots,r)$. Prenent $t = (1,2,3)$, trobem que $z = (1,2,4) \in N$.

■

Corol·lari 1.13.5. *El grup simètric S_n, amb $n \geq 5$, no és resoluble.*

Demostració. Si S_n fos resoluble, A_n seria resoluble. Com que A_n és simple si, i només si, $n \geq 5$, A_n seria cíclic d'ordre primer. Com que el cardinal d'A_n és $|A_n| = \frac{n!}{2} = 3 \cdot 4 \cdot 5 \cdots n$, no és primer per a $n \geq 5$. ■

Corol·lari 1.13.6. *Tot p-grup és resoluble.*

Demostració. Sigui $|G| = p^r$, amb $r \geq 0$. Si $r = 0$, G és el grup trivial i, per tant, resoluble; 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 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 $s < r$; així doncs, resoluble, per hipòtesi d'inducció. Obtenim que G és resoluble. ■

1.14

Grups diedrals

1.14.1 Introducció: conceptes geomètrics

Abans, val la pena introduir alguns conceptes de *Geometria Lineal*. En els apunts de l'assignatura els dona per sabuts, malauradament. Aquí se'n farà un petit recull seguint les meves notes, [Vil22], a les quals podeu accedir senceres consultant la *Bibliografia* d'aquest document.

Definició 1.14.1 (Simetria)**.** Sigui $\mathbb{L} = a + F \subset \mathbb{A}$ una varietat lineal. Suposem que G és un subespai suplementari d'F en E, $\dim F < n$, tal que $E = F \oplus G$. Un vector $u \in E$ descompondrà de manera única en una suma $u_F + u_G$ on cada sumand pertany al subespai que indica el subíndex. Definim la simetria d'eix $\mathbb{L}$ i direcció G com l'aplicació:

$$\begin{array}{rccl} s: & \mathbb{A} & \longrightarrow & \mathbb{A} \\ & p & \longmapsto & s(p) := a + \overrightarrow{ap_F} - \overrightarrow{ap_G}. \end{array} \tag{1.14.1}$$

Observació 1.14.2. Atès que per a qualsevol parella de punts p, q es té que

$$\overrightarrow{s(p)s(q)} = \overrightarrow{s(p)a} + \overrightarrow{as(q)} = \overrightarrow{pa_F} - \overrightarrow{pa_G} + \overrightarrow{aq_F} - \overrightarrow{aq_G} = \overrightarrow{pq_F} - \overrightarrow{pq_G}, \tag{1.14.2}$$

obtenim que s és una afinitat amb endomorfisme associat $\tilde{s}$ determinat per ser la identitat sobre F i $-\mathbb{I}$ sobre G. Dit d'una altra manera, $\tilde{s}$ diagonalitza amb VAPS 1 i -1, F és el subespai de VEPs de VAP 1 i G és el subespai de VEPS de VAP -1. Notem que tots els punts de l'eix $\mathbb{L}$ són fixos i que, per la mateixa definició, s^2 és la identitat en $\mathbb{A}$.

Definició 1.14.3 (Endomorfisme ortogonal)**.** Sigui E un espai vectorial amb un producte escalar. Es diu que un endomorfisme $f : E \longrightarrow E$ és ortogonal si $f(u) \cdot f(v) = u \cdot v, \forall u, v \in E$. Si f és ortogonal, aleshores preserva normes:

$$\|f(v)\| = \sqrt{f(v) \cdot f(v)} = \sqrt{v \cdot v} = \|v\|, \ \forall v \in E. \tag{1.14.3}$$

Definició 1.14.4 (Desplaçament)**.** Sigui $(\mathbb{A}, E)$ un espai afí euclidià. Una afinitat $f : \mathbb{A} \longrightarrow \mathbb{A}$ és un desplaçament si l'endomorfisme $\tilde{f} : E \longrightarrow E$ és ortogonal.

Sigui $f : \mathbb{A} \longrightarrow \mathbb{A}$ un desplaçament amb $\dim E = 2$. Llavors, $\tilde{f} \in O(E) \cong O(2)$.

1r cas $\det \tilde{f} = 1$. Llavors, $\tilde{f} \in SO(E)$. En qualsevol referència ortonormal, f s'expressa com:

$$\begin{pmatrix} x^* \\ y^* \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}. \tag{1.14.4}$$

1. Si $\alpha = 0$, f és una translació, o bé $f = \mathbb{I}$.
2. Si $\alpha \neq 0, \pi$, $\tilde{f}$ no té cap valor propi a $\mathbb{R}$ (en particular, no té VAP 1) i, per tant, f té un únic punt fix p. Llavors, f és una rotació de centre p i angle α. Aquestes afinitats són el·líptiques. Si prenem p com a origen del sistema de referència, aleshores f queda com:

$$\begin{pmatrix} x^* \\ y^* \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{1.14.5}$$

   El cas particular $\alpha = \pi$ correspon a una simetria central, i aleshores $\tilde{f} = -\mathbb{I}$.

2n cas $\det(\tilde{f}) = -1$. Llavors, $\tilde{f}$ té valors propis, i han de ser necessàriament ± 1, ja que $\tilde{f}$ és ortogonal. Si escollim una base e_1, e_2 de E amb $f(e_1) = e_1, f(e_2) = -e_2$ l'expressió de f és

$$\begin{pmatrix} x^* \\ y^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}, \quad x^* = x + a,\ y^* = -y + b. \tag{1.14.6}$$

Estudiem els punts fixos que compleixen $x = x + a$, $y = -y + b$:

1. Si $a = 0$, llavors $y = \frac{1}{2}b$ és una recta de punts fixos i f és una simetria axial (també es diu reflexió). f és una homologia general de raó -1 amb el feix de rectes invariants perpendicular a la recta de punts fixos.
2. Si $a \neq 0$, llavors f no té punts fixos. La recta $y = \frac{1}{2}b$ és invariant per f: $x^* = x + a$ i $y^* = -y + b$. f és composició d'una simetria axial amb una translació en la direcció de la recta invariant. Es diu que f és una reflexió amb lliscament. El vector de la translació és:

$$v = \frac{1}{2}\overrightarrow{pp^{**}}, p \text{ qualsevol.} \tag{1.14.7}$$

   A més, la recta invariant passa pel punt mitjà de p i p^* per a p arbitrari. Comprovem la descomposició de f en una reflexió i una translació:

$$\begin{pmatrix} 1 & 0 & a \\ 0 & -1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & b \\ 0 & 0 & 1 \end{pmatrix} \tag{1.14.8}$$

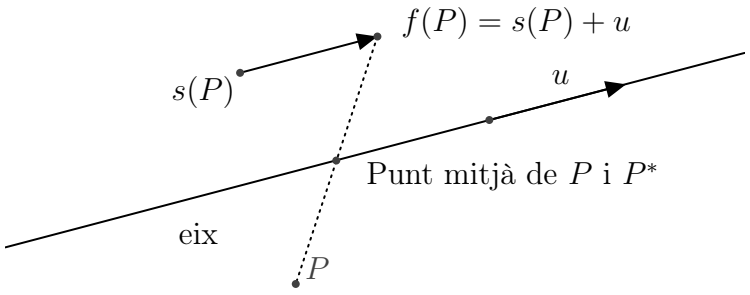


Figura 1.6: Simetria axial seguida d'una translació.

1.14.2 El grup diedral

El grup diedral D_{2n} és el grup de desplaçaments del pla que deixen invariant un polígon regular P de n costats ($n \geq 3$).
Un polígon regular té $2n$ simetries diferents: n simetries de rotació i n simetries de reflexió. Les rotacions i reflexions associades configuren el grup diedral D_{2n}. Si n és senar, cada eix de simetria connecta el punt mig d'una cara amb el vèrtex oposat. Si n és parell, hi ha $\frac{n}{2}$ eixos de simetria que connecten vèrtexs oposats. En qualsevol cas, hi ha n eixos de simetria i $2n$ elements al grup de simetria. Una reflexió respecte a un eix seguida d'una reflexió respecte a un altre eix resulta en una rotació d'angle doble que l'angle format pels eixos.
Si deixen invariant P, han de deixar fix el centre de simetria O de P, per tant són rotacions amb centre O o bé simetries amb eix passant per O. Un desplaçament que deixi P invariant ha de transformar un vèrtex de P en un altre vèrtex de P. Per tant les rotacions que deixen P invariant són les rotacions amb centre O i angle múltiple de $\frac{2\pi}{n}$ i les simetries que deixen P invariant són les simetries axials respecte d'un dels radis de P.

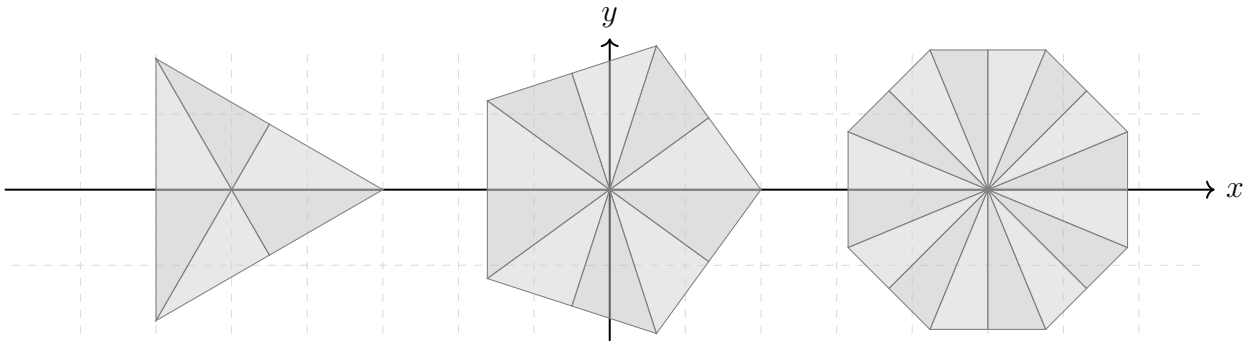


Figura 1.7: Si centrem el polígon regular a l'origen, llavors els elements del grup diedral actuen com a transformacions lineals del pla. El funcionament seria el mateix per a tots els n-gons; en particular, 3-gon, 5-gon i 8-gon que es mostren.

Podem escollir un sistema de referència ortonormal de forma que O sigui l'origen i el punt $(1, 0)$ un dels vèrtexs de P. Posem ρ la rotació d'angle $\frac{2\pi}{n}$ i centre O i σ la simetria axial respecte de l'eix de les x. En el sistema de referència escollit, les matrius de ρ i σ són

$$\begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.14.9}$$

Podem comprovar que es compleix $\rho^n = Id, \sigma^2 = \text{Id}$ i $\sigma\rho\sigma = \rho^{-1}$. A més, les rotacions de D_{2n} són les potències $\rho^k, 0 \leq k \leq n-1$, ja que ρ^k és la rotació de centre O i angle $2k\pi/n$. Ara si fem el producte $\rho\sigma$, obtenim

$$\begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & -\cos(\frac{2\pi}{n}) \end{pmatrix}. \tag{1.14.10}$$

La matriu obtinguda és de simetria axial. Calculem l'eix d'aquesta simetria. Posem $\alpha = \frac{2\pi}{n}$. L'equació

$$(\cos\alpha - 1)x + \sin\alpha y = 0 \tag{1.14.11}$$

té solució

$$\begin{aligned}(\sin\alpha, 1-\cos\alpha) &= \big(2\sin(\alpha/2)\cos(\alpha/2), 1-\big(\cos^2(\alpha/2)-\sin^2(\alpha/2)\big)\big)\\ &= \big(2\sin(\alpha/2)\cos(\alpha/2), 2\sin^2(\alpha/2)\big) = 2\sin(\alpha/2)(\cos(\alpha/2),\sin(\alpha/2))\end{aligned} \tag{1.14.12}$$

Per tant, $\rho\sigma$ és la simetria axial respecte de la recta que fa un angle de π/n amb l'eix de les x. Anàlogament, $\rho^k\sigma$ és la simetria axial respecte de la recta que fa un angle de $k\pi/n$ amb l'eix de les x. Obtenim doncs que totes les simetries de D_{2n} s'escriuen com $\rho^k\sigma, 0 \leq k \leq n-1$. Aleshores tenim que D_{2n} és generat per ρ i σ i que $D_{2n} = \{Id, \rho, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \ldots, \rho^{n-1}\sigma\}$ és un grup d'ordre $2n$.
Veiem ara que les relacions $\rho^n = Id, \sigma^2 = Id$ i $\sigma\rho\sigma = \rho^{-1}$ són suficients per definir el grup D_{2n}. Primer, d'aquestes relacions se segueix que els elements de D_{2n} són exactament els $2n$ elements escrits a dalt, ja que ρ té ordre n, σ té ordre 2 i $\sigma\rho = \rho^{n-1}\sigma$. Ara, pel producte, tenim

$$\begin{aligned}\rho^k\rho^l &= \rho^{k+l} \pmod n\\ \rho^k\left(\rho^l\sigma\right) &= \rho^{k+l} \pmod n\sigma\\ \left(\rho^k\sigma\right)\rho^l = \rho^k\left(\sigma\rho^l\right) &= \rho^k\left(\rho^{-l}\sigma\right) = \rho^{k-l} \pmod n\sigma\\ \left(\rho^k\sigma\right)\left(\rho^l\sigma\right) = \rho^k\left(\sigma\rho^l\right)\sigma &= \rho^k\left(\rho^{-l}\sigma\right)\sigma = \rho^{k-l} \pmod n\sigma^2 = \rho^{k-l} \pmod n\end{aligned} \tag{1.14.13}$$

Definició 1.14.5 (Grup diedral D_{2n}). Per tant D_{2n} és el grup generat per ρ i σ amb relacions $\rho^n = Id$, $\sigma^2 = Id$ i $\sigma\rho\sigma = \rho^{-1}$. Posem

$$D_{2n} = \left\langle \rho, \sigma \mid \rho^n = Id, \sigma^2 = Id, \sigma\rho\sigma = \rho^{-1} \right\rangle. \tag{1.14.14}$$

Observació 1.14.6. La següent taula de Cayley mostra l'efecte de la composició en el grup D_3 (les simetries d'un triangle equilàter). La rotació r_0 denota la rotació identitat; r_1 i r_2 denoten rotacions de 120º i 240º, respectivament, en sentit antihorari, i s_0, s_1 i s_2 denoten reflexions.

	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

Figura 1.8: Taula de Cayley de la composició en el grup D_3.

Teorema 1.14.7. *El grup diedral $D_{2\cdot 3}$ és isomorf a S_3. Per a $n > 3$, D_{2n} és subgrup propi de S_n.*

Demostració. Tornem a emfatitzar, podem numerar els vèrtexs de P en sentit antihorari, de forma que el vèrtex n-èsim sigui el punt $(1, 0)$ i definir una aplicació φ de D_{2n} en S_n que enviï

cada element de D_{2n} a la permutació que fa dels vèrtexs de P. Aleshores, φ és monomorfisme de grups. Per tant, podem identificar D_{2n} amb el subgrup $\varphi(D_{2n})$ de S_n. Tenim:

$$\begin{aligned}\varphi(\rho) &= (1,\dots,n),\\ \varphi(\sigma) &= \begin{cases}(1,n-1)(2,n-2)\cdots(\frac{n}{2}-1,\frac{n}{2}+1) & \text{si } n \text{ és parell}\\ (1,n-1)(2,n-2)\cdots(\frac{n-1}{2},\frac{n+1}{2}) & \text{si } n \text{ és senar}\end{cases}\end{aligned} \tag{1.14.15}$$

Tenim que $\varphi(D_{2n}) = \langle\varphi(\rho),\varphi(\sigma)\rangle$, obtenint el que volíem. ■

Exercici 1.14.8 (El grup dels quaternions). *Sigui H_8 el subgrup de $GL(2,\mathbb{C})$ generat per les matrius:*

$$Id, \quad \boldsymbol{i} := \begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}, \quad \boldsymbol{j} := \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}, \quad \boldsymbol{k} := \begin{pmatrix} 0 & i\\ i & 0\end{pmatrix}. \tag{1.14.16}$$

1. *Demostreu que H_8 és subgrup d'ordre 8 tal que Id és l'element neutre i es compleixen les igualtats $i^4 = Id$, $i^2 = j^2$ i $ij = ji^3$.*
2. *Calculeu l'ordre de cadascun dels elements d'H_8.*
3. *Demostreu que, si H és un grup definit pels generadors a, b i les relacions $a^4 = 1$, $a^2 = b^2$ i $ab = ba^3$, llavors H és isomorf a H_8.*

Demostració. Dividirem el nostre problema en els tres apartats separats que se'ns demanen:

1. Primerament, verificarem que es compleixen les igualtats que se'ns demanen. Notem que, demostrat $i^4 = Id$, $ij = ji^3$ es pot reescriure com $iji = j$, força més intuïtiva per calcular.

$$\begin{aligned}\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}^4 = \begin{pmatrix} i^2 & 0\\ 0 & (-i)^2\end{pmatrix}^2 = \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix} \quad (i^4 = Id)\\ \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}^2 = \begin{pmatrix} -(1)^2 & 0\\ 0 & -(1)^2\end{pmatrix} = \begin{pmatrix} i^2 & 0\\ 0 & (-i)^2\end{pmatrix} = \begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}^2 \quad (i^2 = j^2)\\ \begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix} = \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix} \quad (iji = j)\end{aligned} \tag{1.14.17}$$

   L'element neutre del grup dels quaternions és Id. Notem que $i^{-1} = -i$, $j^{-1} = -j$ i $k^{-1} = -k$; per tant, les inverses han de caure dins d'H_8 perquè sigui grup (existència de l'element invers). També ens falta $-Id$. Notem que $ij = k \in H_8$ i $ki = j \in H_8$.
2. L'ordre de la identitat és 1, per definició. $\text{ord}(i) = 4$ ja que no existeix cap potència més petita que ens doni la identitat. $\text{ord}(j) = \text{ord}(i) = 4$ a causa que $(i^2)^2 = (j^2)^2 = Id$. $\text{ord}(k) = 2$ donat que $k^2 = (ij)^2 = i^4 = Id$.
3. Com que $ij = k$, podem escriure k com a combinació lineal d'i, j. Com que el nombre d'elements generadors és el mateix i les relacions es corresponen, H és isomorf a H_8.

■

Exercici 1.14.9. *Calculeu tots els subgrups del grup dels quaternions H_8 i digueu quins són normals.*

Exercici 1.14.10. *Considerem el grup diedral D_{2n}:*

1. *Expliciteu tots els subgrups $D_{2\cdot 4}$ i digueu quins són normals.*
2. *Demostreu que D_{2n} té un subgrup normal d'ordre n que és cíclic.*
3. *Demostreu que $D_{2\cdot 3} \simeq S_3$.*

Demostració. Primerament, mostrem $D_{2\cdot 4}$ segons la definició 1.14.5:

$$D_{2\cdot 4} = \langle \sigma, \rho \mid \sigma^2 = Id, \rho^4 = Id, \sigma\rho\sigma = \rho^{-1} \rangle. \tag{1.14.18}$$

Pel teorema de Lagrange, sabem que els subgrups cal que siguin d'ordre 1, 2, 4 o bé 8.

1. Ordre 1: $\{Id\}$, que és un subgrup normal.
2. Ordre 2: $\{Id, \sigma\}, \{Id, \rho\sigma\}, \{Id, \rho^2\sigma\}, \{Id, \rho^3\sigma^2\}$ no són normals i $\{Id, \rho^2\}$ és normal.
3. Ordre 4: $\{Id, \rho, \rho^2, \rho^3\}$, $\{Id, \sigma, \rho, \sigma\rho^2\}$ i $\{Id, \sigma\rho, \rho, \sigma\rho^3\}$. Tots són d'índex 2 i, per tant, normals.
4. Ordre 8: $D_{2\cdot 4}$, que és un subgrup normal ja que és el total.

El segon apartat és molt més simple. Escollim qualsevol H subgrup tal que $H = \langle \rho \rangle$ i $|H| = n$.

$$|D_{2n}| = |H| \cdot [D_{2n} \cdot H] \iff 2n = n[D_{2n} : H] \iff [D_{2n} : H] = 2 \implies H \text{ és normal.} \tag{1.14.19}$$

En la última implicació hem usat un exercici on provàvem que si l'índex $[G : H] = 2$, H era normal. ■

Exercici 1.14.11. *Siguin n un nombre enter i d un divisor propi de n. Demostreu que el subgrup $\langle \rho^d \rangle$ de D_{2n} és subgrup normal i que el grup quocient és isomorf a D_{2d}.*

Demostració. Comencem amb un parell d'observacions. La primera és que, per a qualsevol rotació en un sistema de referència prou bo, podem fer $\rho^\ell \rho^d \rho^{-\ell} = \rho^d \in \langle \rho^d \rangle$. Al seu torn, tenim que $\sigma\rho\sigma = \rho^{-1}$, per a tota rotació ρ i qualsevol simetria σ. Ens val amb comprovar solament la propietat amb els generadors:

$$\sigma_i \rho^{d\ell} \sigma_i = (\rho^{d\ell})^{-1} = \rho^{n-d\ell} \in \langle \rho^d \rangle, \tag{1.14.20}$$

ja que $d \mid n$. ■

II

Accions d'un grup sobre un conjunt

2.1

Definicions

Definirem el que és una acció per l'esquerra i una acció per la dreta, separadament, i treballarem generalment amb accions per l'esquerra.

Definició 2.1.1 (Acció d'un grup per la dreta). 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 actua per la dreta en X, si existeix una acció $G \times X \longrightarrow X$, que escriurem $(g, x) \longmapsto x^g$, per a la qual se satisfan les dues propietats següents:

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

Definició 2.1.2 (Acció per l'esquerra d'un grup). Sigui S un conjunt i G un grup. Una acció de G sobre S és una aplicació:

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, s) & \longmapsto & g \cdot s \end{array} \tag{2.1.1}$$

Complint:

1. $g, h \in G$ tal que $(gh)s = g(hs)$, per a tot $g, h \in G$ i $s \in S$.
2. $eg = g$, per a tot $g \in G$.

Exemple 2.1.3. Podem definir $S_n \times \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ tal que $(\sigma, i) \longmapsto \sigma(i)$. Si tenim una acció $\varphi : G \times S \longrightarrow S$, per a $g \in G$, fix:

$$\begin{array}{rccc} \varphi_g : & S & \longrightarrow & S \\ & s & \longmapsto & g \cdot s \end{array} \tag{2.1.2}$$

és una aplicació bijectiva (és injectiva i exhaustiva clarament) i, per tant, podem definir una inversa $\varphi_{g^{-1}}$:

$$(\varphi_{g^{-1}} \circ \varphi_g)(s) = g^{-1}(g(s)) = g^{-1}(gs) = (g^{-1}g)s = es = s \implies \varphi_{g^{-1}} \circ \varphi_g = Id_S. \tag{2.1.3}$$

Observació 2.1.4. 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 gg' 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. 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.

Definició 2.1.5 (Permutació d'S). Diem permutació de S una bijecció d'S en S. El conjunt $\operatorname{Perm} S$ de permutacions de S és un grup amb la composició d'aplicacions.

$$\begin{array}{rccc} \Phi_g: & G & \longrightarrow & \operatorname{Perm} S \\ & g & \longmapsto & \varphi_g \end{array} \tag{2.1.4}$$

i Φ és un morfisme de grups, $\varphi_{gh} = \varphi_g \circ \varphi_h$.

$$\begin{gathered} \varphi_{gh}(s) = (gh)s \\ (\varphi_g \circ \varphi_h)(s) = \varphi_g(\varphi_h(s)) = g(hs). \end{gathered} \tag{2.1.5}$$

Recíprocament, si $\Phi : G \longrightarrow \operatorname{Perm} S$ és morfisme de grups, definim

$$\begin{array}{rccc} \rho: & G \times S & \longrightarrow & S \\ & (g,s) & \longmapsto & \Phi(g)(s) \end{array} \tag{2.1.6}$$

És acció de G sobre S ja que $\Phi(e) = Id$; per tant, $\Phi(e)(s) = s$ per a tot $s \in S$. Per a $g, g' \in G$ tenim $\Phi(gg') = \Phi(g) \circ \Phi(g')$ i per a $s \in S$,

$$\begin{aligned} (gg')s = \rho(gg', s) = \Phi(gg')(s) = (\Phi(g) \circ \Phi(g'))(s) = \Phi(g)(\Phi(g')(s)) \\ = \rho(g, \rho(g', s)) = g(g's). \end{aligned} \tag{2.1.7}$$

Com comentarem a continuació, donar una acció de G sobre S és, per tant, equivalent a donar un morfisme de grups de G en $\operatorname{Perm} S$. Si ρ és una acció d'un grup G en un conjunt S, diem que G *actua* o *opera* sobre S.

Observació 2.1.6. Donada una acció per l'esquerra d'un grup G en un conjunt X, $G \times X \longrightarrow X$, podem considerar una aplicació $\Phi : G \longrightarrow \operatorname{Bij}(X)$, de G en el conjunt de les aplicacions bijectives ($\operatorname{Perm}(X) \subset \operatorname{Bij}(X)$) del conjunt X en si mateix. D'aquesta manera, és equivalent considerar accions per l'esquerra del grup G en el conjunt X o bé considerar morfismes del grup G en el conjunt $\operatorname{Bij}(X)$.

Definició 2.1.7 (Acció fidel). Una acció de G en S es diu fidel si el morfisme de grups corresponent és injectiu. En general, diem *nucli de l'acció* el nucli del morfisme $G \longrightarrow \operatorname{Perm} S$ associat.

Definició 2.1.8 (Acció transitiva). Donada una acció ρ d'un grup G en un conjunt S, diem que ρ és transitiva o que G actua transitivament sobre S (mitjançant ρ) si per a tot parell d'elements s, s' de S, existeix un element g de G tal que $gs = s'$. Un subgrup de S_n es diu transitiu si opera transitivament sobre $\{1, 2, \ldots, n\}$.

Definició 2.1.9 (Òrbita d'una acció). Si $G \times S \longrightarrow S$ és una acció, $s \in S$, diem òrbita de S el conjunt $\{gs \mid g \in G\} = O_s$ (o Gs). L'estabilitzador de s és $E(s) = \{g \in G \mid gs = s\}$.

Lema 2.1.10. *Sigui S i $s \in S$, qualsevol. L'estabilitzador $E(s)$ és subgrup de G.*

Demostració. Clarament el neutre pertany a l'estabilitzador de S, $e \in E(s)$. Per veure que és una operació tancada: donats $g, h \in E(s)$, $(gh)s = g(hs) = gs = s \implies gh \in E(s)$. Ara, per veure l'existència d'element invers:

$$g \in E(s) \mid gs = s \implies g^{-1}(gs) = (g^{-1}g)s = g^{-1}s \implies g^{-1} \in E(s). \tag{2.1.8}$$

■

Definició 2.1.11 (Fix per l'acció)**.** Diem que $s \in S$ és fix per l'acció de G si $gs = s$, per a tot $g \in G$. Equivalentment, $O(s) = \{s\}$ o $E(s) = G$.

Proposició 2.1.12. *Donada una acció p de G sobre S, amb $s \in S$, l'aplicació:*

$$\begin{array}{ccc} G & \longrightarrow & S \\ g & \longmapsto & gs \end{array} \tag{2.1.9}$$

dona una bijecció del conjunt de classes per la dreta de G mòdul $E(s)$ en $O(s)$. Si G és finit, $|O(s)| \cdot |E(s)| = |G|$.

Demostració. Hem de veure que la imatge de l'aplicació és $O(s)$: $g, h \in S$ tenen la mateixa imatge per l'aplicació si. i només si:

$$gs = hs \iff h^{-1}(gs) = h^{-1}(hs) = s \iff h^{-1}g \in E(s) \iff g \in hE(s). \tag{2.1.10}$$

Veiem clarament que g cau a la classe d'equivalència per la dreta d'h sobre l'estabilitzador $E(s)$ si, i només si, tenen les mateixes imatges. Per tant, tenim una bijecció $G/E(s) \longleftrightarrow O(s)$.

$$|G/E(s)| = [G : E(s)] = \frac{|G|}{|E(s)|} = |O(s)|. \tag{2.1.11}$$

I ja hem acabat. ■

Proposició 2.1.13. *Sigui $\rho : G \times S \longrightarrow S$ una acció $s \in S$ i $g \in G$. Es compleix que $gE(s)g^{-1} = E(gs)$ per a tot $s \in S$ i tot $g \in G$.*

Demostració. Agafem $h \in E(gs)$.

$$\begin{aligned} h \in E(gs) \iff h(gs) = gs \iff g^{-1}(h(gs)) = (g^{-1}hg)s = g^{-1}(gs) = s \\ \iff g^{-1}hg \in E(s) \iff h \in gE(s)g^{-1}. \end{aligned} \tag{2.1.12}$$

Com que tot són equivalències, obtenim les igualtats directament. ■

Observació 2.1.14. Si $\rho : G \times S$ és una acció, es compleix $\ker(\rho) = \bigcap_{s \in S} E(s)$.

