Apunts d'àlgebra

Llorenç Cerdà-Alabern
llorenc@ac.upc.edu
Barcelona, 11 d'octubre de 2017

Índex

Prefaci

Vaig escriure aquests apunts mentre preparava l'assignatura *Estructuras algebráicas* del curs 2015-16 i *Àlgebra* del curs 2016-17 del grau de matemàtiques de la UNED. Els apunts estan basats fonamentalment en el llibres de les assignatures [3, 4] Gallian [2] i Schaum [1]. El contingut no és rigorós ni complert, i només hi ha demostracions senzilles orientades a entendre o ajudar a memoritzar les relacions que demostren. L'edició l'he fet amb LaTeX.

Capítol 1
Definicions

Definició 1.1 Relació d'equivalència en un conjunt X és un conjunt $R \subseteq X^2$ de parells ordenats d'elements d'X tals que:

1. $(a,a) \in R \forall a \in X$ (**propietat reflexiva**).
2. $(a,b) \in R \Rightarrow (b,a) \in R$ (**propietat de simetria**).
3. $(a,b),(b,c) \in R \Rightarrow (a,c) \in R$ (**propietat transitiva**).

Exemple 1.1 (relació d'equivalència)
Si $X = \{1,2,3,4\}$,

$$R = \{(1,1),(2,2),(3,3),(4,4),(1,3),(1,4),\\ (3,1),(3,4),(4,1),(4,3)\}$$

és una relació d'equivalència en X. Notar que $3R4$, doncs $(3,4) \in R$, però $2\not R4$ ($2R4$ no és correcte), doncs $(2,4) \notin R$.

Notació S'escriu $a\,R\,b$ o, en termes conjuntistes, $(a,b) \in R$. També s'escriu $a \sim b$ o $a \equiv b$ en comptes d'$a\,R\,b$, doncs una relació d'equivalència és una generalització del concepte d'igualtat. Per exemple, la relació de congruència en $\mathbb{Z}$ (veure l'apèndix B) és una relació d'equivalència i en $\bmod 10$ s'escriu $3 \equiv 13$, doncs $3 \bmod 10 = 13 \bmod 10$.

Definició 1.2 Funció (o aplicació, *mapping*)

$$f : A \to B$$

d'un conjunt A (domini) a un conjunt B (codomini) és una regla que fa correspondre a cada element a (preimatge de b) de A exactament un element $b = f(a)$ (imatge de a) de B. El subconjunt de B que conté totes les imatges de A es diu imatge de A, i es denota per $f(A)$[1].
Nota: Amb la notació del Schaum's [1] es fan servir lletres gregues per a les funcions, *mappings*, (p.e. α en comptes de f), i en comptes de la notació $b = \alpha(a)$ es posa $b = a\alpha$.

Definició 1.3 Funció restringida a un subconjunt. Sigui $f : A \to B$ i $X \subseteq A$ aleshores es defineix

$$f|_X : X \to B \tag{1.1}$$

a la funció que assigna a cada element $x \in X$ l'element $f(x) \in B$.

Definició 1.4 Composició de funcions $f : A \to B$ i $g : B \to C$ és

$$(g \circ f)(x) = g\,f(x) = g(f(x)),\ x \in A \tag{1.2}$$

Nota: Amb la notació del Schaum's [1] es fan servir lletres gregues per a les funcions (*mappings*) (p.e. α i β en comptes de f i g), i en comptes de la notació $(\beta \circ \alpha)(x) = \beta(\alpha(x))$ es posa $(x\alpha)\beta$. Notar que amb la notació del Schaum's es canvia l'ordre de les funcions, és a dir, $(x\alpha)\beta = (\beta \circ \alpha)(x) = \beta(\alpha(x))$.

Definició 1.5 Funció injectiva (*one-to-one*)

$$\forall (a,b) \in A :\ f(a) = f(b) \Rightarrow a = b \tag{1.3}$$

És a dir, a iguals imatges, iguals preimatges.