Exercici 2.1.15. *Considerem el subconjunt de* $\mathrm{GL}(3, \mathbb{Z}/3\mathbb{Z})$

$$G := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\}. \tag{2.1.13}$$

1. *Proveu que G és subgrup de $\mathrm{GL}(3,\mathbb{Z}/3\mathbb{Z})$ i determineu l'ordre de G.*
2. *Proveu que tots els elements de G diferents de la identitat tenen ordre 3.*
3. *Determineu si els subgrups de G*

$$H_1 := \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \text{ i } H_2 := \left\langle \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \tag{2.1.14}$$

   són normals.
4. *Determineu el centre de G.*

Demostració. Fixem-nos que G descriu un subconjunt de matrius triangulars superiors tal que el seu determinant és 1. El producte de matrius triangulars superiors és, en efecte, triangular superior (la operació és tancada), el neutre val per a $a = b = c = 0$ i té inversa (triangular superior, també) ja que és invertible.
L'ordre de G és el nombre d'elements que té el grup. En aquest cas, quantes matrius podem escriure?

$$\#\{\text{valors d'}a\} \cdot \#\{\text{valors de } b\} \cdot \#\{\text{valors de } c\} = 27. \tag{2.1.15}$$

L'ordre dels elements s'ha de determinar mitjançant la definició:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = Id \implies \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}c \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} = Id \tag{2.1.16}$$

On hem generalitzat la potència de la matriu triangular superior a aquesta forma, mitjançant inducció. Necessàriament, $a, b, c \in \overline{0}$ i l'ordre és 3.
Per veure si és normal, apliquem la definició (i ho passem pel *MatrixCalc*):

$$\begin{gathered} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies H_1 \lhd G,\ \forall a, b, c. \\ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies H_2 \not\lhd G,\ \forall c \notin \overline{0}. \end{gathered} \tag{2.1.17}$$

Per determinar el centre de G, volem saber quins parells de matrius són commutables quan les multipliquem. Siguin $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ i $a', b', c' \in \mathbb{Z}/n\mathbb{Z}$ els valors d'aquestes dues matrius. Necessitem:

$$b + ac' + b' = b + ca' + b' \iff ac' = ca' \text{ (ens val amb què } ac' \equiv a'c \bmod 3). \tag{2.1.18}$$

En particular, com que $b \in \mathbb{Z}/3\mathbb{Z}$ queda lliure obtenim, justament, $Z(G) = H_1$. ∎

2.2

Exemples d'accions

2.2.1 Acció per conjugació d'un grup sobre ell mateix

L'acció per conjugació d'un grup sobre ell mateix és:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & ghg^{-1} \end{array} \tag{2.2.1}$$

El nucli és $\{g \in G \mid ghg^{-1} = h, \forall h \in G\} \iff \{g \in G \mid gh = hg, \forall h \in G\}$. Es diu centre de G, es denota per $Z(G)$ i $Z(G) \lhd G$.

$$\begin{array}{c} E(h) = \{g \in G \mid ghg^{-1} = h\} = Z_G(h), \text{ centralitzador d'} h \text{ en } G. \\ O(h) = \{ghg^{-1} \mid g \in G\}, \text{ és la classe de conjugació d'} h. \end{array} \tag{2.2.2}$$

2.2.2 Acció per conjugació d'un grup sobre el conjunt dels seus subgrups

Sigui H subgrup de G. Sigui $g \in G$. El conjugat d'H per g és un subgrup de G tal que $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. L'acció per conjugació d'un grup sobre el conjunt dels seus subgrups és

$$\begin{array}{c} (gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1}. \\ (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}. \end{array} \tag{2.2.3}$$

En particular, gHg^{-1} és el conjugat d'H per G. Prenem $\mathscr{H} = \{H \mid H \text{ és subgrup de } G\}$.

$$\begin{array}{ccc} G \times \mathscr{H} & \longrightarrow & \mathscr{H} \\ (g,H) & \longmapsto & gHg^{-1} \end{array} \tag{2.2.4}$$

L'òrbita d'un subgrup H de G per aquesta acció és el conjunt dels seus conjugats. Els punts fixos per aquesta acció són els subgrups normals de G. $E(H) = \{g \in G \mid gHg^{-1} = H\}$ és el normalitzador d'H en G i el denotem per N_GH (evidentment, $H \lhd N_GH$, i $H \lhd N_GH \iff \forall g \in N_GH, gHg^{-1} = H$). *És el subgrup més gran de G que conté H com a subgrup normal.*

Exercici 2.2.1. *Sigui G un grup.*

1. *Proveu que, per a $x \in G$, l'aplicació $\varphi_x : G \longrightarrow G, y \mapsto xyx^{-1}$ és un automorfisme de grups.*
2. *Un subgrup H d'un grup G es diu característic si es compleix $\varphi(H) = H$ per a tot automorfisme φ de G. Proveu que un subgrup característic és un subgrup normal.*
3. *Proveu que $Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}$ és un subgrup característic de G.*
4. *Proveu que si H és subgrup característic de G, el seu normalitzador $N(H) = \{x \in G \mid xHx^{-1} \subset H\}$ també és un subgrup característic de G.*

Demostració. Com que φ_x és un endomorfisme, ens cal comprovar les condicions d'injectivitat i exhaustivitat per inferir que és un automorfisme i, en particular, un morfisme de grups.

- Per comprovar que és injectiu, provem que $\varphi_x(y) = \varphi_x(y') \implies y = y'$.

$$xyx^{-1} = xy'x^{-1} \iff x^{-1}xyx^{-1}x = x^{-1}xy'x^{-1}x \iff y = y'. \tag{2.2.5}$$

- Per comprovar que és exhaustiu, cal que $\mathrm{im}(\varphi_x) = G$. En efecte, $\mathrm{im}(\varphi_x) = \{z \in G \mid z = xyx^{-1}\} = \{z \in G \mid y = x^{-1}zx\} = \{y \in G \mid y = x^{-1}zx\} = G$ (també podríem argumentar que l'ordre de $\mathrm{im}(\varphi_x)$ coincideix amb el de G i $\mathrm{im}(\varphi_x) \subset G$; per tant, han de ser iguals).
- Cal que es conservin les operacions, és a dir, que es doni $\varphi_x(z)\varphi_x(y) = \varphi_x(zy)$:

$$\varphi_x(z)\varphi_x(y) = xzx^{-1} \cdot xyx^{-1} = xzyx^{-1} = \varphi_x(zy). \tag{2.2.6}$$

  Per tant, φ_x és un morfisme de grups.

Amb això, obtenim que és un automorfisme de grups.
Per altra banda, ens demanen demostrar que donat un subgrup invariant per φ, un automorfisme qualsevol, aquest ha de ser necessàriament normal. Un subgrup és normal si $xHx^{-1} = H$. Solament ho farem per l'automorfisme del primer apartat, tot i que s'hauria de provar per tot automorfisme:

$$H = \varphi(H) = xHx^{-1},\ \varphi_x(H) = \{xyx^{-1} \in G \mid y \in H\}. \tag{2.2.7}$$

$Z(G)$, en particular, compleix que $\ker(\varphi_x) = Z(G)$ i $Z(G) \triangleleft G$ (però la normalitat és una condició necessària i no pas suficient per ser subgrup característic).

$$\varphi(Z(G)) = Z(G) \iff \varphi(y) = y, \forall y \in Z(G) \xrightarrow{y \in Z(G)} \varphi(y) = xyx^{-1} = yxx^{-1} = y, \tag{2.2.8}$$

on hem usat que $y \in Z(G) \iff yz = zy, \forall z \in Z$ (i, en particular, per a $z = x$). Finalment, si H és subgrup característic també és normal en G, i $N(H) = G$ perquè és el subgrup més gran de G que conté H com a subgrup normal. Com $\mathrm{im}(\varphi) = G$ (és exhaustiva), $\varphi(G) = G$ i $N(H)$ és característic. ■

2.2.3 Accions per translació

Si H és un subgrup d'un grup G, podem considerar l'acció de H en G per translació a l'esquerra

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg. \end{array} \tag{2.2.9}$$

Observació 2.2.2. Siguin $h_1, h_2 \in H$ i $e \in H$. Notem que l'acció de translació per la dreta no és la mateixa de translació per l'esquerra, ja que la commutativitat no està assegurada.

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg. \end{array} \qquad \begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & gh. \end{array} \tag{2.2.10}$$

Si prenem (h_1h_2, g), aleshores clarament $g(h_1h_2) = (gh_1)h_2 \neq (gh_2)h_1$.

Més en general, si F és qualsevol subgrup de G, podem considerar l'acció per translació a l'esquerra de H sobre el conjunt quocient G/D_F de classes per la dreta de G mòdul F:

$$\begin{array}{rccc} \rho: & H \times G/D_F & \longrightarrow & G/D_F \\ & (h, gF) & \longmapsto & (hg)F. \end{array} \tag{2.2.11}$$

L'acció de G sobre G/D_F per translació a l'esquerra és transitiva. L'acció de H sobre G per translació a l'esquerra és fidel. Per a l'acció de H sobre G/D_F, el nucli és

$$H \cap \left(\bigcap_{g \in G} gFg^{-1} \right). \tag{2.2.12}$$

En efecte, posem $\varphi : H \longrightarrow \mathrm{Perm}\,(G/D_F)$ tal que $h \longmapsto \rho_h$. Tenim $\rho_h(gF) = (hg)F = gF \iff g^{-1}hg \in F \iff h \in gFg^{-1}$. Per tant, $\rho_h = \mathrm{Id}_{G/D_F} \iff h \in \bigcap_{g \in G} gFg^{-1}$.
Anàlogament per la dreta, la translació per la dreta d'H sobre G és

$$\begin{array}{ccc} (h, g) & \longmapsto & gh^{-1} \\ (h_1h_2, g) & \longmapsto & g(h_1h_2)^{-1} = (gh_2^{-1})h_1^{-1} \end{array} \tag{2.2.13}$$

F és subgrup de G i G/D_F classes per la dreta de G mòdul F.

$$\begin{array}{ccc} H \times G/D_F & \longrightarrow & G/D_F \\ (h, gF) & \longrightarrow & (hg)F \end{array} \tag{2.2.14}$$

I ens queda que $E(gF) = \{h \in H \mid hgF = gF\}$ i

$$hgF = gF \iff g^{-1}hgF = F \iff g^{-1}hg \in F \iff h \in gFg^{-1}. \tag{2.2.15}$$

Per tant, $E(gF) = H \cap gFg^{-1}$ i el nucli és $H \cap \bigcap_{g \in G} gFg^{-1}$. Aquesta última intersecció ($\bigcap_{g \in G}$) és sempre un subgrup normal: posem $\bigcap_{g \in G} gFg^{-1} = F_0$ i sel·leccionem $h \in G$, qualsevol. Aleshores:

$$hF_0f^{-1} = \bigcap_{g \in G} (hgF(hg)^{-1}) = \bigcap_{g \in G} gFg^{-1}. \tag{2.2.16}$$

2.3

Equacions d'òrbites

Donada una acció ρ d'un grup G en un conjunt S, la relació $s \sim t \iff t = gs$ per a algun $g \in G$ és una relació d'equivalència a S.

$$\left.\begin{array}{c} s \sim s \\ s \sim t \\ s \sim t \wedge t \sim u \end{array}\right\} \implies \left\{\begin{array}{c} s = es \\ t = gs \implies s = g^{-1}t \\ t = gs \wedge u = ht \implies u = (hg)s. \end{array}\right. \tag{2.3.1}$$

La classe d'un element $s \in S$ és la seva òrbita Gs. Per tant les òrbites formen una partició de S. Si posem S/G el conjunt d'òrbites, tenim

$$|S| = \sum_{O \in S/G} |O|. \tag{2.3.2}$$

En particular, si S és finit, i $S_0 \subset S$ és el conjunt de punts fixos per ρ, aleshores

$$|S| = |S_0| + \sum_{i=1}^{r} |O_i| \,, \tag{2.3.3}$$

on $\{O_1, \ldots, O_r\}$ és el conjunt d'òrbites amb més d'un element. Equivalentment:

$$|S| = |S_0| + \sum_{i=1}^{r} [G : E(x_i)] \,, \tag{2.3.4}$$

amb $x_i \in O_i, 1 \leq i \leq r$. Qualsevol de les relacions (2.3.3), (2.3.4) es diu equació d'òrbites. Veiem ara exemples d'aplicació de l'equació d'òrbites.

Proposició 2.3.1 (Equació de les classes)**.** *Si G és un grup finit, es compleix*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : Z_G(x_i)] \tag{2.3.5}$$

on $\{x_1, \ldots, x_r\}$ és un conjunt de representants de les classes de conjugació amb més d'un element.

Demostració. Considerem l'acció de G sobre ell mateix per conjugació. Aleshores $Z(G)$ és el conjunt de punts fixos, $Z_G(x_i)$ és l'estabilitzador de x_i i (2.3.4) dona la fórmula de l'enunciat. ■

Definició 2.3.2 (p-grup)**.** Si p és un nombre primer, un grup finit G s'anomena p-grup si $|G| = p^r$, per a algun r enter natural > 0.

Proposició 2.3.3 (Congruència dels punts fixos)**.** *Si G és un p-grup que opera sobre un conjunt finit S, aleshores*

$$|S| \equiv |S_0| \pmod{p} \tag{2.3.6}$$

Demostració. Si $x_i \in O_i$ de manera que O_i són òrbites amb més d'un element, és a dir, no és punt fix, $[G : E(x_i)]$ divideix $|G|$ i és > 1. Per tant, $[G : E(x_i)]$ és divisible per p. Ja sabem que $|S| - |S_0| = \sum_{i=1}^{r} [G : E(x_i)]$. Com que l'ordre de G és una potència de p per ser un p-grup, $[G : E(x_i)]$ és divisible per p. ■

Corol·lari 2.3.4. *Si G és un p-grup, el seu centre $Z(G)$ és no trivial.*

Demostració. $Z(G)$, els punts fixos per l'acció de G sobre G per conjugació, conté, per definició, al menys e. Per tant, $|Z(G)| \geq 1$. Per 2.3.2, obtenim $|Z(G)| \equiv |G| \pmod{p}$ i, per tant, $|G| \equiv 0 \pmod{p}$ i $p \mid |Z(G)|$. En concret, $|Z(G)| > 1$. ■

Corol·lari 2.3.5 (Congruència del normalitzador)**.** *Sigui H un p-subgrup d'un grup finit G. Aleshores*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}. \tag{2.3.7}$$

Demostració. Considerem l'acció de H en G/D_H per translacions per l'esquerra, és a dir

$$H \times G/D_H \longrightarrow G/D_H, \quad (h, gH) \longmapsto hgH. \tag{2.3.8}$$

Es dona que gH és fix si, i només si, tenim $hgH = gH$, per a tot $h \in H$. Si, i només si:

$$g^{-1}hg \in H \iff g^{-1}Hg = H \iff gHg^{-1} = H \iff g \in N_G(H),\ \forall h \in H. \tag{2.3.9}$$

Per tant, el conjunt de punts fixos és $N_G(H)/H$. ■

Teorema 2.3.6 (Teorema de Cauchy)**.** *Sigui G un grup finit d'ordre n i p un nombre primer que divideix n. Aleshores G té un element d'ordre p.*

Demostració. Sigui $S = \left\{(g_1, \ldots, g_p) \in G \times \overset{p}{\cdots} \times G \mid g_1 \cdots g_p = e\right\}$. Podem definir una acció de $S \times \mathbb{Z}/p\mathbb{Z}$ sobre S que corre els índexs k posicions:

$$(k, (g_1, \cdots, g_p)) \longmapsto (g_{k+1}, \ldots, g_{k+p}), \tag{2.3.10}$$

per a $k \in \mathbb{Z}/p\mathbb{Z}, (g_1, \ldots, g_p) \in S$, on la suma en els subíndexs es fa mòdul p. Com $\mathbb{Z}/p\mathbb{Z}$ és un p-grup i $|S| = n^{p-1}$ (g_p queda determinat per $g_1, \ldots, g_{p-1}$) és divisible per p, tenim que el cardinal del conjunt S_0 de punts fixos és divisible per p.

$$|S_0| \equiv |S| \pmod{p} \implies p \mid |S_0|. \tag{2.3.11}$$

El conjunt en qüestió és el següent:

$$S_0 = \{(x, \ldots, x) \mid x \in G, x^p = e\}. \tag{2.3.12}$$

Com $(e, \ldots, e) \in S_0$ i $p \mid |S_0|$, el conjunt S_0 ha de contenir algun $(x, \ldots, x) \in S_0$ amb $x \neq e, x \in G$. En particular, x és, doncs, element d'ordre p. ■

Exercici 2.3.7. *Calculeu totes les classes de conjugació del grup diedral $D_{2\cdot 4}$.*

2.4 Teoremes de Sylow

Sigui G un grup finit, p un nombre primer dividint $|G|$. Volem estudiar els p-subgrups de G. Els p-subgrups de G amb ordre la màxima potència de p dividint $|G|$ es diuen p-subgrups de Sylow de G. En particular, si G és grup d'ordre n i p primer amb $p \mid n$, diem p-subgrup de Sylow de G un subgrup de G d'ordre p^r amb $p^r \mid n$ i $p^{r+1} \nmid n$.

Teorema 2.4.1 (Primer teorema de Sylow)**.** *Sigui G un grup finit, p un nombre primer i $r > 0$ un nombre enter tals que p^r divideix $|G|$. Aleshores existeixen subgrups $H_1, \cdots, H_r$ de G tals que $|H_i| = p^i, 1 \leq i \leq r$, i $H_i \lhd H_{i+1}, 1 \leq i \leq r-1$. En particular, H_r és subgrup de Sylow.*

Demostració. Raonem per inducció. Si $r = 1$, és conseqüència directa del teorema de Cauchy 2.3.6. Seguim la inducció sobre r. Suposem que $r \geq 2$ i que existeixen subgrups $H_1, \ldots, H_{r-1}$ de G tals que $|H_i| = p^i$ i $H_i \lhd H_{i+1}$. Com $p \mid [G : H_{r-1}]$, per la congruència del normalitzador 2.3.5, tenim $p \mid [N_G(H_{r-1}) : H_{r-1}]$. Pel teorema de Lagrange, el grup quocient $N_G(H_{r-1})/H_{r-1}$ (on $H_{r-1} \lhd N_G(H_{r-1})$) té un subgrup divisible per p i, per 2.3.6 un altre cop, aquest és precisament p. La seva antiimatge per la projecció

$$\pi : N_G(H_{r-1}) \longrightarrow N_G(H_{r-1})/H_{r-1} \tag{2.4.1}$$

és un subgrup H_r de $N_G(H_{r-1})$ d'ordre p^r (ja que $[H_r : H_{r-1}] = p$) i tal que $H_{r-1} \lhd H_r$ (ja que $H_r \subset N_G(H_{r-1})$). ■

Corol·lari 2.4.2. *Si G es un grup finit i p un nombre primer dividint $|G|$, aleshores existeixen p-subgrups de Sylow de G.*

Corol·lari 2.4.3. *Tot p-grup és resoluble.*

Demostració. Si G és grup d'ordre p^r, amb p un nombre primer i $r > 0$ un nombre enter, pel primer teorema de Sylow, existeixen subgrups $H_1, \ldots, H_r$ de G tals que $|H_i| = p^i, 1 \leq i \leq r$, i $H_i \lhd H_{i+1}, 1 \leq i \leq r-1$. Tenim doncs que $\{e\} \subset H_1 \subset H_2 \subset \cdots \subset H_r = G$ és una torre abeliana i, per tant G és resoluble. Altrament ho podem raonar dient que $|H_{i+1}/H_i| = p$ i, per tant, que H_{i+1}/H_i és cíclic i, per tant, que són tot subgrups abelians; de manera que $H_0, \ldots, H_r$ formen una torre abeliana i G és, en efecte, resoluble. ■

Sigui H subgrup de G i $x \in G$, amb $|xHx^{-1}| = |H|$. Aleshores:

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & G \\ & y & \longmapsto & xyx^{-1} \end{array} \tag{2.4.2}$$

φ és un automorfisme de G i el conjugat d'un p-subgrup de Sylow de G es també p-subgrup de Sylow de G. Veiem ara el recíproc.

Teorema 2.4.4 (Segon teorema de Sylow). *Siguin G un grup finit, H un p-subgrup de G i S un p-subgrup de Sylow de G, amb p primer. Aleshores existeix $x \in G$ tal que $H \subset xSx^{-1}$. En particular dos p-subgrups de Sylow de G són conjugats.*

Demostració. Considerem l'acció de H en G/D_S per translació a l'esquerra:

$$\begin{array}{ccc} H \times G/D_S & \longrightarrow & G/D_S \\ (h, gS) & \longrightarrow & hgS \end{array} \tag{2.4.3}$$

Per a tot element $gS \in G/D_S, g \in G$, l'estabilitzador de gS és el subgrup conjugat gSg^{-1}. Aleshores, mirem el conjunt de punts fixos per aquesta acció: si existeix algun punt fix, ja hem acabat. Donada una classe xS, tenim que xS queda fixa $\iff hxS = xS$:

$$\begin{aligned} gS \text{ punt fix} \iff hgS = gS \iff g^{-1}hgS = S \iff g^{-1}hg \in S \\ \iff h \in gSg^{-1} \iff H \subset gSg^{-1}, \forall h \in H. \end{aligned} \tag{2.4.4}$$

Per tant, el conjunt de punts fixos és $X_0 = \{xS \in G/D_S \mid H \subset xSx^{-1}\}$. Com que H és p-grup i $|G/D_S| = [G : S]$, la congruència de punts fixos 2.3.3 dona $|X_0| \equiv [G : S] \pmod p$. Com $p \nmid [G : S]$ (G/S és p-subgrup de Sylow), tenim $p \nmid |X_0|$ i, per tant, $|X_0|$ no és buit. ■

Corol·lari 2.4.5. *El grup G té un únic p-subgrup de Sylow S si, i només si, G té un p-subgrup de Sylow que és un subgrup normal.*

Demostració.

⇒ Suposem S p-subgrup de Sylow. Per veure que existeix un p-subgrup normal necessitem que es compleixi $S' = gS'g^{-1}$, la qual cosa és directa ja que, com tots els p-subgrups de Sylow de G són conjugats, en particular, com S és únic, S és conjugat de si mateix i $S = gSg^{-1}$.

⇐ Denotem per S el p-subgrup normal de Sylow, $S = gSg^{-1}$. Tornem a aplicar que per a tot p-subgrup de Sylow de G podem trobar el seu conjugat, $S = gS'g^{-1}$. Aleshores:

$$gSg^{-1} = gS'g^{-1} \iff S = S'. \tag{2.4.5}$$

Per tant, el p-subgrup de Sylow és únic.

■

Teorema 2.4.6 (Tercer teorema de Sylow)**.** *Sigui G un grup finit i n_p el nombre de p-subgrups de Sylow de G. Aleshores es compleix*

1. *$n_p = [G : N_G(S_p)]$, per a tot p-subgrup de Sylow S_p de G;*
2. *$n_p \mid [G : S_p]$, per a tot p-subgrup de Sylow S_p de G;*
3. *$n_p \equiv 1 \pmod p$.*

Demostració.

1. Pel segon teorema de Sylow 2.4.4, n_p és el cardinal de l'òrbita d'un p-subgrup de Sylow S_p per l'acció de G per conjugació sobre el conjunt dels subgrups de G. L'estabilitzador de S_p per a aquesta acció és $N_G(S_p)$, de manera que $n_p = [G : N_G(S_p)]$.
2. Ara $[G : S_p] = [G : N_G(S_p)]\,[N_G(S_p) : S_p]$, per tant, n_p divideix $[G : S_p]$, ja que $S_p \subset N_G \subset G$.

$$[G : S_p] = [G : N_G(S_p)]\,[N_G(S_p) : S_p] \iff \frac{|G|}{|S_p|} = \frac{|G|}{|N_G(S_p)|} \cdot \frac{|N_G(S_p)|}{|S_p|}. \tag{2.4.6}$$

   D'aquesta manera, $n_p \mid [G : S_p]$.
3. Sigui ara X el conjunt de p-subgrups de Sylow de G. Considerem l'acció de S_p en X per conjugació. Aleshores el conjunt de punts fixos és $X_0 = \{T \in X \mid xTx^{-1} = T, \forall x \in S_p\} = \{T \in X \mid S_p \subset N_G(T)\}$. Volem veure $X_0 = \{S_p\}$. En efecte, si $T \in X_0$, aleshores S_p i T són p-subgrups de Sylow de $N_G(T)$ i T és normal en $N_G(T)$. Com que $T \lhd N_G(T)$ implica que $N_G(T)$ té exactament un p-subgrup de Sylow, apliquem 2.4.5 i ens queda $T = S_p$ i $X_0 = \{S_p\}$. Com $|X| = n_p$ i $|X_0| = 1$, per la congruència dels punts fixos, 2.3.3, tenim $n_p \equiv 1 \pmod p$.

Amb tot, havent provat els tres apartats, ja hem acabat. ■

Observació 2.4.7 (Un aclariment sobre la demostració anterior)**.** Pel segon teorema de Sylow, tots els p-subgrups de Sylow de G són conjugats; això és, 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, $N_G(S)$.

Exercici 2.4.8. *Si l'ordre d'un grup G és 96, aleshores G no és simple.*

Demostració. Cal trobar un subgrup normal de G que no sigui ni el normal ni el total. Si trobem un p-subgrup de Sylow (un *únic* p-subgrup de Sylow) és normal i, per tant, ja hauríem acabat. Fem la factorització de $96 = 2^5 \cdot 3$ i obtenim que n_2 és $n_2 \mid 3$ i $n_2 \cong 1 \pmod 2$ i, per tant, $n_2 = 1$ o $n_2 = 3$. A la vegada, $n_3 \mid 2^5$ i $n_3 \cong 1 \pmod 3$ i $n_3 = 1, 4, 16$. Recordem que n_p és el nombre de p-subgrups de Sylow que tenim en G.

1. Si $n_2 = 1$, l'únic subgrup de Sylow és normal en G pel segon teorema de Sylow, $|S_2| = 2^5$ i S_2 és p-subgrup propi i no trivial. Per tant, G no és pas simple.
2. Si $n_2 = 3$, posem $X = \{2-\text{subgrups de Sylow}\} = \{H_1, H_2, H_3\}$. Considerem l'acció per conjugació ρ:
$$\begin{array}{rccc} \rho: & G \times X & \longrightarrow & X \\ \varphi: & G & \longrightarrow & \mathrm{Perm}(X) \simeq S_3. \end{array} \tag{2.4.7}$$
El subgrup φ no pot ser ni el trivial ni el total. Si $\ker(\varphi) = G$, aleshores $xH_1x^{-1} = H_1$ per a tot $x \in G$, que voldria dir que $H_1 \lhd G$ i això implicaria que només hi ha un p-subgrup, però hi ha tres per hipòtesi ($n_2 = 3$ implica que tenim H_1, H_2, H_3, com ja hem comentat); per tant, no pot ser el subgrup trivial. Tampoc pot ser el subgrup total: si $\ker(\varphi) = \{e\}$, pel primer teorema d'isomorfia tindríem que $G \simeq \mathrm{im}(\varphi) \subset S_3$ i $|G| \leq |S_3| = 6$, la qual cosa contradiu que $|G| = 96$. Així doncs, $\ker(\varphi)$ és subgrup normal de G diferent de $\{e\}$ i també de G: G no és simple.

■

Exercici 2.4.9. *Considerem G un grup tal que l'ordre de G és 3304.*

1. *Proveu que G té un subgrup normal H d'ordre 59.*
2. *Proveu que G té un subgrup d'ordre 413.*
3. *G/H no és simple.*
4. *G és resoluble.*

Demostració. Factoritzant, ens queda que $3304 = 2^3 \cdot 7 \cdot 59$. Un subgrup de G d'ordre 59 és un 59-subgrup de Sylow:

$$\left.\begin{array}{c} n_{59} \equiv 1 \pmod{59} \\ n_{59} \mid 56 \end{array}\right\} \implies n_{59} = 1 \xrightarrow{\text{segon teorema d'isomorfia}} \text{el 59-Sylow és normal en } G. \tag{2.4.8}$$

Considerem H el subgrup Sylow de G d'ordre 59. Factoritzem el 413 i obtenim $413 = 59 \cdot 7$. Si apliquem el teorema de Sylow obtenim que existeixen 7 subgrups de Sylow de G. Com que

7 divideix exactament l'ordre del grup G, aquests subgrups han de tenir ordre 7. Sigui F un subgrup de Sylow de G.

$$\left.\begin{array}{l} H \lhd G \\ F \subset G \end{array}\right\} \implies HF \text{ és subgrup de } G \text{ i } \frac{HF}{H} \simeq \frac{F}{F \cap H}. \tag{2.4.9}$$

Com que aquests dos grups són isomorfs, els índexs $[HF : H]$ i $[F : F \cap H]$ han de coincidir i hem de veure l'ordre de la intersecció, $|F \cap H|$. Si la intersecció és buida, obtenim $|HF| = |H| \cdot |F|$.

$$[HF : H] = [F : F \cap H] \implies |HF| = \frac{|H| \cdot |F|}{|F \cap H|}. \tag{2.4.10}$$

Com que H és grup (i subgrup normal) d'ordre 59, els elements diferents d'e, tenen ordre 59 (59 és un nombre primer i podem aplicar una proposició de teoria). Anàlogament, els elements d'F diferent del neutre tenen ordre 7. Per tant, $H \cap F = \{e\}$ i $|HF| = |H| \cdot |F| = 413$.
Per al tercer apartat, $|G/H| = 2^3 \cdot 7$. Definim $\overline{n_p}$ el nombre de p-subgrups de Sylow de $\overline{G} = G/H$.

$$\left.\begin{array}{l} \overline{n_2} \equiv 1 \pmod 2 \\ \overline{n_2} \mid 7 \end{array}\right\} \implies \overline{n_2} = 1 \vee 7. \tag{2.4.11}$$

I per a $\overline{n_7}$:

$$\left.\begin{array}{l} \overline{n_7} \equiv 1 \pmod 7 \\ \overline{n_7} \mid 8 \end{array}\right\} \implies \overline{n_7} = 1 \vee 8. \tag{2.4.12}$$

1. Si $\overline{n_7} = 1$, l'únic 7-subgrup de Sylow és normal en G i, per tant, $\overline{G}$ no és simple.
2. Si $\overline{n_7} = 8$, H_7 i H_7' són 7-subgrups de Sylow tals que $H_7 \cap H_7' = \{e\}$. G tindria $8 \cdot 6 = 48$ elements d'ordre 7 i, per tant, G té $56 - 48$ elements d'ordre diferent que 7. $\overline{G}$ té almenys un 2-subgrup de Sylow d'ordre 8.
3. Si $\overline{n_2} = 1$, l'únic 2-subgrup de Sylow de $\overline{G}$ és normal i $\overline{G}$ no és simple.

Pel que fa a l'últim apartat, $H \subset G$. Com que H és resoluble, solament ens falta veure que G/H és resoluble per implicar que G és resoluble. Dins de $\overline{G}$ tenim un $\overline{H_7}$ normal i cíclic, així doncs resoluble, i $|\overline{G}/\overline{H_7}| = 2^3$ és resoluble pel fet de ser p-grup. Per tant, $\overline{G}$ resoluble. ■

Exercici 2.4.10. *Sigui G un grup finit d'ordre $2p$, on p és un nombre primer més gran que 2. Demostreu que, o bé G és cíclic o bé que G és isomorf al grup diedral D_{2p}.*

Demostració. Denotem per n_2 el nombre de 2-Sylows i per n_p el nombre de p-Sylows. Aplicant el tercer teorema de Sylow obtenim el següent:

$$\left.\begin{array}{l} n_2 \equiv 1 \pmod 2 \\ n_2 \mid p \end{array}\right\} \implies n_2 = 1, p; \qquad \left.\begin{array}{l} n_p \equiv 1 \pmod p \\ n_p \mid 2 \end{array}\right\} \implies n_p = 1. \tag{2.4.13}$$

Per tant, tenim un únic 2-Sylow S_p i $S_p \lhd G$. Si $n_2 = 1$ i S_2 és el 2-Sylow, pot veure's que $G = S_2 S_p$. Suposem ara que $n_2 = p$ i sigui S_2 un 2-Sylow, aleshores podem escriure $S_2 = \langle y \rangle \notin S_p = \langle x \rangle$ i, per tant, $yx \notin \langle x \rangle$ amb la qual cosa $\text{ord}(yx) = 2$ de manera que $yxyx = e \implies yxy = x^{-1}y$ i tenim que:

$$G = \langle x, y \mid \text{ ord}(x) = p, \text{ord}(y) = 2, yxy^{-1} = x \rangle = D_{2p}. \tag{2.4.14}$$

■

Exercici 2.4.11. *Sigui $|G| = p^2$, amb p primer. G és cíclic o bé G és isomorf a $C_p \times C_p$.*

Demostració. Qualsevol element de G té ordre 1, p o p^2 (un divisor de $|G|$). Si G té elements d'ordre p^2, aleshores G és cíclic (ja que $|G| = p^2$). Altrament, és a dir, si G no té elements d'ordre p^2 i són d'ordre 1 o bé d'ordre p, podem usar que tot p-grup té centre no trivial ($1 < |Z(G)| \leq p$):

$$|Z(G)| \leq p \implies \exists x \in G \mid \operatorname{ord}(x) = p,\ x \in Z(G). \tag{2.4.15}$$

$\langle x \rangle$ té ordre p. Agafem $y \in G \setminus \langle x \rangle$ i com, en particular, no és el neutre, necessàriament $\operatorname{ord}(y) = p$. Volem veure que $G = \langle x \rangle \times \langle y \rangle \simeq C_p \times C_p$. En efecte:

$$x \in Z(G) \implies xy = yx, \forall y \in G \implies x^i y^j = y^j x^i \implies \langle x \rangle \cap \langle y \rangle = \{e\}. \tag{2.4.16}$$

Aquesta última implicació es dona perquè si $\langle x \rangle \cap \langle y \rangle \neq \{e\}$, tindríem que $\langle x \rangle = \langle y \rangle$, però $y \notin \langle x \rangle$. Si $\langle x \rangle$ i $\langle y \rangle$ estan en producte directe i $\langle x \rangle \times \langle y \rangle$ té ordre p^2 i $\langle x \rangle \times \langle y \rangle = G$. ■

Observació 2.4.12. Recordem que cada vegada que determinem n_p estem resolent congruències de l'estil, aplicat a l'exemple anterior:

$$\begin{gathered} n_{13} \mid 3^2 \cdot 29 \\ 29 \equiv 3 \pmod{13} \\ 29 \cdot 3 \equiv 3 \cdot 3 \equiv 9 \pmod{13} \\ 29 \cdot 3^2 \equiv 3 \cdot 3^2 \equiv 27 \equiv 1 \pmod{13} \end{gathered} \tag{2.4.17}$$

$$\begin{gathered} n_{29} \mid 3^2 \cdot 13 \\ 3 \cdot 13 \equiv 10 \pmod{29} \\ 3^2 \cdot 13 \equiv 30 \equiv 1 \pmod{29}. \end{gathered} \tag{2.4.18}$$

Exercici 2.4.13. *Si $|G| = 3393 = 3^2 \cdot 13 \cdot 29$. Trobeu que G té un subgrup normal d'ordre 13 o un d'ordre 29. Proveu que G és resoluble. Proveu que G té un únic subgrup d'ordre $13 \cdot 29$ que és normal.*

Demostració. Per veure que G té un subgrup normal d'ordre 13 o un d'ordre 29, hem d'aplicar els teoremes de Sylow:

$$\left.\begin{gathered} n_{13} \equiv 1 \pmod{13} \\ n_{13} \mid 3^2 \cdot 29 \end{gathered}\right\} \implies n_{13} = 1, 3^2 \cdot 29 \qquad \left.\begin{gathered} n_{29} \equiv 1 \pmod{29} \\ n_{29} \mid 3^2 \cdot 13 \end{gathered}\right\} \implies n_{29} = 1, 3^2 \cdot 13. \tag{2.4.19}$$

Ara, si $n_{13} \neq 1$ i $n_{29} \neq 1$ (no podem trobar un únic subgrup normal d'aquests ordres), aleshores cal que $n_{13} = 3^2 \cdot 29$ i $n_{29} = 3^2 \cdot 13$.

$$\left.\begin{gathered} G \text{ té } 3^2 \cdot 29 \cdot 12 \text{ elements d'ordre } 13 \\ G \text{ té } 3^2 \cdot 13 \cdot 28 \text{ elements d'ordre } 29 \end{gathered}\right\} \implies |G| = 3^2 \cdot 377 < 3^2 \cdot 29 \cdot 12 + 3^2 \cdot 13 \cdot 28. \tag{2.4.20}$$

Per tant, un dels n_p (no els dos, o l'un o l'altre) és 1 i, per tant, tenim un únic p-subgrup normal. Ara vegem que G és resoluble: si $n_{29} = 1$, $H_{29} \lhd G$. Com H_{29} és cíclic d'ordre primer, H_{29} és resoluble. Pel teorema de Lagrange i els de Sylow, separadament:

$$\left|\frac{G}{H_{29}}\right| = 3^2 \cdot 13, \qquad \left.\begin{gathered} n_{13} \equiv 1 \pmod{13} \\ n_{13} \mid 9 \end{gathered}\right\} \implies n_{13} = 1. \tag{2.4.21}$$

Si posem $\overline{G} = \frac{G}{H_{23}}$ té un únic 13-Sylow i $\overline{G}$ és normal. Per acabar de veure que $\overline{G}$ és resoluble, $\frac{\overline{G}}{\overline{H_{13}}} = 3^2$ (el seu ordre és una potència de p, un p-grup). Per tant,

$$\begin{array}{c} \overline{H_{13}} \text{ és cíclic d'ordre primer } \implies \text{ resoluble} \\ \overline{G}/\overline{H_{13}} \text{ és } p\text{-grup } \implies \text{ resoluble} \end{array} \tag{2.4.22}$$

H_{23} i $\overline{G}$ resolubles impliquen que G és resoluble. Finalment, G té un únic subgrup d'ordre $13 \cdot 29$, el qual és normal: si $n_{29} = 1$,

$$\pi : G \longrightarrow \overline{G} = \frac{G}{H_{29}},\ |\pi^{-1}(\overline{H})| = 29|\overline{H}|. \tag{2.4.23}$$

Hi ha una correspondència bijectiva entre els subgrups de G que contenen H_{29} ($\ni \pi^{-1}(\overline{H})$) i els subgrups de $\overline{G}$ ($\ni \overline{H}$). Com que $\overline{H} \lhd \overline{G}$, aleshores $\pi^{-1}(\overline{H}) \lhd G$ (és resultat de teoria, l'antiimatge d'un normal també és normal). Si H és subgrup de G d'ordre $13 \cdot 29$, H té un subgrup normal d'ordre 29, que és subgrup de G. Per tant, és H_{29}. Com $\overline{G}$ té un únic subgrup d'ordre 13, G té un únic subgrup d'ordre $13 \cdot 29$.
Efectivament, $H_{13}H_{29}$ és subgrup de G que té ordre $13 \cdot 29$ i, en conseqüència, $H_{13}H_{29}$ és l'únic subgrup de G d'ordre $13 \cdot 29$, que anomenarem F. Si suposem $n_{29} = 1$, tot 13-Sylow de G és subgrup de l'únic subgrup de G d'ordre $13 \cdot 29$ i n'és un 13-Sylow a F:

$$\left.\begin{array}{c} n_{13} \equiv 1 \pmod{13} \\ n_{13} \mid 29 \end{array}\right\} \implies n_{13} = 1 \implies G \text{ té un únic 13-Sylow.} \tag{2.4.24}$$

■

Exercici 2.4.14. *Troba l'ordre del grup* $G = \langle a, b \mid a^5 = 1, b^4 = 1, aba^{-1}b = 1\rangle$.

Demostració. D'$a^5 = 1$, podem concloure que a té ordre 5 o bé té ordre 1. De manera anàloga, b té ordre 4, o 2, o 1. Però no podem concloure a priori que els ordre són exactament 4 i 5. *Com podem afrontar els problemes de grups determinats per relacions?* Malauradament, no tenim cap manera sistemàtica que ens garanteixi ja no una resposta adient, sinó correcta.
En aquest cas, la relació $aba^{-1}b = 1$ ens dona que $aba^{-1} = b^{-1}$ i, per tant, que $ab^{-1}a^{-1} = b$. Això ens diu que $ab^{-1} = ba$, de manera que podem extreure tota expressió que involucri a i b i anorrear cap b que ens aparegui a l'esquerra d'una a intercanviant ba per ab^{-1}.
Podem escriure tot element d'aquest grup de la forma a^ib^j amb $0 \leq i \leq 4$ i $0 \leq j \leq 3$. De fet, podem dir més: com que $aba^{-1} = b^{-1}$ i $ab^{-1}a^{-1} = b$, tenim el següent.

$$\begin{aligned} aba^{-1} &= b^{-1} \\ a^2ba^{-2} &= ab^{-1}a^{-1} = b \\ a^3ba^{-3} &= aba^{-1} = b^{-1} \\ a^4ba^{-4} &= ab^{-1}a^{-1} = b \\ a^5ba^{-5} &= aba^{-1} = b^{-1} \end{aligned} \tag{2.4.25}$$

Però $a^5 = 1$, de manera que $a^5ba^{-5} = b$. Concloem que $b = b^{-1}$ i $b^2 = 1$; podem reduir la tercera relació a $aba^{-1} = b \iff ab = ba$. Això vol dir que l'ordre *màxim* del grup és 10, donat que cada element es pot escriure com $a^ib^j, 0 \leq i \leq 4, 0 \leq j \leq 1$.
Per a provar que l'ordre de G és exactament 10, notem que el grup cíclic d'ordre 10, $C_{10} = \langle x \mid x^{10} = 1 \rangle$ té elements que satisfan les relacions $x^2 = 1$ i $x^5 = 1$. El mapa definit per $a \longmapsto x^2$ i $b \longmapsto x^5$ indueix un morfisme $G \longrightarrow C_{10}$, i com $C_{10} = \langle x^2, x^5 \rangle$, és exhaustiu. Així doncs, $|G| \geq 10$, però com abans hem vist que $|G| \leq 10$, ens queda que $|G| = 10$. El mapa que hem trobat indueix un morfisme bijectiu i G resulta un grup cíclic d'ordre 10. ■

III

Grups abelians finitament generats

En aquest capítol, considerarem grups abelians i denotarem l'operació del grup com a suma, l'element neutre per 0, l'element simètric d'un element x per $-x$. Si $(E,+)$ és un grup abelià, $x \in E, n \in \mathbb{Z}$, posem

$$nx := \begin{cases} x+\overset{n}{\cdots}+x & \text{si } n>0 \\ 0 & \text{si } n=0 \\ (-x)+\overset{-n}{\cdots}+(-x) & \text{si } n<0 \end{cases} \tag{3.0.1}$$

Anomenarem suma directa el producte directe de grups abelians i el denotarem per $\oplus$. Havíem vist que un grup finit és finitament generat però no recíprocament. El grup $\mathbb{Z}$ i, més generalment, la suma directa $\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ d'un nombre finit de còpies de $\mathbb{Z}$ són grups infinits finitament generats.

Proposició 3.0.1. *Si A és un grup abelià finitament generat, existeix un enter $r \geq 0$ i un grup finit F tals que*

$$A \simeq \mathbb{Z}\times\overset{r}{\cdots}\times\mathbb{Z}\times F \tag{3.0.2}$$

i es diu rang d'A, F es diu subgrup de torsió.

Proposició 3.0.2. *Sigui F un grup abelià finit, $|F| = p_1^{k_1}\cdots p_\ell^{k_\ell}$, amb $p_1,\ldots,p_\ell$ nombres primers, diferents dos a dos. Aleshores, $F \simeq F_1\times\cdots\times F_i$ és subgrup abelià d'ordre $p_i^{k_i}, 1\leq i\leq\ell$. Per a $1\leq r\leq\ell$, existeix un enter s_i i enters $k_{i_1}\geq\cdots\geq k_{i_{s_i}}>0$ tals que $k_i = k_{i_1}+\cdots+k_{i_{s_i}}$. $F_i \simeq F_{i_1}\times\cdots\times F_{i_{s_i}}$, amb F_{ij} grup cíclic d'ordre $p_i^{k_{ij}}$. Els enters $p_i^{k_{ij}}$ es diuen divisors elementals de F. Dos grups abelians finits amb els mateixos divisors elementals són isomorfs.*

Exemple 3.0.3. Els grups abelians d'ordre $200 = 2^3\cdot 5^2$. Notem que podem escriure:

$$\begin{gathered} 3 = 2+1 = 1+1+1 \\ 2 = 1+1 \end{gathered} \tag{3.0.3}$$

Quan tenim dos p-grups cíclics tals que el producte és cíclic i els dos ordres són primers entre ells, el producte cartesià dels dos és isomorf al grup cíclic que surt de fer el grup del producte dels dos ordres. En forma d'exemple:

$$\begin{array}{cc|cc} (3,2) & \mathbb{Z}/8\times\mathbb{Z}/25\simeq\mathbb{Z}/200 & (2+1,2) & \mathbb{Z}/4\times\mathbb{Z}/2\times\mathbb{Z}/25\simeq\mathbb{Z}/4\times\mathbb{Z}/50 \\ (3,1+1) & \mathbb{Z}/8\times\mathbb{Z}/5\times\mathbb{Z}/5\simeq\mathbb{Z}/40\times\mathbb{Z}/5 & (2+1,2+1) & \mathbb{Z}/4\times\mathbb{Z}/2\times\mathbb{Z}/5\simeq\mathbb{Z}/20\times\mathbb{Z}/10 \\ (1+1+1,2) & \mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/25\simeq\mathbb{Z}/50\times\mathbb{Z}/2\times\mathbb{Z}/2 & & \\ (1+1+1,1+1+1) & \mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/25\simeq\mathbb{Z}/10\times\mathbb{Z}/10\times\mathbb{Z}/2 & & \end{array} \tag{3.0.4}$$

En altres paraules, hem d'escriure totes les possibles particions dels grups primers i podem associar factors tenint en compte el producte directe de grups. Podem fixar l'ordre que vulguem i podem descriure exactament tots els grups abelians que tenen aquest ordre.

Podeu trobar una extensió d'aquest capítol a l'*Apèndix*, així com altres continguts de grups que no s'han donat a les classes.

Part

II

Anells

$$f(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ f(n-1) + f(n-2) & \text{if } n \geq 2 \end{cases}$$

IV

Anells

4.1 Definicions

Definició 4.1.1 (Anell). És un conjunt A no buit dotat de dues operacions internes, la suma i el producte, tals que:

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

Si, a més, el producte és commutatiu ($ab = ba$), direm que A és **anell commutatiu**. Si A té element neutre pel producte ($1_A \cdot a = a \cdot 1_A = a$), direm que és un **anell amb unitat**.

Exemple 4.1.2.

- $\mathbb{Z}$ és anell commutatiu i unitari (amb la suma i el producte com a operacions internes).
- $\mathbb{R}[X]$ és anell commutatiu i unitari (amb la suma i producte de polinomis).
- $\mathcal{M}_{n\times n}(\mathbb{R})$ és anell unitari i no commutatiu per a $n \geq 2$.
- També podem considerar l'anell trivial, $A = \{0\}$.

Definició 4.1.3 (Element invertible). Un element a d'un anell amb unitat A es diu invertible si té invers a A. Si a és element invertible de l'anell A es compleix $ab = 0 \implies b = 0$, ja que $ab = 0 \implies a^{-1}(ab) = a^{-1} \cdot 0 = 0$, i d'altra banda, $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$.

$$A^* = \{a \in A \mid a \text{ és invertible}\},\ A^* \text{ és grup amb el producte d'} A. \tag{4.1.1}$$

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

Definició 4.1.4 (Cos). Un cos és un anell commutatiu amb unitat en què tot element no nul és invertible.

Exemple 4.1.5. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, amb la suma i el producte usuals, són cossos.

Proposició 4.1.6. *Sigui A un anell, $a \in A$. Aleshores, $a0 = 0$ i $0a = 0$.*

Demostració. És resultat directe de la definició d'anell $a0 = a(0+0) = a0+a0 \implies a0 = 0$. ■

Definició 4.1.7 (Subanell). Sigui A un anell. Un subanell d'A és un subconjunt no buit B d'A tal que:

- $(B, +)$ és subgrup d'$(A, +)$.

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

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

Definició 4.1.8 (Divisor de zero)**.** Un element a d'un anell A, $a \neq 0$, es diu divisor de zero si existeix $b \in A, b \neq 0$ tal que $ab = 0$.

Exemple 4.1.9. Per exemple, posem $A = \mathbb{Z}/6\mathbb{Z}$. Agafem $\overline{2} \in A$ i $\overline{3} \in A$. La seva multiplicació ens dona la classe del 0, $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} \equiv \overline{0} \in A$.

Definició 4.1.10 (Domini d'integritat)**.** Sigui A un anell. Diem que A és un domini d'integritat si no té divisors de zero. Si A és domini d'integritat i prenem $a, b \in A$ tals que $ab = 0$, aleshores $a = 0$ o bé $b = 0$ (o, per contrarrecíproc, $a \neq 0, b \neq 0 \implies ab \neq 0$).

Definició 4.1.11 (Subcòs)**.** Un subanell B d'un cos $\mathbb{K}$ és subcòs de $\mathbb{K}$ si per a tot $z \in B \setminus \{0\}$ i $x^{-1} \in B$.

Exemple 4.1.12. $\mathbb{Z}$ és subanell de $\mathbb{Q}$ i $\mathbb{Q}$ és subcòs de $\mathbb{R}$.

Definició 4.1.13 (Centre)**.** Sigui A un anell. El centre d'A és el conjunt d'elements que commuten amb tot element d'A; això és, $Z(A) = \{z \in A \mid az = za, \forall a \in A\}$.

Proposició 4.1.14. *El centre de tot anell és un subanell.*

Demostració. Sigui A un anell i $Z(A)$ el seu centre. Si $a \in A$, aleshores $0a = 0 = a0$, i $0 \in Z(A)$. Prenem $y, z \in Z(A)$ qualssevol. Per a tot $a \in A$ tenim $a(y - z) = ay - az = ya - za = (y - z)a$, pel fet que y, z són del centre. Així, $y - z \in Z(A)$. De la mateixa manera, $ayz = yaz = yza$ i $yz \in Z(A)$. ∎

Corol·lari 4.1.15. *Si A és un anell commutatiu, el seu centre és tot A; és a dir, $A = Z(A)$.*

Proposició 4.1.16. *Sigui A un anell i $a \in A$. Aleshores, que a sigui invertible implica que a no és divisor de zero. Per tant, tot cos és domini d'integritat.*

Demostració. La demostració ve donada per la definició que hem fet d'element invertible, 4.1.3: si a és element invertible de l'anell A es compleix $ab = 0 \implies b = 0$, ja que $ab = 0 \implies a^{-1}(ab) = a^{-1} \cdot 0 = 0$, i d'altra banda, $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$. ∎

Proposició 4.1.17. *Si A és domini d'integritat, aleshores $A[X]$ és domini d'integritat.*

Demostració. Siguin $P(x), Q(x)$ dos polinomis no nuls, posem n el grau de P i m el grau de Q; a_n el coeficient de X^n en P i b_m el de X^m en Q. Aleshores, el coeficient de X^{n+m} en PQ és $a_n b_m \neq 0$ i, per tant, $PQ \neq 0$.

$$\begin{gathered} P(X) = a_n x^n + \cdots +, Q(X) = b_m x^m + \cdots \\ P(X)Q(X) = a_n b_m x^{n+m} + \cdots \neq 0. \end{gathered} \tag{4.1.2}$$

Això es dona per la definició de domini d'integritat. ∎

Exercici 4.1.18. *Proveu que tot domini d'integritat finit és un cos.*

Demostració. Podem dir que un cos és aquell on tot element no nul és invertible. Sigui A un domini d'integritat. Aleshores, per definició $ab = 0 \iff a = 0$ o bé $b = 0$, que, pel contrarrecíproc, és equivalent a considerar que $ab \neq 0 \iff a \neq 0$ i $b \neq 0$. Volem veure que per a tot $a \neq 0$, a és invertible. Sigui una funció f definida de la següent forma:

$$\begin{array}{rccc} f: & A & \longrightarrow & A \\ & x & \longmapsto & ax \end{array} \tag{4.1.3}$$

f és injectiva, ja que donats $x, y \in A$ tenim que:

$$f(x) = f(y) \implies ax = ay \iff a(x-y) = 0 \iff \left.\begin{array}{c} a = 0 \\ x - y = 0 \end{array}\right\} \implies f \text{ és injectiva.} \tag{4.1.4}$$

Com l'endomorfisme $f : A \longrightarrow A$ és una aplicació amb A finit i f injectiva, f és bijectiva. En particular, f és exhaustiva i, per tant, existeix $b \in A \mid f(b) = ab = 1$ i $ab = ba = 1$ pel fet que A és commutatiu. ■

Exercici 4.1.19. *Caracteritzeu, en funció del nombre enter $m > 1$, quins són els elements invertibles i quins els divisors de zero de l'anell $\mathbb{Z}/m\mathbb{Z}$. Deduïu que $\mathbb{Z}/m\mathbb{Z}$ és un domini d'integritat si, i només si, $\mathbb{Z}/m\mathbb{Z}$ és un cos; si i només si, m és un nombre primer.*

Demostració. 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 mn és un nombre enter diferent de zero; per tant, l'únic nombre enter divisor de zero és 0. 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, $\mathrm{mcd}(n, a) \neq 1$. Si $\mathbb{Z}/m\mathbb{Z}$ és un cos, tot element excepte el neutre és invertible, és a dir, $\mathrm{mcd}(n, a) = 1$, per a tot a representant d'alguna classe. D'aquesta manera, n ha de ser primer. L'altra implicació és similar. ■

4.2 Ideals d'un anell

4.2.1 Definicions i primeres propietats

Definició 4.2.1 (Ideal)**.** Donat un anell A commutatiu (i unitari), un ideal d'A és un subconjunt I d'A tal que

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

Exemple 4.2.2 (Trivial, total i ideal principal)**.**

- Si A és anell, $\{0\}$ i A són ideals (el trivial i el total) d'A.

- Sigui $a \in A$, tal que $I = \{ab \mid b \in A\}$ és ideal d'A:

$$\begin{aligned} (I,+) \text{ és subgrup d'} A \text{ i } a \in I &\implies I \neq \emptyset \\ ab + ac = a(b+c) \in I; -ab = a(-b) &\in I \\ c \in A \wedge ab \in I &\implies cab = a(bc) \in I. \end{aligned} \tag{4.2.1}$$

Diem que I és ideal principal. Per exemple, $\{0\} = (0)$ i $A = (1)$ són ideals principals.

Proposició 4.2.3. *Tot ideal I de $\mathbb{Z}$ és igual a (m), per a algun enter natural m. A $\mathbb{Z}$, $(m) \cap (n) = (\text{mcm}(m,n))$.*

Demostració. Per 1.1.14, tot subgrup de $\mathbb{Z}$ és isomorf a (m), per a algun enter natural m, i (m) és també un ideal de $\mathbb{Z}$. ■

Proposició 4.2.4. *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 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 4.2.5. *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 4.2.6. 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 4.2.7 (Domini d'ideals principals). Si A és domini d'integritat i tots els ideals d'A són principals, diem que A és un domini d'ideals principals (DIP).

Proposició 4.2.8. *Si $\mathbb{K}$ és cos, l'anell $\mathbb{K}[X]$ és domini d'ideals principals.*

Demostració. Com $\mathbb{K}$ és un cos, és domini d'integritat, i $\mathbb{K}[X]$ també ho és. Sigui ara I un ideal de $\mathbb{K}[X]$. Si $I = \{0\}$, tenim $I = (0)$. Si no, I té elements no nuls; per tant, amb grau més gran o igual que 0. Sigui P un element de l'ideal I amb grau mínim entre els elements no nuls de I. Vegem que $I = (P)$:

$I \supset (P)$ Pel fet que P pertany a I.

$I \subset (P)$ Si $A \in I$, fem la divisió euclidiana d'A entre P: $A = PQ + R$, amb $\text{gr}(R) < \text{gr}(P)$ i $0 \leq \text{gr}\, R$. Ara, $R = A - PQ \in I$ implica que $R = 0$, per l'elecció de P (grau mínim). Per tant, $A = PQ \in (P)$.

Com que hem demostrat les dues inclusions, ja hem obtingut el que volíem. ■

Definició 4.2.9 (Divisor)**.** Si A és un anell, amb $a, b \in A$, diem que a divideix b si existeix $c \in A$ tal que $b = ac$. Ho denotem per $a \mid b$. Clarament, $a \mid b \iff b \in (a)$.

Exercici 4.2.10. *Demostreu que l'ideal $(2, X)$ de $\mathbb{Z}[X]$ no és principal.*

Demostració. Es veu clarament que el terme independent és parell:

$$I = (2, X) = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_0 \text{ és parell}\}. \tag{4.2.2}$$

Ara, suposem una funció f tal que $I = (f(x))$ per a algun $f(x) \in I$. Si f és un polinomi constant, aleshores $(f(x))$ conté solament els polinomis amb coeficients parells (no obtenim x). En canvi, si $f(x)$ és de grau més gran o igual que 1, els polinomis diferents del nul que es troben a $(f(x))$ tenen grau com a mínim 1 (no obtenim 2). Per tant, I no és de la forma de $(f(x))$. ■

Exercici 4.2.11. *Siguin A un anell i $f, g \in A[X]$.*

1. *Demostreu que si g és mònic, aleshores existeixen polinomis $q, r \in A[X]$ tals que $f = gq + r$, amb $r = 0$ o bé $\operatorname{gr}(r) < \operatorname{gr}(g)$. Demostreu que q i r són únics per a aquestes condicions.*
2. *Doneu un exemple de no-unicitat i un de no-existència del parell (q, r) en cas que g no sigui mònic.*

Teorema 4.2.12. *Sigui A un anell unitari (amb element neutre pel producte). Si I és un ideal d'A i conté una unitat (un element invertible), aleshores $I = A$.*

Demostració. Sigui $u \in I$ una unitat. Per ser u una unitat, $1 = uu^{-1} \in I$. I per a tot $a \in A$, també tenim $a = 1a \in I$ (per la definició d'ideal). Per tant, $I = A$. ■

4.2.2 Operacions amb ideals

Sigui A un anell i $\{I_j\}_{j \in \mathcal{J}}$ una família d'ideals d'A. La intersecció:

$$\bigcap_{j \in \mathcal{J}} I_j \text{ és ideal d'} A. \tag{4.2.3}$$

Si S és un subconjunt de l'anell A, no necessàriament finit, l'ideal generat per S és la intersecció de tots els ideals d'A que contenen S. El denotem per $(S)_A$ o (S). Clarament, si $S = \emptyset$, $(S) = \{0\}$.

Proposició 4.2.13. *Si S és subconjunt no buit de l'anell A:*

$$(S)_A = \{b_1 a_1 + \cdots + b_k a_k \mid k \in \mathbb{N}; a_1, \ldots, a_k \in S; b_1, \ldots, b_k \in A\}. \tag{4.2.4}$$

Demostració. Clarament, el conjunt $S' = \{b_1 a_1 + \cdots + b_k a_k \mid k \in \mathbb{N}; a_1, \ldots, a_k \in S; b_1, \ldots, b_k \in A\}$ és un ideal que conté S i, si I és ideal d'A contenint S, ha de contenir S' per la definició d'ideal. ■

Notació 4.2.14. Si $S = \{a_1, \ldots, a_r\}$ és un subconjunt finit de l'anell A, posem $(\{a_1, \ldots, a_r\}) = (a_1, \ldots, a_r)$.