Definició 1.6 Funció surjectiva (*sobreyectiva, onto*)

$$f : A \to B \text{ onto } \Rightarrow \forall b \in B\ \exists a \in A\ :\ f(a) = b \tag{1.4}$$

És a dir, tots els elements del codomini tenen una preimatge. Notar que una funció surjectiva pot no ser injectiva.

Definició 1.7 Funció bijectiva (*bijective*) És una funció que és injectiva i surjectiva (*one-to-one and onto*). És a dir, a tots els elements del domini correspon un element diferent del codomini, i viceversa. Per tant. una bijecció d'un conjunt X en Y té inversa de Y en X. Si X és finit, Y té el mateix nombre d'elements. Una funció bijectiva d'un conjunt en ell mateix també s'anomena **permutació (*permutation*)**. Quan una funció f és bijectiva també es posa $f(X) = X$, on s'entén que $f(X)$ és el conjunt que s'obté al aplicar la funció f a tots els elements del conjunt X.

Definició 1.8 Operació binària en un conjunt G és una funció que assigna a cada parell ordenat d'elements de G un element de G.

Definició 1.9 Partició d'un conjunt G és una descomposició de G en conjunts disjunts X_i tals que qualsevol element de G està contingut en algun X_i. És a dir

$$X_i \cap X_j = \emptyset, \forall i.j$$
$$\cup_i X_i = G$$

Definició 1.10 Classe generada per una relació d'equivalència. Sigui R una relació d'equivalència en un conjunt no buit X. Es diu la classe de l'element $a \in X$ generada per R al subconjunt $a\,R$ de X donat per:

$$a\,R = \{b\ :\ a\,R\,b, \forall b \in X\}$$

Exemple 1.2 (classe generada)
Si $X = \{1,2,3,4\}$,

$$R = \{(1,1),(2,2),(3,3),(4,4),(1,3),(1,4),\\ (3,1),(3,4),(4,1),(4,3)\}$$

és una relació d'equivalència en X i les classes generades per R són:

$$1\,R = \{1,3,4\}$$
$$2\,R = \{2\}$$
$$3\,R = \{3,1,4\}$$
$$4\,R = \{4,1,3\}$$

Notar que $1\,R = 3\,R = 4\,R$.

Teorema 1.1 (partició)
Sigui R una relació d'equivalència en un conjunt no buit X. Llavors

[1] Alguns autors distingeixen funció i aplicació considerant que una funció pot fer correspondre el conjunt buit a un element, mentre una aplicació sempre fa correspondre un element que no és el conjunt buit.

1. Si $a\,R \cap b\,R \neq \emptyset$, aleshores $a\,R = b\,R$.
2. $a \in a\,R$, $\forall a \in X$.

La prova és immediata a partir de la definició de relació d'equivalència (1.1, pàg. 1). Per tant, les classes generades per R en X formen una partició de X. Es fa servir la notació X/R per a referir-se a aquesta partició.

El contrari també és cert: donada una partició P existeix una relació d'equivalència R que genera les classes que són els elements de P. Per això basta definir la relació d'equivalència R tal que $a\,R\,b$ si a i b pertanyen al mateix element de P.

NOTA: De la definició de classe generada per R tenim que si $a\,R\,b$ llavors $b \in a\,R$. Del teorema anterior tenim que si $b \in a\,R$ llavors $b\,R = a\,R$. Efectivament, en l'exemple 1.2 es va calcular: $1\,R = \{1, 3, 4\}$, per tant haurà de ser $1\,R = 3\,R = 4\,R$, tal com es va obtenir.

Definició 1.11 Conjunts quocients La partició X/R que resulta de les classes generades per una relació d'equivalència R en un conjunt X (veure el teorema 1.1) s'anomenen **conjunts quocients**. En l'exemple 1.2 els conjunts quocients són $X/R = \{\{1, 3, 4\}, \{2\}\}$.