Definició 4.2.15 (Ideal suma)**.** Donats dos ideals I, J de l'anell A, posem $I + J$ el conjunt dels elements de l'anell A que són suma d'un element d'I i un element de J. Clarament, $I + J$ és un ideal d'A i és l'ideal d'A generat pel conjunt $I \cup J$. Anomenem $I + J$ *l'ideal suma* de I i J. Més generalment, si $\{I_j\}_{j\in\mathcal{J}}$ és una família d'ideals d'A:

$$\text{L'ideal suma } \sum_{j\in\mathcal{J}} I_j \text{ és l'ideal generat per } \bigcup_{j\in\mathcal{J}} I_j. \tag{4.2.5}$$

Proposició 4.2.16. *Si $\{I_j\}_{j\in\mathcal{J}}$ és una família d'ideals d'A:*

$$\sum_{j\in\mathcal{J}} I_j = \{a_1 + \cdots + a_k \mid k \in \mathbb{N}; j_1, \ldots, j_k \in \mathcal{J} \text{ i } a_i \in I_j, 1 \leq i \leq k\}. \tag{4.2.6}$$

Demostració. El conjunt $\{a_1 + \cdots + a_k \mid k \in \mathbb{N}; j_1, \ldots, j_k \in \mathcal{J} \text{ i } a_i \in I_j, 1 \leq i \leq k\}$ és ideal de l'anell A, conté $\bigcup_{j\in\mathcal{J}}$ i està contingut en tot ideal I d'A que contingui $\bigcup_{j\in\mathcal{J}} I_j$. ■

Definició 4.2.17 (Ideal producte)**.** Donats dos ideals I, J de l'anell A, posem IJ el conjunt dels elements de l'anell A que són producte d'un element d'I i un element de J.

$$IJ = \{a_1b_1 + \cdots + a_kb_k \mid k \in \mathbb{N}; a_i \in I, b_i \in J; 1 \leq i \leq k\}. \tag{4.2.7}$$

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

Exercici 4.2.18. *Siguin I, J_1, J_2 ideals d'un anell A. Proveu que:*

1. $I + (J_1 \cap J_2) \subset (I + J_1) \cap (I + J_2)$. *Si $I \subset J_1$ o bé $I \subset J_2$, llavors tenim igualtat.*
2. $I \cap (J_1 + J_2) \supset (I \cap J_1) + (I \cap J_2)$. *Si $I \supset J_1$ o bé $I \supset J_2$, llavors hi ha igualtat.*
3. $I(J_1 + J_2) = (IJ_1) + (IJ_2)$.
4. $(J_1 + J_2)(J_1 \cap J_2) \subset J_1J_2$.

Demostració. Ens haurem d'ajudar de les definicions que hem introduït fins ara i, també, de teoria de conjunts:

- Sigui $a \in I + (J_1 \cap J_2)$. Per definició d'ideal suma, podem escriure $a = a_1 + a_2, a_1 \in I, a_2 \in (J_1 \cap J_2)$. Per tant, podem afirmar que:

$$\begin{array}{ll} a \in I + J_1, & \text{ja que } a_2 \in J_1 \\ a \in I + J_2, & \text{ja que } a_2 \in J_2 \end{array} \tag{4.2.8}$$

Així doncs, $a \in (I+J_1)\cap(I+J_2)$. Com aquest raonament val per a tot $a \in A$, la inclusió queda demostrada. Suposem $I \subset J_1$ ($I \subset J_2$ es provaria de manera anàloga). Aleshores, donat $a \in (I+J_1)\cap(I+J_2)$ tenim que $a \in J_1$ i $a \in I+J_2$, és a dir, que $a = a_1 + a_2 \in J_1$ amb $a_1 \in I, a_2 \in J_2$ ($a_2 \in J_1, a_2 \in J_2$) i es compleix l'altra inclusió.

- Sigui $a \in (I\cap J_1)+(I\cap J_2)$. Anàlogament a l'apartat anterior, $a = a_1 + a_2$ i $a_1 \in I \cap J_1$ i $a_2 \in I \cap J_2$. Si $a_1, a_2 \in I$, $a \in I$. A la vegada, $a_1 \in J_1$ i $a_2 \in J_2$, respectivament. Obtenim, doncs, $a \in I \cap (J_1+J_2)$.

$$I \supset J_1 \implies a \in I \cap (J_1+J_2) \equiv a \in I \wedge a_1 \in J_1 \subset I \wedge a_2 \in J_2, \text{ i } a_2 \in I \ (a \in I). \quad (4.2.9)$$

  Anàlogament per a $I \supset J_2$.
- Ara hem d'usar les propietats de l'ideal producte. En aquest, cas, tenim que:

$$\begin{array}{rl} I(J_1+J_2) & = \{a_1(b_1+b_2) \mid a \in I, b = b_1+b_2 \in J_1+J_2\}, \\ (IJ_1)+(IJ_2) & = \{a_1b_1 + a_2b_2 \mid a_i \in I, b_1 \in J_1, b_2 \in J_2\}. \end{array} \quad (4.2.10)$$

  Amb les definicions ja es veu de manera prou clara la igualtat.
- Sigui $a \in (J_1+J_2)(J_1\cap J_2)$. Provarem que $a \in J_1J_2$. En efecte, per definició tenim que:

$$a = \sum_i y_iz_i, y_i \in J_1+J_2, z_i \in J_1\cap J_2 \implies a = \sum_i y_{i1}z_i + \sum_i y_{i2}z_i \in J_1J_2. \quad (4.2.11)$$

- Sigui $a \in (J_1+J_2)(J_1\cap J_2) \subset J_1J_2$. Podem escriure a com a combinació lineal de termes J_1+J_2 i $J_1\cap J_2$, és a dir:

$$a = a_1b_1 + \cdots + a_nb_n \implies a = \sum_{i=1}^n (a_{i1}+a_{i2})b_i \iff a = \sum_{i=1}^n a_{i1}b_i + \sum_{i=1}^n a_{i2}b_i. \quad (4.2.12)$$

  Així, $a \in (IJ_1)+(IJ_2)$.

Ja hem provat tots els apartats. ■

Exercici 4.2.19. *Siguin I, J ideals d'un anell A. Proveu que $(I:J) = \{a \in A \mid ab \in I, \forall b \in J\}$ és un ideal d'A.*

Demostració. Se segueix de la definició d'ideal: si $(I:J)$ és ideal d'un anell A és un subconjunt $(I:J)$ d'A tal que $(I:J,+)$ és subgrup d'$(A,+)$ i $ax \in (I:J), a \in A, x \in (I:J)$. En efecte:

- $(I:J,+)$ és subgrup ja que $ac - bc \in I, \forall c \in J$, amb $a, b \in (I:J)$, ja que $ac \in I$ i $bc \in I$ per la sel·lecció d'a i b. Fixem-nos que $ac - bc \in I, \forall c \in J \iff (a-b)c \in I, \forall c \in J$ i, així, $a - b \in (I:J)$ (si recordem de *Grups*, per provar que és subgrup és suficient amb demostrar que xy^{-1} és tancada).
- Per altra banda, siguin $a \in A$ i $x \in (I:J)$ qualssevol. Per definició de $(I:J)$, $xb \in I$. Pel fet de ser I un ideal, també $axb \in I$, per a tot $b \in J$. Per tant, $ax \in (I:J)$.

Havent provat les dues condicions d'ideal, ja podem dir que $(I:J)$ és un ideal d'A. ■

Exercici 4.2.20. *Sigui A un anell. Proveu que A és cos, si i només si, els seus únics ideals són (0) i A.*

Demostració. Provarem el resultat per a ambdues implicacions:

⇒ Sigui I un ideal d'A. Si $I = \{0\}$, ja hem acabat, així que sigui $0 \neq a \in A$. Aleshores, a és una unitat pel fet de ser A un cos i, per 4.2.12, $I = A$.

⇐ Solament ens cal provar que tot element diferent de zero té inversa. Per tant, sigui $a \neq 0$ un element d'A. Tenim que $(a) \neq (0)$, ja que $a \neq 0$; per tant, $(a) = (1) = A$.

I ja hem acabat. ■

4.3 Anell quocient

Proposició 4.3.1 (Anell quocient)**.** *Sigui A un anell i I un ideal d'aquest anell A. Aleshores, A/I és anell. En particular, direm que A/I és l'anell quocient d'A per I.*

Demostració. Si I és un ideal d'un anell A, $(I, +)$ és subgrup del grup commutatiu $(A, +)$. Per tant, podem definir el quocient A/I i sabem que A/I és grup quocient commutatiu, amb la suma definida per $[a] + [b] = [a + b]$, per a $[a], [b]$ classes en A/I dels elements $a, b \in A$. Volem veure que podem definir un producte en A/I per $[a][b] = [ab]$ i que, amb la suma i el producte que hem definit, A/I és anell.

1. Veiem primer que el producte està ben definit. Si $a', b' \in A$ són tals que $[a] = [a']$ i $[b] = [b']$, tenim $a' = a + x$, $b' = b + y$, amb $x, y \in I$. Per tant:

$$a'b' = (a + x)(b + y) = ab + xb + ay + xy. \tag{4.3.1}$$

   Per la definició d'ideal $xb + ay + xy \in I$, per tant, $[a'b'] = [ab]$ i el producte d'A/I està ben definit.
2. Clarament, el producte d'A/I és associatiu, commutatiu i distributiu respecte de la suma, per ser-ho el d'A, i [1] és element neutre pel producte d'A/I.

Per tant, A/I és l'anell quocient d'A per I. ■

4.4 Morfisme d'anells

4.4.1 Propietats bàsiques dels morfismes

Definició 4.4.1 (Morfisme d'anells)**.** Si A, A' són anells, una aplicació $f : A \longrightarrow A'$ és morfisme d'anells si compleix:

$$f(a + b) = f(a) + f(b) \text{ i } f(ab) = f(a)f(b), \tag{4.4.1}$$

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

Observació 4.4.2.

1. Si $f : A \longrightarrow A'$ és morfisme d'anells i a és un element invertible d'A, aleshores $f(a)$ és invertible i $f(a^{-1}) = f(a)^{-1}$. En efecte, tenim: $aa^{-1} = 1_A \implies f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_{A'}$.
2. Diem que A^* és el conjunt d'elements invertibles d'A i que B^* és el conjunt d'elements invertibles de B. En particular, A^* és grup amb el producte d'A i B^* és grup amb el producte de B.
3. Amb això, tenim que $f|_{A^*} : A^* \longrightarrow B^*$ és morfisme de grups.

Definició 4.4.3 (Morfisme injectiu)**.** Si $f : A \longrightarrow A'$ és morfisme d'anells, el nucli de f és $\ker(f) = \{a \in A \mid f(a) = 0_{A'}\}$; és a dir, el nucli de f com a morfisme de grups. Tenim, doncs, que f és un morfisme injectiu si, i només si, $\ker(f) = \{0_A\}$.

Exemple 4.4.4. Si I és ideal d'A, l'aplicació

$$\begin{array}{rccc} \pi : & A & \longrightarrow & A/I \\ & a & \longmapsto & [a] \end{array} \tag{4.4.2}$$

és morfisme d'anells. S'anomena morfisme de pas al quocient.

Proposició 4.4.5. *Si $f : A \longrightarrow A'$ és morfisme d'anells, $\ker(f)$ és ideal d'A i $\mathrm{im}(f)$ és subanell d'A'.*

Demostració. Sabem que $\ker(f)$ és subgrup d'$(A, +)$ i $\mathrm{im}(f)$ és subgrup de $(A', +)$. Sigui ara $a \in A$ i $x \in \ker(f)$. Tenim:

$$f(ax) = f(a)f(x) = f(a) \cdot 0 = 0; \tag{4.4.3}$$

per tant, $ax \in \ker(f)$ i $\ker(f)$ és ideal d'A. Siguin $a', b' \in \mathrm{im}(f)$. Podem posar $a' = f(a)$ i $b' = f(b)$, per a certs $a, b \in A$. Per tant, $a'b' = f(a)f(b) = f(ab) \in \mathrm{im}(f)$ i $\mathrm{im}(f)$ resulta ser un subanell d'A'. ■

Observació 4.4.6. Recordem que en teoria de grups tant el nucli com la imatge per un homomorfisme de grups són subgrups, però amb el resultat anterior hem vist que el nucli d'un morfisme φ és, rarament, un subanell. Tot i que compleixen quasi totes les propietats d'un subanell, quasi mai contenen la identitat multiplicativa. El resultat el concretem en el següent teorema.

Teorema 4.4.7. *Sigui $f : A \longrightarrow A'$ un morfisme d'anells. La imatge per f és un subanell d'A', però $\ker(f)$ és subanell d'A si, i només si, $A' = \{0\}$.*

Observació 4.4.8. De la mateixa manera, la imatge d'un ideal per un morfisme d'anells habitualment no és un ideal. *Per exemple, la imatge de $\mathbb{Z}$ per la inclusió $\mathbb{Z} \hookrightarrow \mathbb{Q}$.*

Exercici 4.4.9. *Siguin J_1, J_2 ideals d'un anell A, $\pi_1 : A \longrightarrow A/J_1$ i $\pi_2 : A \longrightarrow A/J_2$ els corresponents morfismes de pas al quocient. Considerem l'anell producte directe $(A/J_1) \times (A/J_2)$ i el morfisme:*

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & (A/J_1) \times (A/J_2) \\ & a & \longmapsto & (\pi_1(a), \pi_2(a)) \end{array} \tag{4.4.4}$$

φ és morfisme exhaustiu si, i només si, $J_1 + J_2 = A$. φ és injectiu si, i només si, $J_1 \cap J_2 = (0)$.

Demostració.

1. Si φ és exhaustiva, en particular existeix $x \in A$ tal que $\varphi(x) = (1,0)$. Per tant, $x + J_1$ i $x + J_2 = 0$ i, aleshores:

$$1 = (1-x) + x \in J_1 + J_2 \implies J_1 + J_2 = A. \tag{4.4.5}$$

   Recíprocament, si demostrem que existeixen $x, y \in A$ tals que $\varphi(x) = (0,1)$ i $\varphi(y) = (1,0)$ ja haurem acabat, ja que per a tot $(a,b) \in (A/J_1) \times (A/J_2)$ tenim que:

$$\varphi(ay + bx) = \varphi(a)\varphi(y) + \varphi(b)\varphi(x) = (a,a')(1,0) + (b',b)(0,1) = (a,b). \tag{4.4.6}$$

   Ara bé, $1 \in A = J_1 + J_2 \implies 1 = x + y, x \in J_1, y \in J_2$ i pot comprovar-se que $\varphi(y) = (0,1)$ i $\varphi(x) = (1,0)$.
2. Calculem $\ker(\varphi)$ i tenim que:

$$(\overline{x}, \overline{x'}) = (0,0) \iff x \in J_1, x \in J_2 \iff x \in J_1 \cap J_2. \tag{4.4.7}$$

   Per tant, φ és injectiva si, i només si, $\ker(\varphi) = J_1 \cap J_2 = (0)$.

■

4.4.2 Teorema d'isomorfia aplicat a anells

Definició 4.4.10 (f factoritza a través d'un anell quocient). Siguin A, A' anells, $f : A \longrightarrow A'$ un morfisme d'anells, I un ideal d'A i $\pi : A \longrightarrow A/I$ si existeix un morfisme d'anells $\overline{f} : A/I \longrightarrow A'$. f factoritza a través d'un anell quocient si $f = \overline{f} \circ \pi$, és a dir, si el diagrama posterior és commutatiu:

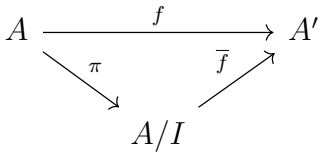


Figura 4.1: Diagrama de factorització a través del quocient

Proposició 4.4.11. *Siguin A, A' anells, $f : A \longrightarrow A'$ un morfisme d'anells, I un ideal propi d'A i $\pi : A \longrightarrow A/I$ el morfisme de pas al quocient. Aleshores, f factoritza a través d'A/I si, i només si, $I \subset \ker(f)$.*

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

$$\overline{f}(1_{A/I}) = \overline{f}([1_A]) = f(1_A) = 1_B \text{ i } \overline{f}([a][b]) = \overline{f}([ab]) = f(ab) = f(a)f(b) = \overline{f}([a])\overline{f}([b]). \tag{4.4.8}$$

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

Teorema 4.4.12 (Primer teorema d'isomorfia per a anells)**.** *Si A, A' són anells i $f : A \longrightarrow A'$ és un morfisme d'anells, aleshores f factoritza a través d'$A/\ker(f)$ i tenim $f = i \circ \tilde{f} \circ \pi$, amb $\tilde{f}$ isomorfisme d'anells d'$A/\ker(f)$ en $\mathrm{im}(f)$, i la inclusió d'$\mathrm{im}(f)$ en A', $\pi : A \longrightarrow A/\ker(f)$ el morfisme de pas al quocient. Tenim, doncs, un diagrama commutatiu:*

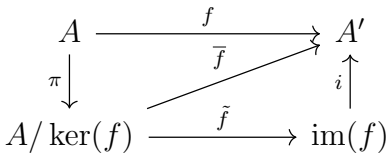


Figura 4.2: Diagrama commutatiu del primer teorema d'isomorfis per a anells

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

4.4.3 Característica d'un anell

Definició 4.4.13 (Característica)**.** Donat un anell A (commutatiu i unitari), existeix un únic morfisme d'anells $\varphi : \mathbb{Z} \longrightarrow A$. En efecte, φ ha de complir $\varphi(1) = 1_A$ i aquesta propietat determina φ, ja que, per a $m \in \mathbb{Z}$, tenim $\varphi(m) = \varphi(1 + \overset{m}{\ldots} + 1) = m1_A$. A més, $\varphi(0) = 0_A$.

1. Ara, φ definit per $\varphi(m) = m1_A$ és morfisme d'anells. Direm que φ és el *morfisme característic* de l'anell A.
2. El nucli de φ és un ideal de $\mathbb{Z}$ i, per 4.2.3, tenim $\ker(\varphi) = (k)$, per a un enter natural k unívocament determinat. Diem que k és la característica de l'anell A. Posem $\mathrm{car}(A) = k$.
   - Si $\mathrm{car}(A) = 0$, φ és injectiu i $\mathrm{im}(\varphi) \cong \mathbb{Z}$ i A conté un subanell isomorf a $\mathbb{Z}$.
   - Si $\mathrm{car}(A) > 0$, $\mathbb{Z}/(k) \cong \mathrm{im}(\varphi)$ i A conté un subanell isomorf a $\mathbb{Z}/(k)$.

La següent proposició aprofundeix més en aquesta idea.

Proposició 4.4.14.

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

Demostració.

1. Si $f : \mathbb{Z}/(k) \longrightarrow A$, $f(\overline{1}) = 1_A$ i $f \circ \pi$ és morfisme de $\mathbb{Z}$ en A, on $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/(k)$ és el morfisme de pas al quocient. Com el morfisme característic $f \circ \pi$ és l'únic morfisme d'anells de $\mathbb{Z}$ en A, f ha de ser únic. Ara aplicant el primer teorema d'isomorfia aplicat a anells, al morfisme característic de A, obtenim un monomorfisme de $\mathbb{Z}/(k)$ en A.
2. Provem les dues implicacions:

$\Rightarrow$ Prenem $\varphi(m) = m \cdot 1_A$. Si $\text{car}(A) = k$, $(k) = \{m \mid m \cdot 1_A = 0\} = \ker(\varphi)$ i (k) és el nucli del morfisme característic de A. En conseqüència, k és el menor enter positiu tal que $k \cdot 1_A = 0_A$. Aleshores, per a $a \in A$, $ka = k\,(1_A a) = (k1_A)\,a = 0_A a = 0$.

$\Leftarrow$ Recíprocament, si k és el menor enter positiu tal que $ka = 0$, per a tot $a \in A$, aleshores com $k1_A = 0$ implica $ka = 0$ per a tot $a \in A$, k és també el menor enter positiu tal que $k1_A = 0$ i, per tant, $\text{car}(A) = k$.

3. Si $\text{car}(A) = k$, amb $k > 0$ i no primer, existeixen enters m, n amb $0 < m, n < k$ tals que $mn = k$ i els elements $m1_A, n1_A$ són divisors de zero a A. En particular, A no seria domini d'integritat.

I ja hem acabat la demostració dels tres apartats. ■

4.5 Ideals primers i maximals

Definició 4.5.1 (Ideal primer)**.** Sigui A un anell, un ideal I d'A es diu *ideal primer* si és ideal propi ($I \subsetneq A$) i es compleix el següent per a tot $a, b \in A$: $ab \in I \implies a \in I$ o bé $b \in I$.

Proposició 4.5.2. *Sigui I un ideal de l'anell A. Aleshores, I és primer si, i només si, A/I és domini d'integritat.*

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

$\Rightarrow$ Si $[a][b] = [0]$, per definició de quocient tenim que $[ab] = [0]$ i això implica que $ab \in I$. Per tant, $a \in I$ o bé $b \in I$; és a dir, $[a] = [0]$ o bé $[b] = [0]$.

$\Leftarrow$ Sigui ara $ab \in I$. Aleshores, $[ab] = [a][b] = [0]$ en A/I. Per tant, $[a] = [0]$ (de manera que $a \in I$) o bé $[b] = [0]$ (de manera que $b \in I$).

■

Proposició 4.5.3. *Els ideals primers de $\mathbb{Z}$ són (p), amb p primer, i (0).*

Definició 4.5.4 (Ideal maximal)**.** Un ideal I d'un anell A es diu maximal si és ideal propi i no existeix cap ideal J d'A tal que $I \subsetneq J \subsetneq A$. En altres paraules:

$$\left.\begin{array}{r} I \subsetneq J \implies J = A \\ I \subset J \subsetneq A \implies J = I \end{array}\right\} \iff I \text{ és maximal.} \tag{4.5.1}$$

Definició 4.5.5 (Ideal maximal, alternativa)**.** Sigui A un anell. Es diu que I un ideal d'A és maximal si

1. si $I \neq A$ i
2. si I és contingut per un ideal J, aleshores $J = I$ o bé $J = A$.

Proposició 4.5.6. *Sigui I un ideal d'un anell A. Aleshores, I és maximal si, i només si, A/I és un cos. En particular, tot ideal maximal és primer.*

Demostració.

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

$$\overline{1} = \overline{x} + \overline{\lambda}\overline{a} \implies \overline{1} = \overline{a} \cdot \overline{\lambda} \implies \overline{\lambda} \text{ és invers d'} \overline{a} \text{ en } A/I. \tag{4.5.2}$$

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

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

$$ab - 1 = x \iff 1 = ab - x \implies 1 \in J \implies J = A. \tag{4.5.3}$$

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

■

Corol·lari 4.5.7. *Tot ideal maximal és primer. En particular, els ideals maximals de $\mathbb{Z}$ són (p), amb p un enter primer.*

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

Demostració alternativa. Certament, (0) no és maximal, ja que $(0) \subsetneq (2) \subsetneq A$. De la mateixa manera, (1) no és maximal, ja que $(1) = A$. Si n és un nombre compost, que denotem per $n = kl$ per a certs k, l, tenim $(n) \subsetneq (k) \subsetneq A$ i (n) no és maximal. Finalment, sigui n un nombre primer. Suposem que I és un ideal d'A amb $(n) \subsetneq I \subsetneq A$. Prenem $a \in I \setminus (n)$. Com a no és divisible per n i n és primer, sabem que $\mathrm{mcd}(a, n) = 1$. Per la identitat de Bézout tenim que $au + nv = 1$, però com $a, n \in I$, això implica que $1 \in I$ i $I = A$ i arribem a contradicció. ■

Proposició 4.5.8. *Sigui $f : A \longrightarrow A'$ un epimorfisme d'anells i sigui P un ideal primer d'A. Aleshores, $f(P)$ és un ideal primer d'A'.*

Observació 4.5.9. Ara, sigui $\pi : A \longrightarrow I$ la projecció canònica per a un ideal I. L'assignació $P \longmapsto \pi(P)$ amb P ideal primer ens dona una *correspondència bijectiva* entre el conjunt d'ideals primers d'A que contenen I i el conjunt d'ideals primers d'A/I. Com π és epimorfisme, la seva inversa ve donada per $P \longmapsto \pi^{-1}(P)$. *Es pot veure més a l'exercici 4.7.1.*

Volem veure ara que tot anell té ideals maximals. Per provar-ho, necessitem el lema de Zorn.

Definició 4.5.10 (Element mínim i minimal)**.** Sigui S un conjunt ordenat. Diem que un element a d'S és mínim si es compleix que $a \leq x$ per a tot $x \in S$. Clarament, si S té mínim, aquest és únic. A més a més, diem que un element m d'S és *minimal* si es compleix que $x \in S$ i $x \leq m$ implica que $x = m$.

Definició 4.5.11 (Element màxim i maximal)**.** Sigui S un conjunt ordenat. Diem que un element a d'S és màxim si es compleix que $x \leq b$ per a tot $x \in S$. Clarament, si S té màxim, aquest és únic. A més a més, diem que un element m d'S és *maximal* si es compleix que $x \in S$ i $x \geq m$ implica que $x = m$.

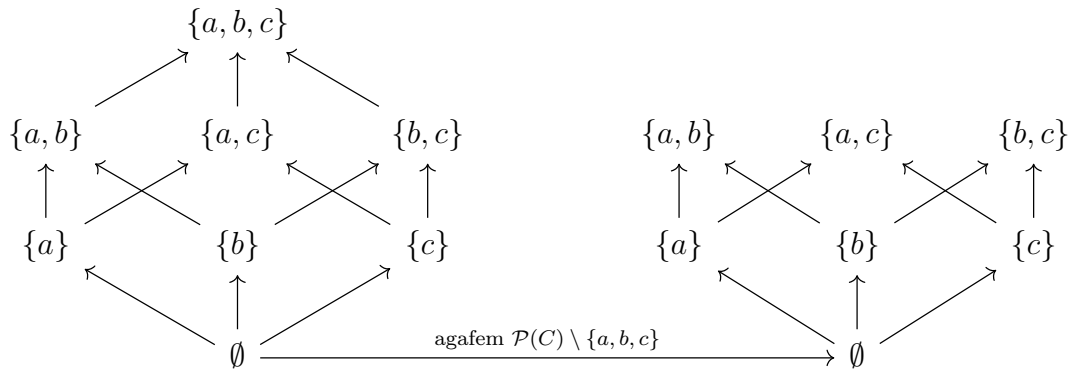
Definició 4.5.12 (Cota superior i inferior)**.** Sigui S un conjunt ordenat i T un subconjunt. Una *cota superior* de T en S és un element b d'S tal que $x \leq b$, per a tot $x \in T$. Anàlogament, anomenem *cota inferior* de T en S un element a d'S tal que $a \leq x$, per a tot $x \in T$.

Definició 4.5.13 (Ordenat inductivament)**.** Sigui S un conjunt ordenat i T un subconjunt. Diem que S està ordenat inductivament si tot subconjunt de S totalment ordenat té cota superior.

Exemple 4.5.14. Sigui $C = \{a, b, c\}$. El conjunt de les parts, $\mathcal{P}(C)$, és:

$$\mathcal{P}(C) = \{\emptyset, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}, \tag{4.5.4}$$

ordenat amb la inclusió. $\mathcal{P}(C) \setminus \{a, b, c\}$ no té màxim i té 3 maximals, $\{a, b\}, \{a, c\}, \{b, c\}$. Podríem representar-ho de la següent forma:



Al seu torn, tenim que $\mathcal{P}(C) \setminus \{a, b, c\}$.

Lema 4.5.15 (Lema de Zorn)**.** *Sigui S un conjunt no buit ordenat inductivament. Aleshores, existeix un element maximal a S.*

Proposició 4.5.16. *Sigui A un anell i $\mathfrak{a}$ un ideal propi d'A, és a dir, un ideal d'A diferent d'A. Aleshores, existeix un ideal maximal d'A que conté $\mathfrak{a}$.*

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

$$S = \{I \mid \mathfrak{a} \subset I,\ I \text{ ideal propi d'} A\}. \tag{4.5.5}$$

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

és a dir que existeix un ideal J propi de A contenint a tal que $I \subset J$, per a tot $I \in T$. Sigui J la reunió de tots els ideals de T, és a dir:

$$J = \bigcup_{I \in T} I \tag{4.5.6}$$

Vegem que J és ideal de A:

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

Vegem ara $J \subsetneq A$, és a dir, que J és un ideal propi. Raonem per reducció a l'absurd: si fos $J = A$, tindríem $1 \in J$, per tant $1 \in I$, per a algun I de T, que donaria $I = A$, que contradiu la definició de S (el conjunt dels ideals propis també és propi). Hem provat doncs que J és cota superior de T.
Aplicant el lema de Zorn, obtenim que S té un element maximal, és a dir que A té un ideal propi M contenint $\mathfrak{a}$ tal que si I és ideal propi de A i $M \subset I$, es té $M = I$. Per tant M és ideal maximal de A. ■

Corol·lari 4.5.17. *Si A és un anell i I un ideal d'A tal que $I \neq A$, aleshores A conté un ideal maximal $\mathfrak{m}$ tal que $I \subset \mathfrak{m}$.*

Demostració. Resulta immediata aplicant 4.5.16 amb $\mathfrak{a} = 0$. ■

Corol·lari 4.5.18. *Tot element no invertible està contingut en un ideal maximal.*

Demostració. Si x no és una unitat, ja hem vist que $(x) \neq A$. Per tant, podem aplicar 4.5.17 i obtenim que l'ideal generat per (x) està contingut en un ideal maximal; en altres paraules, x està contingut en tal ideal maximal. ■

Exercici 4.5.19. *Siguin A, B anells. En el producte cartesià $A \times B$ definim les operacions:*

$$(a, b) + (c, d) = (a + c, b + d) \ i \ (a, b) \times (c, d) = (ac, bd). \tag{4.5.7}$$

1. *Proveu que $(A \times B, +, \cdot)$ és un anell. Aquest anell s'anomena producte directes dels anells A i B.*
2. *Determineu quan $A \times B$ és un domini d'integritat.*
3. *Proveu que si $I \subset A$ i $J \subset B$ són ideals, llavors $I \times J$ és un ideal d'$A \times B$ i que:*

$$(A \times B)/(I \times J) \cong A/I \times B/J. \tag{4.5.8}$$

4. *Proveu que tot ideal d'$A \times B$ és de la forma $I \times J$.*

5. *Proveu que els únics ideals primers d'$A \times B$ són els de la forma $I \times B$, amb $I \subset A$ primer, o bé els de la forma $A \times J$, amb $J \subset B$ primer.*
6. *Demostreu el resultat que s'obté de l'apartat anterior en substituir primer per maximal.*

Demostració. Per provar que és un anell, s'han de complir la seva definició: una operació interna *suma* tal que $(A \times B, +)$ és grup abelià i una altra operació interna *producte* tal que és associatiu i distributiu respecte la suma:

1. Donat que $(A, +)$ i $(B, +)$ són, respectivament, grups abelians amb la suma, $(A \times B, +)$ és un grup abelià amb la suma.
2. L'associativitat es manté clarament, un altre cop, perquè A i B són anells.
3. Per veure que el producte és distributiu respecte la suma:

$$\begin{aligned} a(b+c) = (a,b)((c,d)+(e,f)) = (a,b)(c+e,d+f) = (a(c+e), b(d+f)) = (ac+ae, bd+bf), \\ ab+ac = (a,b)(c,d)+(a,b)(e,f) = (ac,bd)+(ae,bf) = (ac+ae, bd+bf). \end{aligned}$$

$$\begin{aligned} (b+c)a = ((c,d)+(e,f))(a,b) = (c+e,d+f)(a,b) = ((c+e)a, (d+f)b) = (ca+ea, db+fb), \\ ba+ca = (c,d)(a,b)+(e,f)(a,b) = (ca,db)+(ea,fb) = (ca+ea, db+fb). \end{aligned} \tag{4.5.9}$$

   On hem usat que el producte és distributiu en cadascun dels anells A i B.

Segon apartat: $A \times B$ és un domini d'integritat si tenim que $ab = (0,0)$ si, i només si, $a = 0$ o bé $b = 0$. Això és, $(a,b)(c,d) = (ac,bd) = (0,0) \iff ac = 0 \vee bd = 0$. Es veu clarament que si A (resp. B) fos un domini d'integritat, estaríem requerint que a o c (resp. b o d) fossin 0. En altres paraules, $A \times B$ és un domini d'integritat si A i B són dominis d'integritat.
Tercer apartat: Per veure que $I \times J$ és un ideal d'$A \times B$, hem de comprovar la definició:

1. $(I \times J, +)$ és subgrup de $(A \times B, +)$: siguin $a, b \in I \times J$. Aleshores:

$$(a_1, a_2) - (b_1, b_2) = (a_1 - b_1, a_2 - b_2). \tag{4.5.10}$$

   Com I és ideal, $a_1 - b_1 \in I$. El mateix per J i la segona coordenada.
2. $ax \in I \times J$: sigui $a \in A \times B$. Per a tot $x \in I \times J$ tenim $a_1 x_1 \in I$ i $a_2 x_2 \in J$, per ser I, J ideals.

Hem de veure que $(A \times B)/(I \times J)$ és isomorf a $A/I \times B/J$. Sigui:

$$\begin{array}{rccc} \varphi: & A \times B & \longrightarrow & A/I \times B/J \\ & (a,b) & \longmapsto & (\overline{a}, \overline{b}) \end{array} \tag{4.5.11}$$

Hem construït φ de manera que tot element $(a,b) \in I \times J$ sigui enviat a la classe del neutre, $\overline{\overline{0}} = (\overline{0}, \overline{0})$. La comprovació que és morfisme d'anells és rutinària. $\ker(\varphi) = I \times J$ pel que comentàvem, i $\operatorname{im}(\varphi) = A/I \times B/J$ (és exhaustiva). Així, $(A \times B)/(I \times J) \cong A/I \times B/J$ pel primer teorema d'isomorfia.
La resta d'apartats es deixen com a exercici. ■

Definició 4.5.20 (Nilradical)**.** Sigui A un anell commutatiu. El nilradical d'A és l'ideal que està format per tots els elements nilpotents de l'anell.

$$\mathfrak{N}_A = \{f \in A \mid f^m = 0 \text{ per a algun } m \in \mathbb{Z}_{>0}\}. \tag{4.5.12}$$

Proposició 4.5.21. *Sigui A un anell commutatiu. Aleshores, $\mathfrak{N}_A$ és la intersecció de tots els ideals primers $\mathfrak{p}$ de l'anell.*

Exercici 4.5.22. *Sigui A un anell commutatiu.*

1. *Demostreu que $A \setminus A^*$ (el conjunt dels invertibles) és un ideal si, i només si, A té un únic ideal maximal.*
2. *Demostreu que A té un únic ideal primer si, i només si, tot element d'A és invertible o bé nilpotent.*

Demostració. Primer apartat: Hem de demostrar les dues implicacions:

$\Rightarrow$ Per hipòtesi, $A \setminus A^*$ és ideal (compleix $ax \in A \setminus A^*$ per a tot $a \in A$). Per tant, $A \setminus A^* \neq A$ està contingut en un ideal maximal. Sabem que tot element no invertible està contingut en un ideal maximal. Aleshores, l'ideal format per totes les no-unitats, $A \setminus A^*$, és maximal. Si I' fos un altre ideal maximal (I' propi i format per no invertibles), $I' \subset A \setminus A^*$. Com tots dos són maximals, $I' = A \setminus A^*$ i $A \setminus A^*$ és l'únic ideal maximal.

$\Leftarrow$ Ara suposem que A té un únic ideal maximal, I. Com que tot element no invertible cau dins un ideal maximal, i I és l'únic ideal maximal, tot element no invertible cau dins I. Per tant, $A \setminus I$ és el conjunt d'invertibles (que forma un ideal) i $A \setminus A^* = I$ és un ideal.

Segon apartat: Un altre cop, demostrem les dues implicacions.

$\Rightarrow$ Si A té un únic ideal primer, té un únic ideal maximal, ja que tot ideal maximal és primer. Com el nilradical (l'ideal que conté tots els elements nilpotents) és la intersecció dels ideals primers, $\mathfrak{N}$ és l'únic ideal maximal. Per l'apartat anterior, $A \setminus A^* = \mathfrak{N}$ i, per tant, A està format per elements nilpotents i invertibles.

$\Leftarrow$ Recíprocament, si tot element d'A és invertible o nilpotent, $A \setminus A^*$ és el nilradical, que és un ideal. Per l'apartat anterior, $\mathfrak{N}$ és l'únic ideal maximal. Com el nilradical és la intersecció dels ideals primers, i ja hem vist que el nilradical és l'únic ideal maximal, tenim un únic ideal primer.

■

Definició 4.5.23 (Anell reduït)**.** Un anell s'anomena reduït si no té cap nilpotent no nul. Un anell és reduït si, i només si, el seu nilradical és zero. Si A és un anell commutatiu arbitrari, el seu quocient pel radical és un anell reduït i el denotem per A_{red}.

4.6 Cos de fraccions d'un domini

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

$$\left.\begin{array}{l}(a,b) \sim (a',b') \iff ab' = a'b \\ (a',b') \sim (a'',b'') \iff a'b'' = a''b'\end{array}\right\} \implies (ab'')b' = a'bb'' = a''b'b = (a''b)b' \implies ab'' = a''b \iff (a,b) \sim (a'',b''). \tag{4.6.1}$$

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

Definició 4.6.1 (Cos de fraccions d'A). Sigui $\mathbb{K}(A)$ el conjunt quocient de $A \times (A \setminus \{0\})$ per la relació d'equivalència $\sim$. Posem $\frac{a}{b}$ la classe d'(a, b) de manera que:

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b. \tag{4.6.2}$$

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

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}. \tag{4.6.3}$$

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

$$a'd'bd + c'b'bd = adb'd' + bb'cd' \implies \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}. \tag{4.6.4}$$

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

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}. \tag{4.6.5}$$

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

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd) \implies \frac{ac}{bd} = \frac{a'c'}{b'd'}. \tag{4.6.6}$$

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

Observació 4.6.2. L'aplicació:

$$\begin{array}{rccc} i: & A & \longrightarrow & \mathbb{K}(A) \\ & a & \longmapsto & \frac{a}{1} \end{array} \tag{4.6.7}$$

és monomorfisme d'anells i, per tant, podem veure A com un subanell de $\mathbb{K}(A)$.

Proposició 4.6.3. *Siguin A un domini d'integritat, L un cos i $g : A \longrightarrow L$ un monomorfisme d'anells. Aleshores, existeix un únic monomorfisme de cossos $h : \mathbb{K}(A) \longrightarrow L$ tal que $g = h \circ i$; és a dir, tal que el diagrama:*

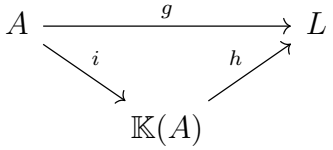


Figura 4.3: Diagrama de 4.6.3

commuta.

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

$$\begin{aligned} h\left(\frac{1}{b}\right) &= h\left(\left(\frac{b}{1}\right)^{-1}\right) = g(b)^{-1} \\ h\left(\frac{a}{b}\right) = h\left(\frac{a}{1}\cdot\frac{1}{b}\right) &= h\left(\frac{a}{1}\right)\cdot h\left(\frac{1}{b}\right) = g(a)g(b)^{-1}, \end{aligned} \tag{4.6.8}$$

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

Corol·lari 4.6.4. *Sigui A un domini d'integritat i F un cos que compleix:*

1. *Existeix un monomorfisme d'anells $f : A \longrightarrow F$.*
2. *Si L és un cos i $g : A \longrightarrow L$ és un morfisme d'anells, aleshores existeix un únic monomorfisme de cossos $h : F \longrightarrow L$ tal que $g = h \circ f$.*

Aleshores, existeix un isomorfisme de cossos $\varphi : \mathbb{K}(A) \longrightarrow F$ tal que $\varphi \circ i = f$, on $i : A \longrightarrow \mathbb{K}(A)$ i compleix $a \longmapsto \frac{a}{1}$.

Demostració. Per la proposició 4.6.3, el següent diagrama (sense tenir en consideració ψ) commuta:

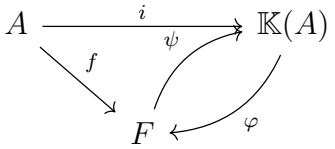


Figura 4.4: Diagrama on volem demostrar $\varphi \circ \psi = Id_F$ i $\psi \circ \varphi = Id_{\mathbb{K}(A)}$.

Fixem-nos que l'existència i unicitat del monomorfisme φ és directa per 4.6.3. Si demostrem que existeix un morfisme ψ tal que $\varphi \circ \psi = Id_F$ i $\psi \circ \varphi = Id_{\mathbb{K}(A)}$, tindrem que φ és un isomorfisme, tal com volem provar.

Aplicarem la segona propietat de la hipòtesi per dir que existeix un monomorfisme $\psi : F \longrightarrow \mathbb{K}(A)$ tal que $i = \psi \circ f$. Com $\varphi \circ i = f$ i $\psi \circ f = i$, obtenim $f = \varphi \circ i = (\varphi \circ \psi) \circ f$. Al seu torn, utilitzant les mateixes igualtats, $i = \psi \circ f = (\psi \circ \varphi) \circ i$.

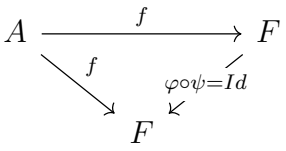


Figura 4.5: $f = \varphi \circ i = (\varphi \circ \psi) \circ f$

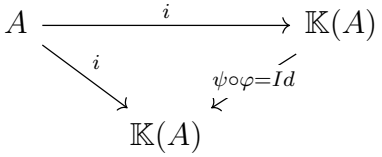


Figura 4.6: $f = \varphi \circ i = (\varphi \circ \psi) \circ f$

Fonamentalment, apliquem 4.6.3 amb $L = \mathbb{K}(A)$ i $g = i$, i obtenim $\psi \circ \varphi = Id_{\mathbb{K}(A)}$; d'altra banda, apliquem la propietat segona de la hipòtesi amb $L = F, g = f$ i queda $\varphi \circ \psi = Id_F$. D'aquesta manera, $\varphi \circ \psi = Id_F$ i $\psi \circ \varphi = Id_{\mathbb{K}(A)}$. ■

Exercici 4.6.5. *Determineu quin dels anells següents són dominis d'integritat i doneu-ne els cossos de fraccions corresponents:* $\mathbb{Z}[X]/(X), \mathbb{Z}[X]/(X^2), (\mathbb{Z}/n\mathbb{Z})[X], \mathbb{Z}[X]/(p, X)$*, amb* $p \in \mathbb{Z}$ *primer.*

Demostració.

1. $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$; per tant, és un domini d'integritat amb cos de fraccions isomorf al cos dels nombres racionals, $\mathbb{Q}$.
2. $\mathbb{Z}[X]/(X^2)$ és un anell amb un element nilpotent no nul, X; per tant, no és un domini d'integritat.
3. $(\mathbb{Z}/n\mathbb{Z})[X]$. L'anell de polinomis amb coeficients $\mathbb{Z}/n\mathbb{Z}$ és un domini d'integritat si, i només si, n és primer. El cos de fraccions és el cos de les fraccions racionals $\frac{f(X)}{g(X)}$ amb $f(X), g(X) \in (\mathbb{Z}/n\mathbb{Z})[X], g(X) \neq 0$ i $\operatorname{mcd}(f(X), g(X)) = 1$.
4. $\mathbb{Z}[X]/(p, X)$, amb $p \in \mathbb{Z}$, primer; l'anell és isomorf a $\mathbb{Z}/p\mathbb{Z}$ que és un cos i, per tant, coincideix amb el seu cos de fraccions.

■

4.7 Exercicis finals

Exercici 4.7.1.

1. *Sigui* $\varphi : \mathbb{K} \longrightarrow L$ *un morfisme d'anells commutatius. Demostreu que si* $\mathfrak{b}$ *és un ideal de* L*, llavors tenim un morfisme injectiu d'anells* $\mathbb{K}/\varphi^{-1}(\mathfrak{b}) \longrightarrow L/\mathfrak{b}$.
2. *Sigui* $\mathbb{K}$ *un anell commutatiu i* $\mathfrak{a} \subseteq \mathbb{K}$ *un ideal. Demostreu que la bijecció entre el conjunt d'ideals de* $\mathbb{K}/\mathfrak{a}$ *i el conjunt d'ideals de* $\mathbb{K}$ *que contenen* $\mathfrak{a}$ *que proporciona el morfisme de projecció* $\pi : \mathbb{K} \longrightarrow \mathbb{K}/\mathfrak{a}$ *transforma ideals primers en ideals primer i ideals maximals en ideals maximals.*

Demostració. Primer apartat: podem considerar el morfisme $\psi : \mathbb{K} \longrightarrow L/\mathfrak{b}$ composició del morfisme $\varphi : \mathbb{K} \longrightarrow L$ amb la projecció $\pi : L \longrightarrow L/\mathfrak{b}$. Llavors, $\ker(\psi) = \varphi^{-1}(\ker(\pi)) = \varphi^{-1}(\mathfrak{b})$. Per tant, pel primer teorema d'isomorfia, $\mathbb{K}/\varphi^{-1}(b) = \mathbb{K}/\ker(\psi)$ s'injecta en $L/\mathfrak{b}$ (és isomorf a la imatge de ψ, que és un subanell de $L/\mathfrak{b}$). En particular, tenim un morfisme injectiu.
Segon apartat: Podem aplicar l'apartat anterior a $L = \mathbb{K}/\mathfrak{a}$ i $\varphi = \pi : \mathbb{K} \longrightarrow L$, la projecció. En aquest cas, donat un ideal $\mathfrak{b}$ de L, com π és exhaustiu, també ho és el corresponent morfisme $\psi : \mathbb{K} \longrightarrow L/\mathfrak{b}$. Llavors, obtenim un isomorfisme $\mathbb{K}/\pi^{-1}(\mathfrak{b}) \simeq L/\mathfrak{b}$. En particular, $\mathbb{K}/\pi^{-1}(\mathfrak{b})$ és un domini d'integritat si, i només si, ho és $L/\mathfrak{b}$; és a dir, $\pi^{-1}(\mathfrak{b})$ és un ideal primer de $\mathbb{K}$ si, i només si, $\mathfrak{b}$ és un ideal primer de $\mathbb{K}/\mathfrak{a}$ i $\pi^{-1}(\mathfrak{b})$ és un ideal maximal de $\mathbb{K}$ si, i només si, $\mathfrak{b}$ és un ideal maximal de $\mathbb{K}/\mathfrak{a}$. ■

Observació 4.7.2. Respecte el segon apartat de l'exercici anterior, podem dir que els ideals primers de $\mathbb{K}/\mathfrak{a}$ es corresponen amb els ideals primers de $\mathbb{K}$ que contenen $\mathfrak{a}$, i els ideals maximal de $\mathbb{K}$ es corresponen amb els ideals maximals de $\mathbb{K}$ que contenen $\mathfrak{a}$.

Definició 4.7.3 (Contracció i extensió)**.** Siguin $f : A \longrightarrow B$ un morfisme d'anells, I un ideal d'A i J un ideal de B. $J^c := f^{-1}(J)$ és un ideal d'A i l'anomenarem contracció de J en A. Definim l'extensió d'I en B, que denotarem per I^e com l'ideal de B generat per $f(I)$.

Exercici 4.7.4.

1. *Siguin J un ideal d'A i $\pi : A \longrightarrow A/J$ el morfisme de pas al quocient. Proveu que $I^e = (I + J)/J$, per a I ideal d'A.*
2. *Considerem el morfisme d'inclusió $i : A \longrightarrow A[X]$. Proveu que $I^e = I[X]$ i que:*

$$\frac{A[X]}{I[X]} \cong \frac{A}{I}[X]. \tag{4.7.1}$$

Demostració. Primer apartat: El morfisme de pas al quocient envia tot element a la seva classe corresponent; això és, tot element de l'ideal I d'A s'envia a la seva classe en A/J. En aquest sentit, sigui $i \in I$, qualsevol. Aleshores,

$$\pi(i) = \overline{i} = \overline{i} + \overline{j} = \overline{i + j},\ j \in J. \tag{4.7.2}$$

Per tant, podem posar $a = i + j$ per a $a \in I + J$. Llavors, $\overline{a} \in (I + J)/J$ per a a arbitrari i, en conseqüència, $I^e = (I + J)/J$.
Segon apartat: L'ideal generat per $\mathfrak{a}$ en $A[X]$ conté tots els productes d'elements de $\mathfrak{a}$ per elements de A; en particular, tots els monomis $a_k X^k$, per $a_k \in \mathfrak{a}, k \geq 0$; i, per tant, totes les sumes d'aquests elements. És a dir, l'ideal generat per $\mathfrak{a}$ en $A[X]$ conté $\mathfrak{a}[X]$. I com que $\mathfrak{a}[X]$ és un ideal que conté $\mathfrak{a}$, els dos ideals $\mathfrak{a}^e$ i $\mathfrak{a}[X]$ coincideixen.
Ara, el morfisme d'anells $A \longrightarrow A/\mathfrak{a}$, que és exhaustiu, s'estén a un morfisme $A[X] \longrightarrow (A/\mathfrak{a})[X]$, també exhaustiu, el nucli del qual és exactament $\mathfrak{a}[X]$. Només cal aplicar el primer teorema d'isomorfia. ■

Exercici 4.7.5. *Sigui p un nombre natural primer.*

1. *Proveu que*

$$A := \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n > 0, \operatorname{mcd}(m, n) = 1 \text{ i } p \text{ no divideix } n \right\} \tag{4.7.3}$$

   és un subanell de $\mathbb{Q}$.
2. *Proveu que $M := \left\{ \frac{m}{n} \in A \mid p \text{ divideix } m \right\}$ és ideal maximal de A i és l'únic ideal maximal d'A.*
3. *Proveu $A/M \simeq \mathbb{Z}/p\mathbb{Z}$.*

Demostració. Primer apartat: La prova de subanell es basa en demostrar que és subgrup per la suma i el producte és tancat. En efecte:

- A és subgrup amb la suma de $\mathbb{Q}$ ja que donats $a, b \in A$ qualssevol, la diferència $a - b$ cau dins A clarament. *Indicació*: Compleix $\frac{mn'-m'n}{nn'}$ les condicions imposades per al subanell?
- A és tancat pel producte de $\mathbb{Q}$. Prenent $\frac{m'}{n'} \in A$, $\frac{mm'}{nn'} \in A$ perquè $p \nmid nn'$ (no divideix cap dels dos factors) i, després, esdevé condició necessària que $\mathrm{mcd}(m, n') = \mathrm{mcd}(m', n) = 1$.

Amb les dues condicions provades, doncs, ja hauríem acabat.

Segon apartat: M és un ideal maximal si, i només si, M és propi i donat J un ideal que el conté, aquest és $J = M$ o bé $J = A$. És clar que M és propi, ja que $p \mid m$. Per provar que aquest ideal és únic, veurem que $A \setminus A^*$ és un ideal que, concretament, serà M. Per definició,

$$A \setminus A^* = \left\{ \frac{m}{n} \in A \;\middle|\; p \nmid n, m \right\}. \tag{4.7.4}$$

Tenim que $M = A \setminus A^*$ i, per tant, $A \setminus A^*$ és un ideal i M és l'únic ideal maximal.

Tercer apartat: Ara, construïm un morfisme de la següent manera:

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & \frac{m}{n} & \longmapsto & \overline{mn} \end{array} \tag{4.7.5}$$

És un morfisme exhaustiu tal que $\ker(\varphi) = M$. Pel primer teorema d'isomorfia, existeix un isomorfisme entre A/M i $\mathbb{Z}/p\mathbb{Z}$ i $A/M \cong \mathbb{Z}/p\mathbb{Z}$. ■

Exercici 4.7.6. *Sigui $A = \mathbb{R}[X]$ i considerem $I = (X^2 + 1)$ i $J = (X^2 + 3)$ ideals d'A.*

1. *Determineu un sistema de representants d'A/I. Proveu que A/I és un cos isomorf al cos dels nombres complexos.*
2. *Demostreu que $A/I \cong A/J$ i expliciteu un isomorfisme.*

Demostració. Com A és, en particular, un domini d'integritat i I és un ideal, A/I és l'anell quocient d'A per I. Per definició d'ideal i, en concret, d'I, tenim que $(x^2+1)q(x) \in I$ per a tot $q(x) \in \mathbb{R}[X]$. Siguin $p(x), r(x) \in \mathbb{R}[X]$ tals que $\overline{p(x)} = \overline{r(x)}$, és a dir, que:

$$\overline{p(x)} - \overline{r(x)} = \overline{0} \xrightarrow{\text{anell quocient}} \overline{p(x) - r(x)} = \overline{0}, \tag{4.7.6}$$

i $p(x) - r(x) = q(x)(x^2 + 1)$, amb $\mathrm{gr}(r(x)) \leq 1$. Per tant, podem triar com a conjunt de representants de $\mathbb{R}[X]/(x^2 + 1)$ polinomis de la forma $aX + b$ (de grau més petit o igual a 1). Per provar que $A/I \simeq \mathbb{C}$, cal trobar una aplicació φ_1 que factoritzi a través del quocient:

$$\begin{array}{rccc} \varphi_1: & \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ & p(x) & \longmapsto & p(i) \end{array} \tag{4.7.7}$$

És un morfisme d'anells clarament. A la vegada, tenim que $\ker(\varphi_1) = (x^2 + 1) \iff x^2 + 1 = 0 \iff x = i$ (d'aquí la definició de l'aplicació). Com que $\mathrm{im}(\varphi_1) = \mathbb{C}$, pel primer teorema d'isomorfia existeix un isomorfisme $\tilde{\varphi_1}$ entre $\mathbb{R}[X]/(x^2 + 1)$ i els complexos; en altres paraules, $A/I \cong \mathbb{C}$. També es podria haver fet a partir de la definició del producte en els complexos.

Segon apartat: Ens val amb demostrar que $\mathbb{R}[x]/(x^2+3) \cong \mathbb{C}$; això, és, trobar un isomorfisme entre aquests dos anells. El procediment és el mateix que a l'apartat anterior: cal trobar una aplicació φ_2 que factoritzi a través del quocient:

$$\begin{array}{rccc} \varphi_2: & \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ & p(x) & \longmapsto & p(\sqrt{3}i) \end{array} \tag{4.7.8}$$

És un morfisme d'anells clarament. A la vegada, tenim que $\ker(\varphi_2) = (x^2+3) \iff x^2+3 = 0 \iff x = \sqrt{3}i$. Com que $\mathrm{im}(\varphi_2) = \mathbb{C}$, pel primer teorema d'isomorfia $A/J \cong \mathbb{C}$. Ja tenim que $A/I \cong A/J$, donat que tots dos són isomorfs al cos dels complexos. De totes maneres, se'ns demana un isomorfisme explícit.
Per últim, l'isomorfisme entre $A/(X^2+1)$ i $A/(X^2+3)$ es pot raonar de la següent manera:

$$\begin{array}{ccc} A & \xrightarrow{\quad\psi\quad} & A/(X^2+3) \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle i} \\ A/\ker(\psi) & \xrightarrow{\quad\tilde{\psi}\quad} & \mathrm{im}(\psi) \end{array} \qquad \begin{array}{rccc} \psi: & A & \longrightarrow & A/(X^2+3) \\ & p(x) & \longmapsto & \overline{p\left(\frac{x}{\sqrt{3}}\right)} \end{array} \tag{4.7.9}$$

Certament, si agafem $p(x) \in (X^2+1)$ (posem, sense pèrdua de generalitat, $p(x) = x^2+1$) resulta

$$\psi(x^2+1) = \overline{\frac{x^2}{3}+1} = \frac{\overline{1}}{3} \cdot \overline{x^2+3} = \overline{0}. \tag{4.7.10}$$

Per tant, $\ker(\psi) = (X^2+1)$ i obtenim l'isomorfisme $\tilde{\psi} : A/(X^2+1) \longrightarrow A/(X^2+3)$ desitjat pel primer teorema d'isomorfia per a anells. ■

Observació 4.7.7. En l'exercici anterior, $A/(X^2+1)$ és un cos. Primerament, pel fet de ser isomorf al cos dels complexos. Després, com que A és un domini d'ideals principals (com $\mathbb{R}$ és un cos, $\mathbb{R}[X]$ és domini d'ideals principals) i x^2+1 és irreductible en A, per 5.3.10, (X^2+1) és maximal. Donat que A és anell commutatiu amb unitat i (X^2+1) és maximal, $A/(X^2+1)$ és un cos.

Exercici 4.7.8.

1. *Demostreu que, donat un morfisme d'anells commutatius, la contracció d'un ideal primer és, en efecte, un ideal primer.*
2. *Considerem la injecció de $\mathbb{Z}$ en $\mathbb{Z}[i]$. Proveu que l'extensió de l'ideal (2) no és un ideal primer.*
3. *Siguin K un anell commutatiu i $\mathfrak{p}$ un ideal primer. Proveu que l'extensió de $\mathfrak{p}$ a $K[X]$ és un ideal primer.*

Demostració. Primer apartat: Si $\varphi : K \longrightarrow L$ és un morfisme d'anells commutatius i J és un ideal primer de L, sigui $ab \in \varphi^{-1}(J)$; aleshores, $\varphi(ab) \in J$ i, per la definició de morfisme d'anells, $\varphi(a)\varphi(b) \in J$. Pel fet que J és un ideal primer, $\varphi(a) \in J$ o bé $\varphi(b) \in J$. $J^c = f^{-1}(J)$ és, per tant, un ideal primer.
Segon apartat: L'ideal (2) en $\mathbb{Z}$ és justament $2\mathbb{Z}$. Per tant, l'extensió de $2\mathbb{Z}$ en $\mathbb{Z}[i]$ és justament $2\mathbb{Z}[i]$. Tot element de $2\mathbb{Z}[i]$ té la forma $2(a+bi)$, on $a, b \in \mathbb{Z}$. Com a contraexemple, podem prendre $ab = (1+i)^2 = 2i \in 2\mathbb{Z}[i]$ i $a = b \notin 2\mathbb{Z}[i]$.
Tercer apartat: $\mathfrak{p}$ és ideal primer d'A si, i només si, $A/\mathfrak{p}$ és domini d'integritat si, i només si, $(A/\mathfrak{p})[X]$ és domini d'integritat si, i només si, $\frac{A[X]}{[X]}$ és domini d'integritat si, i només si, $\mathfrak{p}$ és ideal primer en $A[X]$. Hem d'observar que $\mathfrak{p}$ en $A[X]$ és $\mathfrak{p}[X]$. ■

V

Factorialitat

5.1

DIVISIBILITAT

Definició 5.1.1 (Elements associats)**.** Dos elements a, b d'un anell A es diuen associats si existeix una unitat $u \in A$ (element invertible) tal que $b = ua$. Posem $a \sim b$ per indicar que a i b són associats. Clarament, la relació $\sim$ és d'equivalència.

Proposició 5.1.2. *Sigui A un anell, $a, b \in A$. Si més no un dels dos elements a, b és no divisor de zero, es compleix:*

$$a \mid b \text{ i } b \mid a \iff a \sim b. \tag{5.1.1}$$

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

Demostració. Si $a \sim b$, tenim $b = ua$, amb u unitat i, per tant, $a \mid b$ i, si v és l'invers d'u, tenim $a = vb$, que implica $b \mid a$. Si $a \mid b$ i $b \mid a$, tenim $b = ac$ i $a = bd$, per a certs elements $c, d \in A$. Suposem que a no és divisor de zero. Aleshores, $a = bd = acd$ implica que $1 = cd$; per tant, c i d són unitats. ■

Definició 5.1.3 (Divisors propis)**.** Si a és un element no nul d'un anell A, les unitats d'A i els elements associats d'a divideixen a. Direm divisors propis d'a els divisors d'a diferents d'aquests.

Definició 5.1.4 (Element irreductible)**.** Un element a no nul d'un domini d'integritat d'A s'anomena *irreductible* si no és una unitat i no té divisors propis. Un element a no nul i no unitat s'anomena compost si té divisors propis.

Exemple 5.1.5. Els elements irreductibles de $\mathbb{Z}$ són els $\pm p$ amb p primer. Si $\mathbb{K}$ és cos, els elements irreductibles de $\mathbb{K}[X]$ són els polinomis de grau més gran o igual que 1, irreductibles.