Capítol 2
Grups

Definició 2.1 Grup[1] és un conjunt G dotat d'una operació binària $a\,b$ (normalment la multiplicació) que compleix:

1. Associativitat: $(a\,b)\,c = a\,(b\,c)$.
2. Identitat: Existeix l'element neutre o identitat e tal que $a\,e = e\,a = a$. Nota: es farà servir indistintament la notació e o 1 per referir-se a l'element identitat.
3. Inversa: $a\,a^{-1} = a^{-1}\,a = e$.

Per exemple, el conjunt d'enters $\mathbb{Z}$ i l'operació binària $+$ és un grup. L'element neutre és 0, doncs $a + 0 = a$, $\forall a \in \mathbb{Z}$, i l'element invers és $a^{-1} = -a$, doncs $a - a = 0$, $\forall a \in \mathbb{Z}$. Aquest grup es denota per la tupla $(\mathbb{Z},+)$ (o simplement per *grup* $\mathbb{Z}$) i s'anomena el **Grup additiu dels enters**. Altres exemples són:

- **Grup additiu dels racionals**, $(Q,+)$.
- **Grup multiplicatiu dels racionals diferents de zero**, $Q^* = Q \setminus \{0\}$. Notar que amb el 0 no seria un grup, doncs 0 no té inversa.
- **Grup additiu dels enters mòdul** n: $\mathbb{Z}_n = \{0, 1, 2, \cdots (n-1)\}$.
- **Grup additiu dels enters múltiples de** m: $m\,\mathbb{Z} = \{m\,x : x \in \mathbb{Z}\} = \{\cdots, -2\,m, -m, 0, m\,2, m, \cdots\}$.

Exemple 2.1 (grup quaternió)
Veure [3, ex. 14, pàg 49]. És el grup format per els 8 símbols:

$$Q = \{1, -1, i, j, k, -i, -j, -k\} \tag{2.1}$$

amb l'operació $Q \times Q \to Q$ associativa, element neutre $e = 1$, que compleix la regla usual del signe: $a\,(-b) = -(a\,b)$, $\forall a,b \in Q$, i:

$$\begin{aligned} i &= j\,k = -k\,j \\ j &= k\,i = -i\,k \\ k &= i\,j = -j\,i \\ i^2 &= j^2 = k^2 = -1. \end{aligned}$$

Per exemple, l'element invers de i és $i^2\,i^2 = 1 \to i\,i^3 = 1 \to i^{-1} = i^3$. En els exemples 2.8, pàg. 6 i 2.2, pàg. 5 s'investiguen les propietats d'aquest grup.

Proposició 2.1 La condició d'associativitat d'un grup implica que l'element invers és únic.

Demostració. Si un element a té 2 elements inversos h, h', aleshores seria:

$$\begin{aligned} h &= h\,e \\ &= h\,(a\,h') \\ &= (h\,a)\,h' \\ &= e\,h' \\ &= h' \end{aligned}$$

□

Teorema 2.1 (e **és únic)**
L'element neutre e és únic.

Demostració. Si hi hagués 2 elements neutres e i e' seria $e\,e' = e$ i $e\,e' = e'$. Per tant $e = e'$. □

Teorema 2.2 (Cancel·lació)

$$b\,a = c\,a \Rightarrow b = c \tag{2.2}$$
$$a\,b = a\,c \Rightarrow b = c. \tag{2.3}$$

Teorema 2.3 $(a\,b)^{-1} = b^{-1}\,a^{-1}$

[1] Nota: Alguns autors, com en el Schaum's [1], introdueixen primer el conceptes de: (1) **grupoide**, tupla (G, α) formada per un conjunt G i una operació, α, binària en G; (2) **grupoide abelià**, si l'operació és commutativa; i (3) **grupoide associatiu o semigrup**, si l'operació és associativa.