Definició 5.1.6 (Màxim comú divisor)**.** Siguin A un anell, $a, b, d \in A$. Diem que d és un màxim comú divisor d'a i b si se satisfan les dues propietats següents:

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

Definició 5.1.7 (Mínim comú múltiple)**.** Siguin A un anell i $a, b, m \in A$. Diem que m és un màxim comú múltiple d'a i b si se satisfan les dues propietats següents:

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

Observació 5.1.8. Tenint en compte 5.1.2, si A és domini d'integritat i $a, b, d \in A$ tals que d és màxim comú divisor d'a i b, aleshores $d' \in A$ és màxim comú divisor d'a i b si, i només si, d' és associat de d ($d' \mid d$ i $d \mid d'$, per la segona propietat del màxim comú divisor). Anàlogament, el mínim comú múltiple queda determinat tret d'associats.

5.2

Dominis euclidians

5.2.1 Dominis euclidians

Definició 5.2.1 (Domini euclidià)**.** Sigui A un domini d'integritat. Direm que A és un domini euclidià si existeix una aplicació $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

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

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

Exemple 5.2.2. $\mathbb{Z}$ és domini euclidià amb $\delta(a) = |a|$, per a $a \in \mathbb{Z} \setminus \{0\}$. Si $\mathbb{K}$ és un cos, $\mathbb{K}[X]$ és un domini euclidià amb $\delta(P) = \mathrm{gr}(P)$, per a $P \in \mathbb{K}[X] \setminus \{0\}$.

Proposició 5.2.3. *Sigui (A, δ) un domini euclidià. Siguin $a, b \in A \setminus \{0\}$.*

1. *Si a, b són associats, aleshores $\delta(a) = \delta(b)$.*
2. *Si $a \mid b$ i $\delta(a) = \delta(b)$, aleshores a, b són associats.*

Demostració.

1. Si a, b són associats, tenim $a \mid b$ i $b \mid a$, respectivament; per tant, $\delta(a) \leq \delta(b)$ i $\delta(b) \leq \delta(a)$, respectivament. Així, necessàriament, $\delta(a) = \delta(b)$.
2. La divisió entera d'a entre b respecte de δ ens dona que existeixen $q, r \in A$ tals que $a = qb + r$, amb $\delta(r) < \delta(b)$ sempre que $r \neq 0$. Com $a \mid b$, existeix $a' \in A$ tal que $b = a'a$. Per tant, $r = a - qb = a - qa'a = (1 - qa')a$. Si $r \neq 0$, tindríem que $\delta(a) \leq \delta(r)$ pel fet que $a \mid r$ (recordem 5.2.1), i també que $\delta(r) < \delta(b)$ (per la definició de divisió entera). Obtenim que $\delta(a) \leq \delta(r) < \delta(b)$, en contradicció de la hipòtesi $\delta(a) = \delta(b)$. Tenim, doncs, $r = 0$ i $b \mid a$. Com $a \mid b$ per hipòtesi, tenim $a \sim b$.

■

Observació 5.2.4. En general no és cert que $\delta(a) = \delta(b) \implies a \sim b$. En el cas de $\mathbb{Z}$, $|m| = |n|$ sí implica que m i n són associats, però a $\mathbb{K}[X]$ tenim, per exemple, X i $X + 1$ amb el mateix grau i no associats.

Corol·lari 5.2.5. *Un element $a \in A \setminus \{0\}$ és una unitat si, i només si, $\delta(a) = \delta(1)$.*

Demostració. Un element $a \in A \setminus \{0\}$ és una unitat; en altres paraules, una unitat a és element associat a 1; per tant, $\delta(a) = \delta(1)$. Com $1 \mid a$, si $\delta(a) = \delta(1)$, tenim a associat a 1 i, per tant, a és una unitat. ■

Proposició 5.2.6. *Tot domini euclidià és domini d'ideals principals.*

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

5.2.2 Normes euclidianes

Definició 5.2.7 (Norma euclidiana)**.** Sigui A un anell. Una norma d'A és una aplicació $N : A \longrightarrow \mathbb{Z}$ tal que compleix les següents propietats:

1. Si $a \in A$, $N(a) = 0$ si, i només si, $a = 0$;
2. $N(ab) = N(a)N(b)$ per a qualssevol elements a, b d'A.

Exemple 5.2.8. La identitat és una norma per a $\mathbb{Z}$. Si $\mathbb{K}$ és cos, l'aplicació $P \longmapsto 2^{\mathrm{gr}(P)}$, si $P \neq 0$ i $0 \longmapsto 0$ és una norma per a $\mathbb{K}[X]$.

Proposició 5.2.9. *Sigui A un anell que té una norma N; aleshores:*

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

Demostració.

1. Siguin $a, b \in A$ tals que $ab = 0$. Prenent normes, tenim $N(a)N(b) = N(ab) = N(0) = 0$. Com $\mathbb{Z}$ és domini d'integritat, hem de tenir $N(a) = 0$ o bé $N(b) = 0$ i, per la primera propietat de la definició de norma, $a = 0$ o bé $b = 0$.
2. Siguin $a, b \in A \setminus \{0\}$ tals que $a \mid b$. Aleshores, tenim $b = ac$ per a un cert $c \in A \setminus \{0\}$ i $N(b) = N(a)N(c)$. Com $|N(c)| \geq 1$, obtenim $|N(a)| \leq |N(b)|$.
3. Tenim $1 \cdot 1 = 1$ i, prenent normes, $N(1)N(1) = N(1)$, que implica $N(1) = 1$.
4. Si $u \in A^*$, tenim $uv = 1$ per a un cert $v \in A$ i, prenent normes, $N(u)N(v) = N(1) = 1$, que implica $N(u) \in \mathbb{Z}^*$ i, per tant, $N(u) = \pm 1$.

■

Observació 5.2.10. Per a un anell $\mathbb{Z}[\sqrt{d}]$, amb d lliure de quadrats, l'últim apartat és una equivalència; és a dir, si tenim A un anell que té una norma N, $u \in A^* \iff N(u) = \pm 1$. Estudiarem aquest tipus d'anells més a fons en el següent exemple.

Exemple 5.2.11. Per a un nombre enter lliure de quadrats, d, considerem $\mathbb{Z}[\sqrt{d}] := \{a+b\sqrt{d} : a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Comprovem que $\mathbb{Z}[\sqrt{d}]$ és subanell de C. Si $\left(a_1+b_1\sqrt{d}\right), \left(a_2+b_2\sqrt{d}\right) \in \mathbb{Z}[\sqrt{d}]$, tenim

$$\begin{aligned}\left(a_1+b_1\sqrt{d}\right) - \left(a_2+b_2\sqrt{d}\right) &= (a_1-a_2) + (b_1-b_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \\ \left(a_1+b_1\sqrt{d}\right)\left(a_2+b_2\sqrt{d}\right) &= (a_1a_2+db_1b_2) + (a_1b_2+a_2b_1)\sqrt{d} \in \mathbb{Z}[\sqrt{d}],\end{aligned} \tag{5.2.1}$$

Definim l'aplicació

$$\begin{aligned}N : \mathbb{Z}[\sqrt{d}] &\to \mathbb{Z} \\ a+b\sqrt{d} &\mapsto (a+b\sqrt{d})(a-b\sqrt{d}) = a^2-db^2.\end{aligned} \tag{5.2.2}$$

Comprovem que l'aplicació N és una norma. Clarament $N(0)=0$. Recíprocament sigui $a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ amb $N(a+b\sqrt{d}) = a^2-db^2 = 0$. Si $b \neq 0$, tenim $d=(a/b)^2$, que contradiu d lliure de quadrats; ara, $b=0$ implica $a=0$. Vegem ara la segona propietat de la definició de norma. Si $\left(a_1+b_1\sqrt{d}\right), \left(a_2+b_2\sqrt{d}\right) \in \mathbb{Z}[\sqrt{d}]$, tenim

$$\begin{aligned}&N\left(\left(a_1+b_1\sqrt{d}\right)\left(a_2+b_2\sqrt{d}\right)\right) = N\left((a_1a_2+db_1b_2)+(a_1b_2+a_2b_1)\sqrt{d}\right) \\ &= \left((a_1a_2+db_1b_2)+(a_1b_2+a_2b_1)\sqrt{d}\right)\left((a_1a_2+db_1b_2)-(a_1b_2+a_2b_1)\sqrt{d}\right) \\ &N\left(a_1+b_1\sqrt{d}\right)N\left(a_2+b_2\sqrt{d}\right) = \left(a_1+b_1\sqrt{d}\right)\left(a_1-b_1\sqrt{d}\right)\left(a_2+b_2\sqrt{d}\right)\left(a_2-b_2\sqrt{d}\right) \\ &= \left(a_1+b_1\sqrt{d}\right)\left(a_2+b_2\sqrt{d}\right)\left(a_1-b_1\sqrt{d}\right)\left(a_2-b_2\sqrt{d}\right) \\ &= \left((a_1a_2+db_1b_2)+(a_1b_2+a_2b_1)\sqrt{d}\right)\left((a_1a_2+db_1b_2)-(a_1b_2+a_2b_1)\sqrt{d}\right)\end{aligned} \tag{5.2.3}$$

Per a $\alpha = a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}], N(\alpha) = \pm 1$ implica α invertible. En efecte, si $N(\alpha)=1, a-b\sqrt{d}$ és invers de α i, si $N(\alpha)=-1, -a+b\sqrt{d}$ és invers de α.

5.3 Factorització en un domini d'ideals principals

Proposició 5.3.1. *Si A és un domini d'ideals principals, llavors d és un màxim comú divisor d'a i b si, i només si, es compleix la igualtat d'ideals principals $(d)=(a,b)$ i sempre existeix el màxim comú divisor de dos elements.*

Demostració.

⇒ Si d és màxim comú divisor d'a i b, tenim $d \mid a$ i $d \mid b$; per tant, $a \in (d)$ i $b \in (d)$ i obtenim $(a,b) \subset (d)$ (l'ideal generat per aquests dos elements es troba contingut en l'ideal generat per d). Com A és domini d'ideals principals, tenim $(a,b)=(c)$, per a un cert $c \in A$. Com $a \in (c)$, tenim $c \mid a$, i com $b \in (c)$, $c \mid b$. Per la segona propietat de la definició de màxim comú divisor tenim $c \mid d$; per tant, $(a,b) \subset (d) \subset (c) = (a,b)$ i $(d)=(a,b)$.

⇐ Recíprocament, si $(a,b)=(d)$, tenim $a,b\in(d)$; per tant, $d\mid a$ i $d\mid b$. Si $c\mid a$ i $c\mid b$, tenim $c\mid ma+nb$, per a $m,n\in A$ qualssevol ($c\mid a \implies c\mid ma$ i $c\mid b \implies c\mid nb$ de manera que $c\mid ma+nb$) i, en particular, $c\mid d$, ja que per $(d)=(a,b)$, d és combinació lineal d'a i b. Per tant, d és màxim comú divisor d'a i b.

Com hem demostrat les dues implicacions, cap a l'esquerra i cap a la dreta, ja hem acabat. ■

Volem veure que en un domini d'ideals principals, tot element diferent de zero i no unitat és producte d'elements irreductibles.

Proposició 5.3.2. *Sigui A un domini d'integritat i a un element d'A diferent de zero i no unitat. Si a no és producte d'elements irreductibles, aleshores existeix una successió $\{a_n\}_{n\in\mathbb{N}}$ d'elements d'A tals que a_{n+1} és divisor propi d'a_n, per a tot $n\in\mathbb{N}$.*

Demostració. Construirem inductivament una successió amb la propietat de l'enunciat i, a més, de forma que a_n no és producte d'irreductibles per a tot n. Posem $a_0=a$ i suposem que $a_0,\dots,a_n, n\geq 0$, ja estan construïts. Com a_n no és producte d'irreductibles, ha de ser compost, i ho denotarem per $a_n=bc$, amb b,c divisors propis de a_n i, clarament al menys un dels dos factors no pot ser producte d'irreductibles (b i c no unitats). En altres paraules, almenys b o c no és producte d'irreductibles i posem $a_{n+1}=b$ o c, el que no és producte d'irreductibles. ■

Proposició 5.3.3. *Sigui A un domini d'ideals principals i $\{a_n\}_{n\geq 1}$ una successió d'elements d'A tal que $(a_n)\subset(a_{n+1})$ per a tot n. Aleshores, existeix $m\in\mathbb{N}$ tal que $(a_n)=(a_m)$, per a tot $n\geq m$.*

Demostració. Prenem $I=\bigcup_{n\geq 1}(a_n)$, que és un ideal d'A (la reunió d'ideals és ideal). Com, per hipòtesi, tot ideal d'A és principal, és $I=(a)$, per a un cert $a\in I$. Ara, $a\in I$ implica que $a\in(a_m)$, per a algun m i, per tant, per a $n\geq m$:

$$(a_m)\subset(a_n)\subset(a)\subset(a_m) \implies (a_n)=(a_m). \tag{5.3.1}$$

■

Demostració anàloga, feta a classe. Prenem $I=\bigcup_{n\geq 1}(a_n)$, que és un ideal d'A (la reunió d'ideals és ideal). Prenem $b,c\in I$, de manera que podem triar n_1 i n_2 tals que $b\in(a_{n_1})$ i $c\in(a_{n_2})$. Si $n_1\leq n_2$ aleshores $(a_{n_1})\subset(a_{n_2})$ i $b,c\in(a_{n_2}) \implies b-c\in(a_{n_2})\subset I$. Si $x\in A$ i $b\in I$, $b\in(a_n)$ implica que $xb\in(a_n)\subset I$. Com que A és domini d'ideals principals, $I=(a)$ per a algun $a\in A$ i $a\in(a_m)$. Per tant, $I=(a)\subset(a_m)\subset(a_n)\subset I$ per a $n\geq m$ i obtenim $(a_n)=(a_m)$ per a tot $n\geq m$. ■

Corol·lari 5.3.4. *Sigui A un domini d'ideals principals. Si $a\in A\setminus\{0\}$ i a no és una unitat, existeixen elements irreductibles $p_1,\dots,p_r$ tals que $a=p_1\cdots p_r$.*

Demostració. Si existís un element a no nul i no unitat d'A que no fos producte d'elements irreductibles, tindríem una successió (a_n) d'elements d'A amb a_{n+1} divisor propi d'a_n, per 5.3.2. Aleshores, les inclusions d'ideals $(a_n)\subset(a_{n+1})$ serien estrictes (és a dir, subconjunts propis), en contradicció amb la proposició anterior. ■

Exemple 5.3.5. Sigui $A = \{x \in \mathbb{C} \mid z \text{ és arrel de } P(x) \in \mathbb{Z}[X], P(x) \text{ mònic}\}$ subanell de $\mathbb{C}$. A és anell dels enters algebraics tals que $\sqrt{2} \in A$ arrel de $X^2 - 2$, $\sqrt[n]{2} \in A$, arrel de $X^n - 2$ i $\frac{1}{\sqrt{2}} \notin A$ arrel de $X^2 - \frac{1}{2}$ i

$$(\sqrt{2}) \subsetneq (\sqrt[4]{2}) \subsetneq \cdots \subsetneq (\sqrt[2^n]{2}) \tag{5.3.2}$$

Definició 5.3.6 (Element primer)**.** Un element p d'un domini d'integritat A es diu primer si p és no nul i no unitat, i per a $a, b \in A$ es compleix:

$$p \mid ab \implies p \mid a \text{ o bé } p \mid b. \tag{5.3.3}$$

Proposició 5.3.7. *En un domini d'integritat, tot element primer és irreductible.*

Demostració. Sigui p un element primer d'A i suposem $p = ab$, Aleshores, $p \mid ab \implies p \mid a$ o $p \mid b$. Suposem $p \mid a$. Aleshores, existeix $c \in A$ tal que $a = pc$. Aleshores, $a = pc = abc$ i, per tant, $1 = bc$ (per la propietat cancel·lativa dels dominis d'integritat). L'element b és, per tant, una unitat i p és irreductible (la seva factorització és única exceptuant associats). ■

Proposició 5.3.8. *En un domini d'integritat A, un element p no nul és primer si, i només si, l'ideal (p) és primer.*

Demostració. En efecte, per a $a \in A$, la condició $p \mid a$ equival a $a \in (p)$. ■

Proposició 5.3.9. *En un domini d'ideals principals, tot element irreductible és primer.*

Demostració. Sigui p un element irreductible d'un domini d'ideals principals A. Volem veure que p és primer. Suposem $p \mid ab$ i $p \nmid a$. De la definició d'irreductible, es dedueix que p i a són coprimers, és a dir, $\text{mcd}(a, p) = 1$. Tenim, doncs, la igualtat d'ideals $(a, p) = (1)$; per tant, existeixen elements $p', a' \in A$ tals que $1 = pp' + aa'$ d'on $b = pp'b + aba'$ (realment, $ba'a$, però el producte és commutatiu ja que estem en un domini d'integritat). Com p és factor del primer sumand i, per hipòtesi, $p \mid ab$, obtenim $p \mid b$. ■

Proposició 5.3.10. *Sigui A un domini d'ideals principals. Un element no nul p d'A és irreductible si, i només si, l'ideal (p) és maximal. Per tant, en un domini d'ideals principals tot ideal primer no nul és maximal.*

Demostració. Hem de provar les dues implicacions:

⇒ Sigui p un element irreductible d'A i suposem que existeix un ideal I d'A tal que $(p) \subset I$. Com A és domini d'ideals principals, tenim $I = (a)$ per a un cert $a \in A$. Ara, $(p) \subset (a)$ implica $a \mid p$ i com p és irreductible,

1. a ha de ser una unitat, que implica $(a) = A$;
2. o a associat de p, que implica $(a) = (p)$.

Tenim, doncs, que (p) és maximal.

⇐ Recíprocament, sigui p un element no nul d'A tal que l'ideal (p) és maximal. Sigui $a \in A$ un divisor de p. La relació $a \mid p$ implica $(p) \subset (a)$ i, com (p) és maximal, ha de ser $(p) = (a)$. La relació $a \mid p$ implica $(p) \subset (a)$ i, com (p) és maximal, ha de ser:

- $(p) = (a)$, que implica a associat de p,
- o $(a) = A$, que implica a unitat.

Com ja hem provat les dues implicacions, hem acabat. ■

Proposició 5.3.11. *Sigui a un element no nul i no unitat d'un domini d'ideals principals A i $a = p_1 \dots p_r$ una descomposició d'a en producte d'elements irreductibles. Si p és irreductible, $p \mid a$ si i només si existeix un índex $i, 1 \leq i \leq r$, tal que p i p_i són associats.*

Demostració. Si $p \mid a = p_1 \dots p_r$, com p és primer, per la proposició 5.3.9, tenim $p \mid p_i$, per a algun i. Com p_i és irreductible i p no és unitat, p i p_i han de ser associats. ■

Corol·lari 5.3.12. *Siguin $p_1, \dots, p_r, q_1, \dots, q_s$ elements irreductibles d'un domini d'ideals principals A i suposem $p_1 \dots p_r = q_1 \dots q_s$. Aleshores, $r = s$ i existeix una permutació σ de $\{1, \dots, r\}$ tal que $p_i \sim q_{\sigma(i)}, 1 \leq i \leq r$.*

Demostració. Veurem que existeix σ com a l'enunciat, donant successivament $\sigma(1)$ tal que $p_1 \sim q_{\sigma(1)}, \sigma(2)$ tal que $p_2 \sim q_{\sigma(2)}$ i, en general, $p_i \sim q_{\sigma(i)}$, per a tot $i = 1 \div r$.
Si $p_1 \dots p_r = q_1 \dots q_s$, tenim $p_1 \mid q_1 \dots q_s$ i per 5.3.11 existeix $j_1 \in \{1, 2, \dots s\}$ tal que p_1 és associat de q_{j_1}. Tenim doncs $p_1 = u_1 q_{j_1}$, amb u_1 unitat. Posem $\sigma(1) = j_1$. Ara tenim $u_1 q_{j_1} p_2 \dots p_r = q_1 \cdots q_s$ i, simplificant el factor q_{j_1}, obtenim

$$u_1 p_2 \cdots p_r = q_1 \cdots q_{j_1 - 1} q_{j_1 + 1} q_s. \tag{5.3.4}$$

Tenim $p_2 \mid q_1 \dots q_{j_1-1} q_{j_1+1} q_s$ i, de nou per 5.3.11, existeix $j_2 \in \{1, 2, \dots s\}, j_2 \neq j_1$ tal que p_2 és associat de q_{j_2}. Tenim doncs $p_2 = u_2 q_{j_2}$, amb u_2 unitat. Posem $\sigma(2) = j_2$. Ara tenim

$$u_1 u_2 q_{j_2} p_3 \cdots p_r = q_1 \cdots q_{j_1 - 1} q_{j_1 + 1} q_s \tag{5.3.5}$$

i, simplificant el factor q_{j_2}, obtenim

$$u_1 u_2 p_3 \cdots p_r = \prod_{j \neq j_1, j_2} q_j. \tag{5.3.6}$$

Repetim el procés. Notem que no pot ser $r > s$ ja que arribaríem a $u_1 \cdots u_s p_{s+1} \cdots p_r = 1$ que donaria $p_{r+1}, \dots, p_s$ unitats, que seria absurd. Tampoc no pot ser $r < s$, ja que en aquest cas, arribaríem a $u_1 \cdots u_r = \prod_{j \neq j_1, \dots, j_r} q_j$, que donaria que els q_j que queden a la dreta de la igualtat són unitats, un altre cop absurd. Tenim doncs $r = s$ i existeix una permutació σ de $\{1, \dots, r\}$ tal que $p_i \sim q_{\sigma(i)}, 1 \leq i \leq r$. ■

5.4 Dominis de factorització única

Definició 5.4.1 (Domini de factorització única)**.** Un domini d'integritat A es diu *domini de factorització única* si es compleixen les dues propietats següents:

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

Definició 5.4.2 (Domini de factorització)**.** Si A és un domini d'integritat que compleix la primera propietat de la factorització única, direm simplement que és un *domini de factorització.*

Proposició 5.4.3. *Sigui un domini de factorització única A. Si $p_1, \dots, p_r, q_1, \dots, q_s$ són elements irreductibles d'A tals que $p_1 \cdots p_r = q_1 \cdots q_s$, aleshores, $r = s$ i existeix una permutació σ de $\{1, \dots, r\}$ tal que $p_i \sim q_{\sigma(i)}$ i $1 \leq i \leq r$.*

Demostració. En efecte, es dedueix de la propietat segona de la definició. ■

Observació 5.4.4. Tenim que tot domini euclidià és un domini d'ideals principals. Al seu torn, tot domini d'ideals principals és domini de factorització única. Es dona, doncs, aquesta cadena d'equivalències.

Proposició 5.4.5. *Sigui A un domini de factorització. Aleshores, A és domini de factorització única si, i només si, tot element irreductible d'A és primer.*

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

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

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

$$p \mid p_1 \cdots p_r q_1 \cdots q_s \implies \left.\begin{matrix} p \sim p_i \implies p \mid a \\ p \sim q_j \implies p \mid b \end{matrix}\right\} \; p \mid a \text{ o bé } p \mid b \implies p \text{ primer.} \tag{5.4.1}$$

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

Exemple 5.4.6 (Identificació de dominis de factorització única)**.** Donem ara un exemple d'anell que no és domini de factorització única. Considerem l'anell $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Tenim la igualtat següent: $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Volem veure que $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ són elements irreductibles d'aquest anell i, per tant, $6 = 2 \cdot 3$ i $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ són dues descomposicions de 6 en producte d'irreductibles.
Considerem la norma de $\mathbb{Z}[\sqrt{-5}]$ definida per

$$N = (a + b\sqrt{-5}) = a^2 + 5b^2, \; a, b \in \mathbb{Z}. \tag{5.4.2}$$

Observem que $N(\alpha) \geq 0$ per a tot $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Els elements invertibles de $\mathbb{Z}[\sqrt{-5}]$ són els de la norma igual a 1. L'equació $a^2 + 5b^2 = 1$ només té les solucions enteres $a = \pm 1, b = 0$; per tant, $(\mathbb{Z}[\sqrt{-5}])^* = \{\pm 1\}$. Tenim:

$$\begin{array}{cc} N(2) = 4 & N(3) = 9 \\ N(1+\sqrt{-5}) = 6 & N(1-\sqrt{-5}) = 6 \end{array} \tag{5.4.3}$$

- Si 2 no fos irreductible, tindríem $2 = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$, no unitats. I $4 = N(2) = N(\alpha)N(\beta)$,

$$\begin{cases} N(\alpha) = 1, N(\beta) = 4 \implies \alpha \text{ invertible}, \\ N(\alpha) = 2, N(\beta) = 2 \implies \alpha \text{ a continuació veiem que no pot ser}, \\ N(\alpha) = 4, N(\beta) = 1 \implies \beta \text{ invertible}. \end{cases} \tag{5.4.4}$$

  Hauria de ser, doncs, $N(\alpha) = N(\beta) = 2$, però l'equació $a^2 + 5b^2 = 2$ no té solucions enteres (2 no és un quadrat mòdul 5); per tant, a $\mathbb{Z}[\sqrt{-5}]$ no hi ha elements de norma 2 i tenim que 2 és irreductible.
- Si 3 no fos irreductible, tindríem $3 = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$, no unitats. $9 = N(3) = N(\alpha)N(\beta)$,

$$\begin{cases} N(\alpha) = 1, N(\beta) = 9 \implies \alpha \text{ invertible}, \\ N(\alpha) = 3, N(\beta) = 3 \implies \alpha \text{ a continuació veiem que no pot ser}, \\ N(\alpha) = 9, N(\beta) = 1 \implies \beta \text{ invertible}. \end{cases} \tag{5.4.5}$$

  Hauria de ser, doncs, $N(\alpha) = N(\beta) = 3$, però l'equació $a^2 + 5b^2 = 3$ no té solucions enteres (3 no és un quadrat mòdul 5); per tant, a $\mathbb{Z}[\sqrt{-5}]$ no hi ha elements de norma 2 i tenim que 2 és irreductible.
- Com no hi ha elements de norma 2 ni de norma 3, tenim que $1 + \sqrt{-5}, 1 - \sqrt{-5}$ també són elements irreductibles. En efecte, $6 = N(1 \pm \sqrt{-5}) = N(\alpha)N(\beta)$ i

$$\begin{cases} N(\alpha) = 1, N(\beta) = 6 \implies \alpha \text{ invertible}, \\ N(\alpha) = 2, N(\beta) = 3 \implies \alpha \text{ no pot ser}, \\ N(\alpha) = 3, N(\beta) = 2 \implies \alpha \text{ no pot ser}, \\ N(\alpha) = 6, N(\beta) = 1 \implies \beta \text{ invertible}. \end{cases} \tag{5.4.6}$$

- Com $(\mathbb{Z}[\sqrt{-5}])^* = \{\pm 1\}$, és clar que cap dels factors $2, 3$ no és associat a un dels factors $1 + \sqrt{-5}, 1 - \sqrt{-5}$ i, llavors, aquestes dues descomposicions en producte d'irreductibles són diferents.

Obtenim que $\mathbb{Z}[\sqrt{-5}]$ no és un domini de factorització única.

Proposició 5.4.7. *Per a un nombre enter d lliure de quadrats, l'anell $\mathbb{Z}[\sqrt{d}]$ és domini de factorització.*

Demostració. Per veure-ho, raonem per l'absurd. Suposem que existeixen a $\mathbb{Z}[\sqrt{d}]$ elements no nuls i no unitats que no són producte d'irreductibles. Sigui a un d'aquests elements amb $|N(a)|$ mínim (la norma en valor absolut és un nombre natural i, per tant, per la construcció

d'$\mathbb{N}$ existeix un mínim i un ínfim), on N indica la norma a $\mathbb{Z}[\sqrt{d}]$. Com a no és irreductible, tenim $a = bc$ amb b, c no unitats. Ara, $N(a) = N(b)N(c)$ i, com b, c no són unitats, $|N(b)| > 1$ i $|N(c)| > 1$ i, per tant, $|N(b)| < |N(a)|$ i $|N(c)| < |N(a)|$. Per l'elecció d'a, b i c són producte d'irreductibles; llavors, a també és producte d'irreductibles (però hem suposat que a no ho era, contradicció). ■

Observació 5.4.8. Un nombre enter d lliure de quadrats fa que l'arrel s'escrigui d'una única forma (per exemple, $\sqrt{5}$) i això fa que $a + b\sqrt{d}$ estigui determinat de manera única.

5.4.1 Màxim comú divisor i mínim comú múltiple en un DFU

Definició 5.4.9 (Conjunt fonamental d'elements irreductibles). Sigui A un domini de factorització única i P un subconjunt d'A amb les propietats següents:

1. Tot element de P és irreductible.
2. Tot element irreductible d'A és associat a algun element de P.
3. Dos elements diferents de P no són pas associats.

Anomenarem un conjunt P amb aquestes propietats un *conjunt fonamental d'elements irreductibles.*

Exemple 5.4.10. El conjunt dels nombres naturals primers i el conjunt de polinomis mònics irreductibles són conjunts fonamentals d'elements irreductibles a $\mathbb{Z}$ i $\mathbb{K}[X]$ ($\mathbb{K}$ essent un cos). Recordem que un polinomi es diu mònic si el coeficient del terme de grau més alt és 1.

Proposició 5.4.11. *Si A és un domini de factorització única i P és conjunt fonamental d'elements irreductibles, tot $a \in A$ no nul es pot expressar en la forma $a = up_1^{n_1} \cdots p_r^{n_r}$, on u és una unitat, $r \in \mathbb{N}$, $p_1, \ldots, p_r$ són elements diferents (dos a dos) de P i $n_1, \ldots, n_r \in \mathbb{N}$. A més, la unitat u, els irreductibles $p_1, \ldots, p_r$ i els exponents $n_1, \ldots, n_r$ queden unívocament determinats per a; és a dir, la descomposició $a = up_1^{n_1} \cdots p_r^{n_r}$ és única tret de l'ordre.*

Proposició 5.4.12. *Si a i b són dos elements d'un domini de factorització única A, existeixen* $\mathrm{mcd}(a, b)$ *i* $\mathrm{mcm}(a, b)$.

Demostració. Podem escriure, per la proposició anterior, 5.4.11, $a = up_1^{n_1} \cdots p_r^{n_r}$ i $b = vp_1^{m_1} \cdots p_r^{m_r}$, on u, v són unitats, $p_1, \ldots, p_r$ són elements diferents de P i $n_i, m_i \in \mathbb{Z} \geq 0$, per a tot i. Si prenem $k_i = \min\{n_i, m_i\}, l_i = \max\{n_i, m_i\}$, clarament $d = p_1^{k_1} \cdots p_r^{k_r} = \mathrm{mcd}(a, b)$ i $m = p_1^{l_1} \cdots p_r^{l_r} = \mathrm{mcd}(a, b)$. ■

Observació 5.4.13. Notem, la descomposició d'a i b és la mateixa en quant als factors, però queda determinada pels exponents, que poden ser més grans o iguals que 0 i, en particular, diferents en cada descomposició que vulguem fer.

5.4.2 Algorisme d'Euclides per a dominis euclidians

Lema 5.4.14 (Lema d'Euclides). *Sigui A un domini d'integritat, $a, b, q \in A$. Es compleix la igualtat d'ideals $(a, b) = (a - bq, b)$. Per tant, si A és domini d'ideals principals, tenim que els màxims comuns divisors són associats:* $\mathrm{mcd}(a, b) \sim \mathrm{mcd}(a - bq, b)$.

Demostració. Hem de fer dos enunciats, que hem provat a la part de *Problemes*:

1. Si A és domini d'integritat i $a, b \in A$, aleshores $(a) = (b)$ si, i només si, a, b són associats.
2. Si A és DIP (domini d'ideals principals), llavors d és màxim comú divisor d'a i b si, i només si, $(a, b) = (d)$.

Donat això per provat, tenim que si A és DIP i posem $\mathrm{mcd}(a, b) = d$, $\mathrm{mcd}(a - bq, b) = d'$, resulta:

$$(d) = (a, b) = (a - bq, b) = (d'). \tag{5.4.7}$$

En definitiva, es dona la igualtat $(a, b) = (a - bq, d)$ i d i d' són associats. ■

Proposició 5.4.15 (Algorisme d'Euclides). *Siguin (A, δ) un domini euclidià amb $a, b \in A$ tal que $b \neq 0$. El següent algorisme [Vil21] és finit i dona com a resultat $d = \mathrm{mcd}(a, b)$:*

1. *Suposarem $a > b$. En particular, $a > b > 0$. Com $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a) = \mathrm{mcd}(|a|, |b|)$, podem suposar $a \geq b > 0$ (el cas $b = 0$ és trivial, ja que $\mathrm{mcd}(a, 0) = |a|$.*
2. *Si $a = b$ el resultat és $\mathrm{mcd}(a, b) = a$. Per tant, suposem que $a > b > 0$.*
3. *Si $r_1 = 0$, tenim que $b \mid a$, així $\mathrm{mcd}(a, b) = b$.*
4. *Si $r_1 \neq 0$, cal calcular q_2, r_2 tals que $b = r_1 q_2 + r_2$, amb $\delta(r_2) < \delta(r_1)$.*
5. *Si $r_2 = 0$, aleshores $\mathrm{mcd}(a, b) = r_1$.*
6. *En definitiva, donats r_{j-1} i r_{j-2}, amb $j > 2$, si ambdós són no nuls, calculem q_j i r_j tals que $r_{j-2} = r_{j-1} q_j + r_j$, amb $\delta(r_j) < \delta(r_{j-1})$.*
7. *Suposem ara i l'últim índex tal que la resta r_i és no nul·la. Per tant, es té que $r_i = 0$ i $r_{i+1} = 0$. Aleshores, existeix un q_{i+1} tal que $r_{i-1} = r_i q_{i+1} + 0$. Afirmem, doncs, que per a aquest índex i es té que $\mathrm{mcd}(a, b) = r_i$.*

Existeix, doncs, $n \in \mathbb{N}$ tal que $r_1 \neq 0, \ldots, r_{n-1} \neq 0, r_n = 0$ i es compleix $\mathrm{mcd}(a, b) = r_{n-1}$. En termes de la funció δ, tenim una successió estrictament decreixent acotada inferiorment, $\delta(r_1) > \delta(r_2) > \cdots > \delta(r_{n-1}) > 0$.

Demostració. Volem veure que arribem a una resta igual a 0 en un nombre finit de passos. En efecte, si considerem la successió de restes, tenim $\delta(r_1) > \delta(r_2) > \cdots$; per tant, formen una successió estrictament decreixent d'enters naturals i $r_n = 0$ per a algun $n \in \mathbb{N}$. Ara, pel lema 5.4.14 es compleix $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \cdots = \mathrm{mcd}(r_{n-1}, r_n) = \mathrm{mcd}(r_{n-1}, 0) = r_{n-1}$. ■

5.5

Factorialitat dels anells de polinomis

Hem vist que si $\mathbb{K}$ és cos, l'anell de polinomis $\mathbb{K}[X]$ és un domini euclidià i, per tant, tenim un domini d'ideals principals i, per últim, $\mathbb{K}[X]$ és domini de factorització única. La proposició següent mostra que no podem esperar tenir aquestes propietats per a anells de polinomis de coeficients en dominis d'integritat més generals.

Proposició 5.5.1. *Sigui A un domini d'integritat. Les propietats següents són equivalents:*

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

Demostració. Donat que hem vist les dues implicacions anteriors, provem que si $A[X]$ és un domini d'ideals principals, A és un cos. Considerem el morfisme d'anells següent, que envia el polinomi al seu terme independent:

$$\begin{array}{rccc} \varphi: & A[X] & \longrightarrow & A \\ & P & \longmapsto & P(0) \end{array} \tag{5.5.1}$$

Clarament, φ és epimorfisme. El nucli, per construcció de φ, són tots aquells polinomis amb terme independent nul; és a dir, tenim $\ker(\varphi) = (X)$. Pel teorema d'isomorfia, $A[X]/(X) \cong A$. Com X és irreductible i $A[X]$ és domini d'ideals principals, per la proposició 5.3.10, (X) és maximal i, per definició d'ideal maximal, $A[X]/(X)$ és un cos que, pel teorema d'isomorfia un altre cop, és isomorf a A (en altres paraules, A és cos). ■

Exemple 5.5.2. $(2, X)$ és un ideal no principal de $\mathbb{Z}[X]$.

Volem veure ara que si A és un domini de factorització única, $A[X]$ és domini de factorització única. Recordem que si A és domini d'integritat, les unitats d'A són les mateixes que el seu anell de polinomis; és a dir, $(A[X])^* = A^*$.

Definició 5.5.3 (Contingut d'un polinomi). Sigui $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$ un polinomi amb coeficients en un domini de factorització única A. Anomenarem *contingut* de f un màxim comú divisor dels coeficients d'f. Denotem per $c(f)$ el contingut de f. Tenim, doncs:

$$c(f) = \operatorname{mcd}(a_0, a_1, \ldots, a_n). \tag{5.5.2}$$

Clarament, el contingut d'un polinomi d'$A[X]$ queda determinat tret d'un factor d'A^*. Direm que f és primitiu si el seu contingut $c(f)$ és una unitat.

Definició 5.5.4 (Polinomi primitiu corresponent a f). Donat $f \in A[X]$, existeix clarament un polinomi primitiu f^* tal que $f = c(f)f^*$. El polinomi f^* és únic en el sentit següent: si $f = c\tilde{f}$, amb $c \in A$ i $\tilde{f}$ primitiu, aleshores $c \sim c(f)$ i $\tilde{f} \sim f^*$. Direm que f^* és un *polinomi primitiu corresponent a f*.

Proposició 5.5.5 (Lema de Gauss)**.** *Sigui A un domini de factorització única. Aleshores, en $A[X]$ el producte de polinomis primitius és primitiu. Més generalment, si $f, g \in A[X]$, $c(fg) \sim c(f)c(g)$.*

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

$$\begin{array}{rccc} \varphi: & A[X] & \longrightarrow & (A/(p))[X] \\ & \sum_{i=0}^{n} a_i X^i & \longmapsto & \sum_{i=0}^{n} \pi(a_i) X^i \end{array} \tag{5.5.3}$$

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

Corol·lari 5.5.6. *Sigui A un domini de factorització única, $\mathbb{K}$ el cos de fraccions d'A i $f \in A[X]$ mònic. Si $f = gh$, amb $g, h \in \mathbb{K}[X]$ mònics, aleshores $g, h \in A[X]$.*

Demostració. Com f és mònic, $c(f) \sim 1$. Siguin $a, b \in A$ tals que ag i bh pertanyen a $A[X]$. Tenim $abf = abgh = (ag)(bh)$ i, per tant, $ab = c(abf) \sim c(ag)c(bh)$. Com g és mònic, el coeficient del monomi de grau més gran d'ag és a (multipliquem tots els coeficients per a); llavors, tenim $c(ag) \mid a$. Anàlogament, $c(bh) \mid b$. Tenim, doncs, $c(ag) \sim a$ i $c(bh) \sim b$ i, per tant, $g, h \in A[X]$. ∎

5.5.1 Irreductibles d'$A[X]$

Definició 5.5.7 (Element irreductible, anell de polinomis)**.** Sigui A un domini de factorització única. Un element d'A és *element irreductible d'$A[X]$* si, i només si, és element irreductible d'A (un element d'$A[X]$ de grau positiu no pot dividir un element d'A).

Estudiem ara l'irreductibilitat dels elements d'$A[X]$ de grau positiu en funció de la seva irreductibilitat com elements de $\mathbb{K}[X]$, on $\mathbb{K} = \mathbb{K}(A)$ és el cos de fraccions d'A.

Proposició 5.5.8. *Sigui A un domini de factorització única i sigui $f(X) \in A[X]$. Les condicions següents són equivalents:*

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

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

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

$$ab \sim c(abf) = c((ag)(bh)) \sim c(ag)c(bh), \tag{5.5.4}$$

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

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

■

5.5.2 Factorialitat d'$A[X]$

Lema 5.5.9. *Si $p \in A$ és un primer en A, aleshores p també és un primer en $A[X].$*

Demostració. Sigui p un element primer d'A, i suposem $p \mid fg$ i $p \nmid f$, per a $f, g \in A[X]$. Posem:

$$\begin{aligned} f &= a_0 + a_1X + \cdots + a_nX^n \\ g &= b_0 + b_1X + \cdots + b_mX^m \end{aligned} \tag{5.5.5}$$

i sigui i l'índex més petit tal que $p \mid a_k$, per a $0 \leq k < i$, $p \nmid a_i$. Provarem per inducció que p divideix tots els coeficients de f i, per tant, $p \mid g$. El coeficient de X^i de fg és:

$$a_ib_0 + a_{i-1}b_1 + \cdots + a_0b_i. \tag{5.5.6}$$

Com $p \mid a_{i-1}b_1 + \cdots + a_0b_i$ i $p \mid fg$, tenim $p \mid a_ib_0$ i $p \nmid a_i$, que implica $p \mid b_0$. Suposem ara que hem provat $p \mid b_k$, per a $k < j$. El coeficient de X^{i+j} de fg és:

$$a_{i+j}b_0 + a_{i+j-1}b_1 + \cdots + a_{i+1}b_{j-1} + a_ib_j + a_{i-1}b_{j+1} + \cdots + a_0b_{i+j}. \tag{5.5.7}$$

Com $p \mid a_{i-1}b_{j+1} + \cdots + a_0b_{i+j}$ i $p \mid a_{i+j}b_0 + a_{i+j-1}b_1 + \cdots + a_{i+1}b_{j-1}$ per hipòtesi d'inducció, a més que $p \mid fg$, tenim $p \mid a_ib_j$ i $p \nmid a_i$ que implica $p \mid b_j$. ■

Teorema 5.5.10. *Si A és un domini de factorització única, aleshores $A[X]$ és un domini de factorització única.*

Demostració. Primerament, volem veure que $A[X]$ és domini de factorització. Per a tot $f \in A[X]$, no nul i no unitat, f és producte d'irreductibles d'A per ser A domini de factorització.

1. $f \in A$ ($\mathrm{gr}(f) = 0$), f és producte d'irreductibles d'A que ho són, també, a $A[X]$.
2. Suposem, doncs, que $\mathrm{gr}(f) > 0$, $f = g_1 \cdots g_r$ amb $g_1, \ldots, g_r$ irreductibles de $K[X]$, K cos de fraccions d'A (i $\mathbb{K}[X]$ domini euclidià).

Vegem com a partir d'aquesta factorització de f a $\mathbb{K}[X]$ podem deduir una descomposició de f com a producte d'irreductibles d'$A[X]$. Suposem $a_1, \ldots, a_r \in A \setminus \{0\}$, tals que $a_i g_i \in A[X]$ i $a = a_1 \cdots a_r$. Escrivim $a = a_1 \cdots a_r$ i:

$$\begin{aligned} af &= (a_1 g_1) \cdots (a_r g_r) \\ f &= c(f) f^* \text{ i } a_i g_i = c(a_i g_i) g_i^*,\ f^*, g_i^* \text{ polinomis primitius.} \end{aligned} \tag{5.5.8}$$

g_i^* és primitiu i irreductible a $K[X]$ de manera que g_i^* és irreductible a $A[X]$. Podem trobar l'associat a f^*, tenint en compte que $ac(f)f^*$ és el producte d'una constant per un primitiu i que el seu associat també ho és ($g_1^*, \ldots, g_r^*$ és primitiu pel lema de Gauss). Amb (5.5.8) escrivim:

$$af = ac(f)f^* = c(a_1 g_1) \cdots c(a_r g_r) g_1^* \cdots g_r^* \implies f^* \sim g_1^* \cdots g_r^*. \tag{5.5.9}$$

En definitiva, $f^* = u g_1^* \cdots g_r^*$ i $f = c(f) f^*$. Si $c(f) \in A$, A domini de factorització única, $c(f)$ és producte d'irreductibles d'A i aquests també són irreductibles d'$A[X]$.
Per provar la unicitat de la descomposició d'un element d'$A[X]$ com a producte d'irreductibles, n'hi ha prou amb provar que tot element irreductible d'$A[X]$ és primer. Sigui $f \in A[X]$, irreductible:

1. $f \in A$ (f té grau zero) implica, per ser A un domini de factorització única, f és primer d'A i, per tant, f és primer d'$A[X]$.
2. Per a $g, h \in A[X]$, $\mathrm{gr}(f) > 0$ i $f \mid gh$. Com f és irreductible a $K[X]$ i $K[X]$ és domini de factorització única, $f \mid g$ o bé $f \mid h$ a $\mathbb{K}[X]$.

Suposem $f \mid g$ a $\mathbb{K}[X]$. Tenim $g = fq$ amb $q \in \mathbb{K}[X]$ i agafem $a \in A \setminus \{0\}$ tal que $aq \in A[X]$. Aleshores, $ag = f(aq)$. Si posem $g = c(g)g^*$ i $aq = c(aq)q^*$ amb g^*, q^* primitius, obtenim la relació:

$$ac(g)g^* = c(aq)(fq^*),\ fq^* \text{ primitiu,} \tag{5.5.10}$$

on, recordem f irreductible i $\mathrm{gr}(f) > 0$. Per ser f irreductible a $A[X]$ i de grau positiu, f primitiu. Així, $q^* f$ és primitiu pel lema de Gauss.

$$g^* \sim fq^* \text{ i } ac(g) \sim c(aq), \tag{5.5.11}$$

d'on se segueix que existeix una unitat $u \in A$ tal que $g^* = ufq^*$; és a dir, $f \mid g^*$ en $A[X]$ i, per tant, $f \mid g$ a $A[X]$, també. ■

Observació 5.5.11. Del teorema anterior obtenim que $\mathbb{Z}[X]$ és domini de factorització única. Sanem que no és domini d'ideals principals, ja que, per exemple, l'ideal $(2, X)$ no és principal.

Corol·lari 5.5.12. *Si A és domini de factorització única, aleshores $A[X_1, \ldots, X_n]$ és domini de factorització única.*

Demostració. Per 5.5.10, tenint en compte $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$. ■

5.5.3 Criteris d'irreductibilitat

En aquesta subsecció A serà un domini de factorització única i $\mathbb{K}$ el cos de fraccions d'A.

Proposició 5.5.13.

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

Demostració. Primer apartat: Pel fet que $\frac{c}{d}$ és una arrel tenim que $f(\frac{c}{d}) = 0$ i en substituïm la X en la forma polinomial.

$$0 = f\left(\frac{c}{d}\right) = a_0 + a_1\left(\frac{c}{d}\right) + \cdots + a_n\left(\frac{c}{d}\right)^n \implies a_0d^n + a_1cd^{n-1} + \cdots + a_nc^n = 0. \tag{5.5.12}$$

Ens queda que $c \mid a_0d^n$, donat que $a_0d^n = -c(a_1d^{n-1} + \cdots + a_nc^{n-1})$. Per a tot irreductible p dividint c tenim $p \mid a_0d^n$, que implica $p \mid a_0$, ja que $p \nmid d$ i p és primer. Per tant, $c \mid a_0$. Anàlogament, $a_nc^n = -d(a_0d^{n-1} + \cdots + a_{n-1}c^{n-1})$ implica $d \mid a_n$.
Segon apartat: Com f és primitiu i de grau positiu, podem expressar-lo a través de la següent factorització no trivial possible.

$$f(x) = g(x)h(x),\ 1 \leq \mathrm{gr}(g), \mathrm{gr}(h) < \mathrm{gr}(f). \tag{5.5.13}$$

f és irreductible a $A[X]$ si, i només si, ho és a $\mathbb{K}[X]$. Com f té grau 2 o 3, redueix sobre $\mathbb{K}$ si, i només si, té un factor de grau 1 si, i només si, té una arrel a $\mathbb{K}$. ■

Exemple 5.5.14. Sigui $X^3 + X + 1 \in \mathbb{Z}[X]$ un polinomi de l'anell d'enters. Pel criteri d'irreductibilitat, les possibles arrels racionals que tenim són ± 1, però veiem que no ho són clarament. Per tant, tenim un polinomi primitiu sense arrels a $\mathbb{Q}$ i és irreductible.

Proposició 5.5.15 (Criteri modular). *Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, primitiu, i suposem que existeix $p \in A$, irreductible, tal que $p \nmid a_n$ i que el polinomi $\overline{f}(X) = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \in (A/(p))[X]$ és irreductible (on $\overline{a}$ indica la classe d'$a \in A$ en el quocient $A/(p)$ pel morfisme de pas al quocient $\pi : A \longrightarrow A/(p)$). Aleshores, f és irreductible en $A[X]$.*

Demostració. Si f redueix sobre A, tenim $f = gh$, amb g, h polinomis d'$A[X]$ de grau $1 \leq \mathrm{gr}(g), \mathrm{gr}(h) < \mathrm{gr}(f)$, ja que f és primitiu. Posem:

$$g = \sum_{i=0}^{r} b_i X^i,\ h = \sum_{j=0}^{s} c_j X^j. \tag{5.5.14}$$

Llavors, $\overline{f} = \overline{g}\overline{h}$ a $(A/(p))[X]$ i, com $p \nmid a_n$, $\overline{a_n} \neq \overline{0}$. En particular, $\overline{a_n} = \overline{b_r}\overline{c_s} \neq \overline{0}$. A més a més, tenim la següent cadena d'implicacions:

$$p \text{ irreductible i } A \text{ DFU} \implies p \text{ primer} \implies (p) \text{ primer} \implies A/(p) \text{ D. Integritat.} \tag{5.5.15}$$

Com $\overline{a_n} \neq \overline{0}$, $\overline{b_m} \neq \overline{0}$ i $\overline{c_k} \neq \overline{0}$. Per tant, $\mathrm{gr}(\overline{f}) = \mathrm{gr}(f), \mathrm{gr}(\overline{g}) = \mathrm{gr}(g), \mathrm{gr}(\overline{h}) = \mathrm{gr}(h)$ i $\overline{f} = \overline{g} \cdot \overline{h}$ és descomposició no trivial; $\overline{f}$ redueix sobre $A/(p)$. Equivalentment, $\overline{f}$ no és irreductible. ■

Exemple 5.5.16. Sigui $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$, amb a, b senars i $p = 2$. $\overline{f}(X) = X^3 + X + 1 \in \mathbb{Z}/(2)[X]$ no té arrels a $\mathbb{Z}/(2)$, ja que $\overline{f}(0) = \overline{f}(1) = 1$ i $\mathrm{gr}(\overline{f}) = 3$. Això vol dir, pel criteri anterior, que $\overline{f}$ és irreductible i, per tant, que f és irreductible.

Exemple 5.5.17. Considerem el polinomi $f(X) = X^4 - X + 1 \in \mathbb{Z}[X]$. Veurem que és irreductible usant la seva reducció mòdul 2. Considerem doncs $\overline{f}(X) = X^4 + X + 1 \in (\mathbb{Z}/(2))[X]$. Primer observem que $\overline{f}(\overline{0}) = \overline{f}(\overline{1}) = \overline{1}$, per tant $\overline{f}$ no té arrels a $\mathbb{Z}/(2)$. Ara hi ha un únic polinomi irreductible de grau 2 a $(\mathbb{Z}/(2))[X]$, $X^2 + X + 1$. Com $\overline{f}$ no pot tenir un factor de grau 1, l'única descomposició possible seria $\overline{f}(X) = (X^2 + X + 1)^2$, però $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq \overline{f}(X)$, per tant $\overline{f}$ és irreductible i, pel criteri modular, f és irreductible sobre $\mathbb{Z}i$, com té grau positiu, també sobre $\mathbb{Q}$.

Proposició 5.5.18 (Criteri d'Eisenstein)**.** *Sigui $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ primitiu i sigui $p \in A$, irreductible en A. Suposem que $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, p \mid a_n$ i $p^2 \nmid a_0$. Aleshores, $f(X)$ és irreductible.*

Demostració. Com f és primitiu, si reduís, seria producte de dos polinomis de grau positiu. Veurem que això no pot ser. Suposem que tenim

$$f(X) = (b_0 + b_1 X + \cdots + b_r X^r)(c_0 + c_1 X + \cdots + c_s X^s), \tag{5.5.16}$$

amb $r, s \geq 1$. Com $a_n = b_r c_s$ i $p \nmid a_n$, tenim $p \nmid b_r$ i $p \nmid c_s$. D'altra banda, $a_0 = b_0 c_0$ i $p \mid a_0, p^2 \nmid a_0$; per tant, $p \mid b_0$ o $p \mid c_0$, però p no divideix a tots dos. Suposem $p \mid c_0$ i $p \nmid b_0$. Com $p \mid c_0$ i $p \nmid c_s$, existeix t amb $0 < t \leq s < n$ tal que (en altres paraules, com que $p \nmid c_s$ hi ha un t intermig, com a mínim, tal que p no divideix el t-èsim coeficient):

$$p \mid c_0, p \mid c_1, \ldots, p \mid c_{t-1}, p \nmid c_t. \tag{5.5.17}$$

Aleshores la igualtat $a_t = b_0 c_t + b_1 c_{t-1} + \cdots + b_t c_0$ implica que $p \mid a_t$, i la relació $p \mid b_1 c_{b-1} + \cdots + b_t c_0$ impliquen $p \mid b_0 c_t$ i, al seu torn, això últim implica que $p \mid b_0$ o bé $p \mid c_t$. Aquest fet és impossible ja que $p \nmid b_0$ i $p \nmid c_t$. ■

Exemple 5.5.19. Posem $f(X) = X^4 + 4X^3 + 6X + 2 \in \mathbb{Z}[X]$. Si agafem $p = 2$ es compleixen les condicions del criteri d'Eisenstein i, per tant, $f(X)$ no seria irreductible. Un altre exemple d'irreductibilitat amb $p = 2$ és $X^n + 2 \in \mathbb{Z}[X]$, que és irreductible per a tot $n \geq 1$.

Observació 5.5.20. Per a $a \in A$, l'aplicació $A[X] \longrightarrow A[X]$ que envia $X \longmapsto X + a$, és un automorfisme de l'anell $A[X]$. Per tant, $f(X)$ és irreductible si, i només si, ho és $f(X + a)$.

Exemple 5.5.21. Sigui p un enter natural primer. Volem provar que el polinomi $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ és irreductible. Tenim $X^p - 1 = (X - 1)\Phi_p(X)$ i, fent el canvi de variable $X = Y + 1$, obtenim

$$(Y + 1)^p - 1 = Y\Phi_p(Y + 1). \tag{5.5.18}$$

Desenvolupant el terme de l'esquerra i aillant $\Phi_p(Y + 1)$, obtenim

$$\Phi_p(Y + 1) = Y^{p-1} + \binom{p}{1} Y^{p-2} + \binom{p}{2} Y^{p-3} + \cdots + \binom{p}{p-1}. \tag{5.5.19}$$

Com p és primer, $\binom{p}{k}$ és divisible per p, per a $1 \leq k \leq p - 1$. D'altra banda el terme de grau zero és igual a p, per tant no divisible per p^2. Tenim doncs que Φ_p és irreductible, pel criteri d'Eisenstein i l'observació anterior.

5.6 Exercicis finals

Exercici 5.6.1. *Considerem l'anell* $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \in \mathbb{C} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$*, i la seva norma,* $N(a + b\sqrt{-5}) := a^2 + 5b^2$*, per a* $a, b \in \mathbb{Z}$

1. *Proveu que l'aplicació* $\varphi : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}/2\mathbb{Z}$*, definida per l'assignació* $a + b\sqrt{-5} \mapsto a + b \pmod 2$*, per a* $a, b \in \mathbb{Z}$*, és un morfisme exhaustiu d'anells.*
2. *Proveu que* $\ker(\varphi)$ *és l'ideal de* $\mathbb{Z}[\sqrt{-5}]$ *generat per 2 i* $1 + \sqrt{-5}$*.*
3. *Proveu que* $\ker(\varphi)$ *és un ideal maximal de* $\mathbb{Z}[\sqrt{-5}]$ *i que no és principal.*

Demostració. Primer apartat: Sigui $\psi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}$ l'únic morfisme d'anells determinat per l'assignació $X \mapsto 1$; clarament, ψ és exhaustiu, i l'ideal principal generat per $X^2 + 5$ està inclòs en el nucli, que és l'ideal generat per 2 i $X - 1$. Per pas al quocient, obtenim un morfisme exhaustiu d'anells

$$\varphi : \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/\left(X^2 + 5\right) \longrightarrow \mathbb{Z}/2\mathbb{Z}. \tag{5.6.1}$$

de fet, l'únic tal que $a + b\sqrt{-5} \mapsto a + b \pmod 2$, per a $a, b \in \mathbb{Z}$.
Segon apartat: Com que els morfismes φ i ψ són exhaustius, el nucli de φ és la imatge per la projecció $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{-5}]$ del nucli de ψ. Així, $\ker(\varphi)$ és l'ideal generat per 2 i $1 + \sqrt{-5}$, que són les imatges de 2 i $1 + X$ (podem prendre $1 + X$ en lloc de $X - 1$, perquè 2 pertany al nucli) en l'anell quocient $\mathbb{Z}[\sqrt{-5}]$.

TERCER APARTAT: Com que $\text{im}(\varphi)$ és un cos, resulta que $\ker(\varphi)$ és un ideal maximal. Només cal veure que no és principal. Però si $\ker(\varphi)$ fos principal, seria generat per un element de la forma $a+b\sqrt{-5}$, amb $a, b \in \mathbb{Z}$. Llavors, $N(a+b\sqrt{-5})$ dividiria $N(2) = 4$, en $\mathbb{Z}$. Però si $N(a+b\sqrt{-5}) = a^2 + 5b^2$ divideix 4, resulta que $b = 0$, de manera que $a + b\sqrt{-5} = a \in \mathbb{Z}$. Llavors, llevat del signe, seria $a + b\sqrt{-5} = 2$ (no pot ser 1, perquè el nucli és un ideal maximal); però $1 + \sqrt{-5}$ no és múltiple de 2, perquè els múltiples de 2 tenen parells els coeficients de 1 i de $\sqrt{-5}$. ■

Exercici 5.6.2. *Siguin* $\xi := \frac{-1}{2} + \frac{\sqrt{3}}{2}i \in \mathbb{C}$, *i* $\mathbb{Z}[\xi] := \{a + b\xi \in \mathbb{C} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

1. *Proveu que* $\mathbb{Z}[\xi]$ *és un subanell de* $\mathbb{C}$.
2. *Proveu que* $\mathbb{Z}[\xi]$ *és isomorf a* $\mathbb{Z}[X]/(X^2 + X + 1)$.
3. *Sigui* $\omega \in \mathbb{Z}[\xi]$. *Proveu que el conjugat complex,* $\overline{\omega}$, *de* ω, *pertany a* $\mathbb{Z}[\xi]$ *i que* $N(\omega) = \omega\overline{\omega}$ *és una norma en l'anell* $\mathbb{Z}[\xi]$.
4. *Calculeu totes les unitats de* $\mathbb{Z}[\xi]$.

Demostració. PRIMER APARTAT: Considerem el morfisme d'anells $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{C}$ determinat per l'assignació $p(X) \longmapsto p(\xi)$, $p(X)$ un polinomi amb coeficients enters qualsevol. *A classe de problemes també hem vist que podem fer l'assignació canònica* $a_0 \longmapsto -\frac{1}{2}$, $X \longmapsto \frac{\sqrt{3}}{2}i$. Fixem, ara, $p(X) = X^2 + X + 1 \in \mathbb{Z}[X]$. És trivial que $p(\xi) = 0$ i, d'aquesta manera, $p(X) \in \ker(\varphi)$. D'altra banda, agafem un polinomi $f(X) \in \mathbb{Z}[X]$, i l'escrivim com $f(X) = p(X)g(X) + r(X)$, amb $g(X), r(X) \in \mathbb{Z}[X]$ i $\text{gr}(r(X)) \leq 1$ pel teorema de la divisió entera (és a dir, $r(X) = a+bX$). La imatge de φ coincideix amb el conjunt $\mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$, ja que $\varphi(f(X)) = \varphi(r(X))$ pel fet que $p(X) \in \ker(\varphi)$. En particular, $\text{im}(\varphi) = \mathbb{Z}[\xi]$ és un subanell de $\mathbb{C}$.
SEGON APARTAT: Prenem φ prèviament definida i, clarament, el nucli de φ és exactament l'ideal generat per $p(X)$. Ja hem dit que $\varphi(f(X)) = \varphi(r(X))$; és a dir, $f(X) \in \ker(\varphi) \iff r(X) \in \ker(\varphi)$, però $r(\xi) = a + b\xi = 0 \iff a = b = 0$. Per tant, $r(X) = 0$ i $f(X) = q(X)p(X) \in (X^2 + X + 1)$. Finalment, ens val amb aplicar el primer teorema d'isomorfia per a anells: $\text{im}(\varphi) = \mathbb{Z}[X]/(p(X)) \cong \mathbb{Z}[\xi]$.
TERCER APARTAT: Si $\omega \in \mathbb{Z}[\xi]$, el podem expressar de la forma $\omega = a + b\xi$, amb $a, b \in \mathbb{Z}$. Llavors, podem intentar trobar el conjugat $\overline{\omega}$ a través de la definició:

$$\left(a - \frac{b}{2} + \frac{\sqrt{3}}{2}bi\right) + \left(a - \frac{b}{2} - \frac{\sqrt{3}}{2}bi\right) = 2a - b \in \mathbb{Z} \subset \mathbb{Z}[\xi] \implies \overline{\omega} = (2a-b) - \omega \in \mathbb{Z}[\xi]. \quad (5.6.2)$$

Ara intentem veure si $N(\omega) = \omega \cdot \overline{\omega}$ és una norma. En efecte:

$$N(\omega) = \omega\overline{\omega} = \omega((2a - b) - \omega) = \frac{(2a - b)^2 + 3b^2}{4} = a^2 - ab + b^2 \in \mathbb{Z} \quad (5.6.3)$$

i l'aplicació N és multiplicativa perquè el conjugat és multiplicatiu i la operació producte és commutativa en $\mathbb{C}$:

$$N(ab) = ab \cdot \overline{ab} = ab \cdot \overline{a} \cdot \overline{b} = a\overline{a} \cdot b\overline{b} = N(a)N(b). \quad (5.6.4)$$

Notem que, a més, $N(\omega) = a^2 - ab + b^2 = \frac{a^2+b^2+(a-b)^2}{2} \geq 0$ i $N(\omega) = 0 \iff a = b = 0$ (es pot fer un anàlisi d'extrems de la funció si no es veu clar).

Quart apartat: Si ω és invertible, existeix α tal que $\omega\alpha = 1$. Tota unitat, a més, compleix que la seva norma és ± 1.

$$N(\omega\alpha) = N(\omega)N(\alpha) = N(1) = 1. \tag{5.6.5}$$

de manera que $N(\omega) = 1$, ja que a l'apartat anterior hem vist que $N(\omega) \geq 0$ per a tot ω. Ara ens quedarà resoldre l'equació diofantina resultant, i veure quins elements de $\mathbb{Z}[\xi]$ la compleixen.

$$N(\omega) = a^2 - ab + b^2 = 1 \iff \begin{Bmatrix} a = \pm 1 \\ b = 0 \end{Bmatrix} \text{ o bé } \begin{Bmatrix} a = 0 \\ b = \pm 1 \end{Bmatrix} \text{ o bé } \begin{Bmatrix} a = \pm 1 \\ b = \pm 1 \end{Bmatrix}. \tag{5.6.6}$$

Així doncs, les úniques solucions *enteres* d'aquesta equació són

$$(a, b) \in A = \{(0, 1), (0, -1), (1, 0), (-1, 0), (1, 1), (-1, -1)\}, \text{ on } (a, b) \in \mathbb{Z} \times \mathbb{Z}. \tag{5.6.7}$$

Les unitats, doncs, corresponen als sis elements $\omega \in \{a + b\xi \mid (a, b) \in A\}$. ■

Exercici 5.6.3. *L'anell $\mathbb{Z}[\sqrt{2}]$ és un domini de factorització única.*

1. *Comproveu que $23 = (3 + 4\sqrt{2})(-3 + 4\sqrt{2}) = (11 + 7\sqrt{2})(11 - 7\sqrt{2})$. Contradiu aquesta igualtat el fet que $\mathbb{Z}[\sqrt{2}]$ sigui domini de factorització única?*
2. *Proveu que $\mathbb{Z}[\sqrt{2}]$ té infinites unitats.*

Demostració. Primer apartat: Les igualtats $23 = (3+4\sqrt{2})(-3+4\sqrt{2}) = (11+7\sqrt{2})(11-7\sqrt{2})$ són clares, i no contradiuen el fet que $\mathbb{Z}[\sqrt{2}]$ sigui un domini de factorització única. En efecte, se satisfà que $(11 + 7\sqrt{2}) = (3 + 4\sqrt{2}) \cdot (1 + \sqrt{2})$, que $(11 - 7\sqrt{2}) = (3 - 4\sqrt{2}) \cdot (1 - \sqrt{2})$, i que $N(1 + \sqrt{2}) = N(1 - \sqrt{2}) = -1$, invertible en $\mathbb{Z}$, de manera que $1 \pm \sqrt{2}$ són unitats de $\mathbb{Z}[\sqrt{2}]$ i les parelles d'elements $(11 + 7\sqrt{2}, 3 + 4\sqrt{2})$, i $(11 - 7\sqrt{2}, 3 - 4\sqrt{2})$ ho són d'elements associats. Segon apartat: Notem que $(1 + \sqrt{2}) > 1$ és un element invertible de $\mathbb{Z}[\sqrt{2}]$, amb invers $-1 + \sqrt{2}$. Per tant, per a tot $r \in \mathbb{Z}$, l'element $(1 + \sqrt{2})^r$ també és un element de $\mathbb{Z}$, invertible, i diferent dels $(1 + \sqrt{2})^s$, si $r \neq s$. Per tant, el grup de les unitats de $\mathbb{Z}[\sqrt{2}]$ conté el subgrup generat per ± 1 i pel grup cíclic infinit generat per $1 + \sqrt{2}$. ■

Observació 5.6.4. No costa gaire demostrar que els elements $\pm(1 + \sqrt{2})^r$, per a $r \in \mathbb{Z}$, són tots els elements invertibles de $\mathbb{Z}[\sqrt{2}]$.

Part

III

Apèndix

$$f(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ f(n-1) + f(n-2) & \text{if } n \geq 2 \end{cases}$$

A

Grups abelians finitament generats

A.1 Bases

Siguin E un grup abelià i $e_1, \ldots, e_r$ elements de E.

1. Els elements $e_1, \ldots, e_r$ són linealment independents sobre $\mathbb{Z}$ si, per a $n_1, \ldots, n_r \in \mathbb{Z}$.

$$n_1 e_1 + \cdots + n_r e_r = 0 \implies n_1 = 0, \ldots, n_r = 0. \tag{A.1.1}$$

2. $(e_1, \ldots, e_r)$ és base de E si els elements $e_1, \ldots, e_r$ són linealment independents sobre $\mathbb{Z}$ i generen E.

Proposició A.1.1. *Siguin E un grup abelià ie$_1, \ldots, e_r$ elements de E. Aleshores, $(e_1, \ldots, e_r)$ és base de E si i només si tot element de E s'escriu de manera única en la forma $n_1 e_1 + \cdots + n_r e_r$, amb $n_1, \ldots, n_r \in \mathbb{Z}$.*

Demostració. Es demostra de manera anàloga a com faríem amb espais vectorials. ■

Definició A.1.2 (Grup abelià finitament generat lliure)**.** Un grup abelià finitament generat és lliure si és isomorf a $\mathbb{Z} \oplus \overset{r}{\cdots} \oplus \mathbb{Z}$, per a algun enter $r > 0$.

Proposició A.1.3. *Un grup abelià finitament generat és lliure si i només si té una base.*

Demostració. Si $(e_1, \ldots, e_r)$ és base de E, definim l'aplicació:

$$\begin{array}{ccc} \mathbb{Z} \oplus \overset{r}{\cdots} \oplus \mathbb{Z} & \longrightarrow & E \\ (n_1, \ldots, n_r) & \longmapsto & n_1 e_1 + \cdots + n_r e_r. \end{array} \tag{A.1.2}$$

Clarament és isomorfisme de grups. Recíprocament, si φ és isomorfisme de grups, $\mathbb{Z} \oplus \overset{r}{\cdots} \oplus \mathbb{Z}$ en E, aleshores $(\varphi(1, 0, \ldots, 0), \ldots, \varphi(0, \ldots, 0, 1))$ és base d'E. ■

Lema A.1.4. *Si $(e_1, \ldots, e_r)$ és base de $E, d_1, \ldots, d_r$ són enters naturals, aleshores*

$$E / \langle d_1 e_1, \ldots, d_r e_r \rangle \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}. \tag{A.1.3}$$

Demostració. Definim l'aplicació

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z} \\ n_1 e_1 + \cdots + n_r e_r & \longmapsto & (n_1 \bmod d_1, \ldots, n_r \bmod d_r)\,. \end{array} \tag{A.1.4}$$

Clarament és epimorfisme de grups i el seu nucli és el subgrup $\langle d_1 e_1, \ldots, d_r e_r \rangle$ del grup E. Pel teorema d'isomorfia 1.6.2, obtenim l'isomorfisme volgut. ■

Proposició A.1.5. *Si un grup abelià E té una base amb r elements, totes les bases de E tenen r elements. L'enter r es diu rang de E.*

Demostració. Sigui $(e_1, \ldots, e_r)$ una base de E. Posem $2E := \{2x \mid x \in E\}$. Clarament $2E$ és el subgrup de E generat per $2e_1, \ldots, 2e_r$ i, per tant $E/2E \simeq \mathbb{Z}/2\mathbb{Z} \oplus \overset{r}{\cdots} \oplus \mathbb{Z}/2\mathbb{Z}$. Com $2E$ no depèn de la base escollida, r tampoc. ■

A.2 Subgrup de torsió

Definició A.2.1. Els elements d'ordre finit d'un grup abelià E s'anomenen també elements de torsió i formen un subgrup $F(E)$ de E anomenat subgrup de torsió de E. Diem que E és lliure de torsió si $F(E) = \{0\}$.

Lema A.2.2. *Si un conjunt de generadors $\{e_1, \ldots, e_r\}$ d'un grup abelià E no és $\mathbb{Z}$-linealment independent, aleshores existeixen un altre conjunt de generadors $\{e'_1, \ldots, e'_r\}$ de E (amb el mateix nombre d'elements) i un enter no nul q tals que $qe'_i = 0$, per a algun índex i.*

Demostració. Siguin $n_1, \ldots, n_r$ enters no tots nuls tals que $n_1e_1 + \cdots + n_re_r = 0$. Si només un n_i és no nul, ja tenim el resultat volgut. Suposem doncs que al menys dos n_i 's són no nuls. Reordenant el e_i 's si cal, podem suposar $|n_1| \geq |n_2| > 0$. Tenim les igualtats

$$n_1e_1 + n_2e_2 = (n_1 - n_2)\, e_1 + n_2\, (e_2 + e_1) = (n_1 + n_2)\, e_1 + n_2\, (e_2 - e_1) \tag{A.2.1}$$

i un dels nombres $|n_1 - n_2|$ o $|n_1 + n_2|$ és estrictament més petit que $|n_1|$. Per tant existeix una relació no trivial, o bé entre els generadors $e_1, e_2 + e_1, \ldots, e_r$, o bé entre els generadors $e_1, e_2 - e_1, \ldots, e_r$, per a la qual la suma dels valors absoluts dels coeficients és estrictament més petita que $m = |n_1| + \cdots + |n_r| > 0$. El resultat s'obté doncs fent inducció sobre m. ■

Proposició A.2.3. *Sigui E un grup abelià finitament generat i lliure de torsió. Aleshores E és un grup abelià lliure.*

Demostració. Sigui $\{e_1, \ldots, e_r\}$ un conjunt de generadors de E amb r mínim. Vegem que $e_1, \ldots, e_r$ són $\mathbb{Z}$-linealment independents. Siguin $n_1, \ldots, n_r$ enters tals que

$$n_1e_1 + \cdots + n_re_r = 0. \tag{A.2.2}$$

Volem veure $n_i = 0$, per a tot $i, 1 \leq i \leq r$. Raonem per l'absurd. Suposem que no tots els n_i 's són nuls. Aleshores, pel lema 3.2.2, existeixen un conjunt de generadors $\{e'_1, \ldots, e'_r\}$ de E, un enter no nul q i un índex i tals que $qe'_i = 0$. Com E no té elements de torsió no nuls, ha de ser $e'_i = 0$ però aleshores, E es pot generar amb $r - 1$ elements, contradient la minimalitat de r. ■

Proposició A.2.4. *Tot grup abelià finitament generat és suma directa d'un grup abelià lliure i un grup finit.*

Demostració. Sigui E un grup abelià finitament generat i sigui F el seu subgrup de torsió. Aleshores $L = E/F$ és lliure de torsió i finitament generat. Per la proposició 3.2.3, L és lliure. Siguin $e_1, \ldots, e_r$ elements de E tals que les seves classes $[e_1], \ldots, [e_r]$ a L formin base de L. Sigui $L' = \langle e_1, \ldots, e_r \rangle$. Com la imatge de L' pel morfisme de pas al quocient $E \longrightarrow L$ és igual a L, tenim $L' + F = E$. D'altra banda, $e_1, \ldots, e_r$ són linealment independents sobre $\mathbb{Z}$, ja que una relació de dependència entre ells donaria una entre $[e_1], \ldots, [e_r]$, per tant L' és lliure. Això implica $L' \cap F = \{0\}$. Notem que F és isomorf al quocient E/L' i per tant finitament generat i, per ser de torsió, finit. ■

Direm que un grup abelià finitament generat E té rang r si $E/F(E)$ té rang r. Els grups abelians finits són els grups abelians finitament generats de rang 0.

A.3

Estructura dels grups abelians finitament generats

Proposició A.3.1. *Sigui L un grup abelià lliure de rang r i L' un subgrup de L. Aleshores existeixen una base $(e_1, \ldots, e_r)$ de L, un enter natural $s \leq r$ i enters positius $d_1, \ldots, d_s$ tals que $(d_1 e_1, \ldots, d_s e_s)$ és base de L' i $d_i \mid d_{i+1}$, per a $1 \leq i < s$.*

Teorema A.3.2 (Estructura dels grups abelians finitament generats)**.** *Sigui E un grup abelià finitament generat de rang r. Existeixen un nombre natural s i enters positius $d_1, \ldots, d_s$ amb d_j dividint d_{j+1} per a $1 \leq j \leq s$ tals que E és suma directa de subgrups cíclics F_j d'ordre d_j i de r subgrups cíclics infinits.*

Corol·lari A.3.3. *Si F és un grup abelià finit, existeixen un nombre natural s i enters positius $d_1, \ldots, d_s$ amb d_j dividint d_{j+1} per a $1 \leq j \leq s$ tals que E és suma directa de subgrups cíclics F_j d'ordre d_j. En particular, l'ordre de F és igual al producte $d_1 \cdots d_s$.*

Definició A.3.4 (Factors invariants)**.** Els enters $d_1, \ldots, d_s$ del corol·lari anterior s'anomenen factors invariants de F.

Proposició A.3.5. *Sigui F un grup abelià finit. Sigui $|F| = p_1^{k_1} \cdots p_l^{k_l}$ la descomposició de l'ordre de F en producte de nombres primers. Aleshores, existeixen enters positius s_i i $k_{i1} \geq k_{is_i} > 0$ tals que:*

$$F = \bigoplus_{1 \leq i \leq l} \left(\bigoplus_{1 \leq j \leq s_i} F_{ij} \right), \tag{A.3.1}$$

on F_{ij} és grup cíclic d'ordre $p_i^{k_{ij}}$, $1 \leq j \leq s_i, 1 \leq i \leq l$ i $k_i = k_{i1} + \cdots + k_{is_i}$. A més, els primers $p_1, \ldots, p_l$ i les successions k_{ij} queden determinats unívocament pel grup F.

Definició A.3.6. Els enters $p_i^{k_{ij}}$ de la proposició anterior s'anomenen divisors elementals del grup F.

Corol·lari A.3.7. *Dos grups abelians finits compleixen la següent cadena d'equivalències:*

$$\textit{mateixos divisors elementals} \iff \textit{són isomorfs} \iff \textit{mateixos factors invariants} \quad \text{(A.3.2)}$$

Per A.3.5, podem determinar, tret d'isomorfisme, tots els grups abelians finits d'un ordre donat n. Si $n = p_1^{k_1} \cdots p_l^{k_l}$ com $k_j = k_{1j} + \cdots + k_{sj}$ el conjunt de les classes d'isomorfisme dels grups abelians d'ordre n està en bijecció amb el conjunt $\Pi_1 \times \cdots \Pi_l$, on $\prod_j$ és el conjunt de particions de k_j.

Exemple A.3.8. Determinarem tots els grups abelians d'ordre 72, tret d'isomorfisme. Tenim $72 = 2^3 \cdot 3^2$. Aleshores $l = 2, k_1 = 3, k_2 = 2$. Tenim $3 = 2 + 1 = 1 + 1 + 1, 2 = 1 + 1$, per tant $\Pi_1 = \{3, 2 + 1, 1 + 1 + 1\}, \Pi_2 = \{2, 1 + 1\}$, de forma que hi ha 6 classes d'isomorfisme de grups abelians d'ordre 72:

1. $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ amb divisors elementals $8, 9$;
2. $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ amb divisors elementals $4, 2, 9$;
3. $(\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/9\mathbb{Z}$ amb divisors elementals $2, 2, 2, 9$;
4. $\mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2$ amb divisors elementals $8, 3, 3$;
5. $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2$ amb divisors elementals $4, 2, 3, 3$;
6. $(\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^2$ amb divisors elementals $2, 2, 2, 3, 3$.

Determinem ara els factors invariants.

1. $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/72\mathbb{Z}$ té factors invariants $d_1 = 72$.
2. $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ té factors invariants $d_1 = 2, d_2 = 36$.
3. $(\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ té factors invariants $d_1 = 2, d_2 = 2, d_3 = 18$.
4. $\mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2 \simeq \mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ té factors invariants $d_1 = 3, d_2 = 24$.
5. $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2 \simeq \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ té factors invariants $d_1 = 6, d_2 = 12$.
6. $(\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^2 \simeq \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ té factors invariants $d_1 = 2, d_2 = 6, d_3 = 6$.

B

Grup lliure generat per un conjunt

Sigui S un conjunt. Posem $S' = S \times \{'\}$ i, per a cada $s \in S$m posem s' en lloc d'$(s,')$. Diem símbols els elements de $S \cup S'$. Sigui $G^*(S)$ el conjunt de successions finites de símbols; és a dir, el conjunt de paraules formades amb l'alfabet $S \cup S'$. Designem per e la successió buida. Direm que una paraula és reduïda si no conté parelles cancel·lables, és a dir, de la forma ss' o $s's$.

Exemple B.0.1. A $G^*(\{x, y\})$ les paraules $x, e, x'x'x'yxyx'$ són reduïdes; la paraula $xxyy'yxy'y'$ no és reduïda, ja que no conté yy' i $y'y$.

B.1

Reducció de paraules

Sigui $G(S)$ el subconjunt de $G^*(S)$ format per les paraules reduïdes. Per a cada paraula $w \in G^*(S)$, denotem per $\rho(w)$ la paraula reduïda associada a w definida en la forma següent:

1. si w és reduïda, posem $\rho(w) = w$;
2. si w no és reduïda, sigui $\tilde{w}$ la paraula obtinguda suprimint el primer parell cancel·lable de w;
3. si $\tilde{w}$ és reduïda, posem $\rho(w) = \tilde{w}$;
4. si $\tilde{w}$ no és reduïda, considerem $\tilde{\tilde{w}}$ i repetim el procés fins a obtenir una paraula reduïda que prenem com a $\rho(w)$.

Exemple B.1.1. Obtenim una aplicació $\rho : G^*(S) \longrightarrow G(S)$ que és la identitat sobre $G(S)$.

$$w = xxyy'x'yxx'y' \in G^*(\{x, y\}) \implies \begin{cases} \tilde{w} = xxx'yxx'y' \\ \tilde{\tilde{w}} = xyxx'y' \\ \tilde{\tilde{\tilde{w}}} = xyy' \\ \rho(w) = x \end{cases} \tag{B.1.1}$$

B.2

El grup $G(S)$

El conjunt $G^*(S)$ té una operació binària natural, la concatenació de paraules. És clar que e és l'element neutre, per la dreta i per l'esquerra, però $G^*(S)$ no és grup, ja que només e és invertible. Definim una operació binària en $G(S)$ per:

$$\begin{array}{rccc} \rho: & G(S) \times G(S) & \longrightarrow & G(S) \\ & (w, z) & \longmapsto & \rho(wz) = wz \end{array} \tag{B.2.1}$$

És clar que e és neutre i que tot element $w \in G(S)$ té invers. Tenim $s^{-1} = s', (s')^{-1} = s$ i, en general, l'invers d'una successió és la successió formada pels inversos dels seus termes, en ordre invers.

Lema B.2.1. *Siguin $w \in G(S)$ i $z \in G^*(S)$. Aleshores, $\rho(wz) = \rho(w\rho(z))$ i $\rho(zw) = \rho(\rho(z)w)$.*

Demostració. Provem la primera igualtat, la segona es prova de forma anàloga. Si z és reduïda, tenim $\rho(z) = z$ i la igualtat és una identitat. Suposem que z no és reduïda. Fem inducció sobre el nombre de símbols de z. Si l'últim símbol de w i el primer de z no formen un parell cancel·lable, aleshores el primer parell cancel·lable de wz coincideix amb el primer parell cancel·lable de z i, per tant, $\rho(wz) = \rho(w\tilde{z})$. Per hipòtesi d'inducció, $\rho(w\tilde{z}) = \rho(w\rho(\tilde{z}))$ i $\rho(\tilde{z}) = \rho(z)$; per tant $\rho(wz) = \rho(w\rho(z))$.
Suposem ara que l'últim símbol de w i el primer de z formen un parell cancel·lable. Sigui $w = us, z = s't$, amb $s \in S, u \in G(S), t \in G^*(S)$. Aleshores $\rho(wz) = \rho(ut) = \rho(u\rho(t))$, on la segona igualtat és per hipòtesi d'inducció. D'altra banda, $\rho(w\rho(z)) = \rho\left(us\rho\left(s't\right)\right) = \rho\left(us\rho\left(s'\rho(t)\right)\right)$, on de nou la segona igualtat és per hipòtesi d'inducció. Posant $v = \rho(t)$, n'hi ha prou amb veure $\rho(uv) = \rho\left(us\rho\left(s'v\right)\right)$, per a tot parell de paraules reduïdes u, v. Suposem primer que s no és el primer símbol de v. Aleshores $s'v$ és reduïda i per tant $\rho\left(us\rho\left(s'v\right)\right) = \rho\left(uss'v\right) = \rho(uv)$. Si ara $v = sx, \rho\left(s'v\right) = \rho\left(s'sx\right) = x$, ja que x és reduïda i $\rho\left(us\rho\left(s'v\right)\right) = \rho(usx) = \rho(uv)$. ■

Proposició B.2.2. *L'operació producte definida a $G(S)$ és associativa.*

Demostració. Siguin $u, v, w \in G(S)$. Aleshores, $u(vw) = \rho(u\rho(vw)) = \rho(uvw)$, on la primera igualtat es dedueix de la definició de $\cdot$ i la segona del lema anterior. Anàlogament, $(uv)w = \rho(\rho(uv)w) = \rho(uvw)$. Hem provat que $(G(S), \cdot)$ és un grup, que anomenarem *grup lliure generat per S*. ■

Observació B.2.3. Tot element w de $G(S)$ es pot escriure d'una única manera en la forma $w = s_1^{\varepsilon_1} \cdots s_r^{\varepsilon_r}$, on $r \in \mathbb{N}; s_1, \ldots, s_r \in S; \varepsilon_i = \pm 1, 1 \leq i \leq r$ i $\varepsilon_{i+1} \neq -\varepsilon_i$ si $s_{i+1} = s_i$. Direm que $s_1^{\varepsilon_1} \cdots s_r^{\varepsilon_r}$ és la forma canònica de w. En particular, $S \subset G(S)$ i S genera $G(S)$.

Proposició B.2.4. *Sigui S un conjunt, G un grup i $f : S \longrightarrow G$ una aplicació. Aleshores, existeix un únic morfisme de grups $\varphi : G(S) \longrightarrow G$ tal que $\varphi(s) = f(s)$ per a tot $s \in S$. A més,* $\mathrm{im}(\varphi) = \langle f(S) \rangle$.

Demostració. Volem que φ sigui morfisme, per tant l'única definició possible és:

$$\varphi\left(s_1^{\varepsilon_1} \ldots s_r^{\varepsilon_r}\right) = f\left(s_1\right)^{\varepsilon_1} \ldots f\left(s_r\right)^{\varepsilon_r}. \tag{B.2.2}$$

Amb aquesta definició, obtenim un morfisme ja que la imatge per φ d'un parell cancel·lable és el neutre de G. Ara, com S genera $G(S), \varphi(S) = f(S)$ genera $\mathrm{im}(\varphi)$. ■

Si $S \subset G$ és un conjunt de generadors de G i $f : S \to G$ és la inclusió, aleshores el morfisme $\varphi : G(S) \to G$ és un epimorfisme. Aplicant el primer teorema d'isomorfia aplicat a grups, obtenim que tot grup és quocient d'un grup lliure.

C

Grups definits per generadors i relacions

Definició C.0.1. Sigui G un grup i S un sistema de generadors de G. Sigui $\varphi : G(S) \longrightarrow G$ el morfisme corresponent a la inclusió de S en G. Els elements de $\ker(\varphi)$ s'anomenen relacions de S.

Exemple C.0.2. Considerem el grup S_3, el sistema de generadors $\{t_1, s_1\}$, on $t_1 = (2,3)$ i $s_1 = (1,2,3)$, i el morfisme $\varphi : G(\{t_1, s_1\}) \longrightarrow S_3$. Aleshores, $t_1^2, s_1^3, t_1 s_1 t_1 s_1$ són relacions ja que a S_3 es compleix $t_1^2 = e, s_1^3 = e, t_1 s_1 t_1 s_1 = e$.

Notació C.0.3. Si tenim una relació u, normalment diem la relació $u = e$, Si tenim una relació uv^{-1}, normalment diem la relació $u = v$.

Definició C.0.4. Sigui ara S un conjunt i $R \subset G(S)$. Posem $N(R)$ el mínim subgrup normal de $G(S)$ que conté R, és a dir la intersecció de tots els subgrups normals de $G(S)$ que contenen R i posem $G(S,R) = G(S)/N(R)$. Direm que $G(S,R)$ és el grup definit pel conjunt de generadors S i les relacions R. Més en general, direm que un grup G està definit pels generadors S i les relacions R si és isomorf a $G(S,R)$.

Exemple C.0.5. El grup S_3 és el grup definit pels generadors t_1, s_1i les relacions $t_1^2 = e, s_1^3 = e, t_1 s_1 t_1 s_1 = e$. En efecte, si $S = \{t_1, s_1\}$, en el subgrup quocient de $G(S)$ pel mínim subgrup normal $N(R)$ de $G(S)$ que conté el conjunt $S = \{t_1^2, s_1^3, t_1 s_1 t_1 s_1\}$, es compleix $t_1 s_1 = s_1^{-1} t_1^{-1} = s_1^2 t_1$ i , per tant, els elements d'aquest quocient són $e, t_1, s_1, s_1 t_1, s_1^2, s_1^2 t_1$. Tenim doncs $G(S,R) \simeq S_3$.

Bibliografia

[Lan02] Serge. Lang. *Algebra*. eng. 3rd ed. 2002. Graduate Texts in Mathematics, 211. New York, NY: Springer New York, 2002. ISBN: 1-4613-0041-X.

This book is intended as a basic text for a one-year course in Algebra at the graduate level, or as a useful reference for mathematicians and professionals who use higher-level algebra. It successfully addresses the basic concepts of algebra. For the revised third edition, the author has added exercises and made numerous corrections to the text.

[Tra20] Artur Travesa. *Estructures algebraiques*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2020.

Apunts de l'assignatura Estructures Algebraiques, impartida per Artur Travesa.

[Del21] Félix Delgado. *Introducción al álgebra*. spa. 2ª edición. Madrid: Ediciones Paraninfo, 2021. ISBN: 9788413664972.

Ampli recull dels continguts obligatoris de l'assignatura d'Àlgebra dels estudis de Grau en Matemàtiques de la majoria d'universitats, amb nombrosos exercicis i problemes complementaris. El segon volum inclou el solucionari dels problemes complementaris.

[Vil21] Mario Vilar. *Aritmètica*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2021. URL: `https://mariovilar.github.io/matematiques-enginyeria-informatica/1/segon-semestre/ARIT/2020-2021ApuntsARITM.pdf`.

Apunts de l'assignatura Aritmètica, impartida per Artur Travesa i Luis Dieulefait durant el semestre de primavera del curs 2020/2021.

[Cre22] Teresa Crespo. *Estructures algebraiques*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2022.

Apunts de l'assignatura Estructures Algebraiques, impartida per Teresa Crespo durant el semestre de tardor del curs 2022-2023.

[Vil22] Mario Vilar. *Geometria Lineal*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2022. URL: `https://mariovilar.github.io/matematiques-enginyeria-informatica/2/tercer-semestre/GL/GL.pdf`.

Apunts de l'assignatura.