Demostració.

$$\begin{aligned}(a\,b)(b^{-1}\,a^{-1}) &= a\,(b\,b^{-1})\,a^{-1}\\ &= a\,e\,a^{-1}\\ &= a\,a^{-1}\\ &= e\end{aligned}$$ □

Definició 2.2 Subgrup H és un subconjunt de G que és també un grup sota la mateixa operació binaria de G. Amb altres paraules, és una tupla $(H, \cdot\,|_H)$, $H \subseteq G$ que també és grup, on $\cdot|_H$ és la operació binària de G restringida a H. Notar que els subconjunts formats per l'element neutre $\{e\}$, o el mateix grup G són també subgrups de G. Si un subgrup H de G és $H \neq \{e\}$ i $H \neq G$ es diu **subgrup propi**.

Teorema 2.4 Tots els subgrups del grup additiu dels enters $(\mathbb{Z},+)$ són subconjunts de la forma

$$m\,\mathbb{Z} = \{m\,x : x \in \mathbb{Z}\} = \{\cdots, -m\,2, -m, 0, m, m\,2, \cdots\} \quad (2.4)$$

on m és un enter no negatiu. Veure la demostració en [3, pàg. 27].

Test de subgrup Sigui $H \neq \emptyset, H \subset G$. H és un subgrup de G si es compleix qualsevol de les següents condicions:

$$a\,b^{-1} \in H, \forall a,b \in H. \quad (2.5)$$
$$a\,b \in H, \forall a,b \in H \text{ i } a^{-1} \in H, \forall a \in H. \quad (2.6)$$
$$H \text{ és finit i tancat sota l'operació binària de } G. \quad (2.7)$$

Definició 2.3 Grup abelià és un grup que a més té la propietat commutativa: $a\,b = b\,a$.

Notar que un grup de 2 elements és abelià, doncs un dels elements ha de ser l'element neutre, que és commutatiu.

Teorema 2.5 Sigui el grup G.
1. Si $a^2 = e, \forall a \in G$, llavors G és abelià.
2. Si $(a\,b)^2 = a^2\,b^2, \forall a,b \in G$, llavors G és abelià.

Demostració. (1) $a^2 = e \Rightarrow a = a^{-1} \Rightarrow a\,b = (a\,b)^{-1} = b^{-1}\,a^{-1} = b\,a$. (2) $a\,(b\,a)\,b = (a\,b)^2 = a^2\,b^2 = a\,(a\,b)\,b \Rightarrow a\,b = b\,a$. □

Definició 2.4 Ordre d'un grup $\mathrm{o}(G)$ és el nombre d'elements de G (pot ser ∞).

Notar que el grup additiu dels enters i tots els seus subgrups són infinits, Veure el teorema 2.4.

Definició 2.5 Subgrup generat $\langle S\rangle$. Sigui $S \neq \emptyset, S \subset G$. Es defineix el subgrup generat per S a:

$$\langle S\rangle = \{s_1^{h_1}\,s_2^{h_2}\cdots s_n^{h_n} : n \in \mathbb{N}, s_i \in S, h_i \in \mathbb{Z}\} \quad (2.8)$$

Demostració. Donats

$$\begin{aligned}x,y &\in \langle S\rangle,\\ x &= s_1^{h_1}\,s_2^{h_2}\cdots s_n^{h_n},\\ y &= t_1^{p_1}\,t_2^{p_2}\cdots t_n^{p_m}.\end{aligned}$$

Tenim $x\,y^{-1} = s_1^{h_1}\,s_2^{h_2}\cdots s_n^{h_n}\,t_1^{-p_1}\,t_2^{-p_2}\cdots t_n^{-p_m} \in \langle S\rangle$. Per tant, per (2.5) $\langle S\rangle$ és un subgrup de G. □

Definició 2.6 Sistema generador. Sigui $S \neq \emptyset, S \subseteq G$. Es diu que S és un sistema generador de G si $\langle S\rangle = G$.

Es diu que S és un **generador minimal** de G si qualsevol **subconjunt propi** d'S (és a dir, diferent d'$\{e\}$ i de S) pot generar només un subgrup G d'ordre estrictament menor que G (és a dir, un **subgrup propi** de G). Amb altres paraules, no es pot prescindir de cap element d'S perquè sigui un generador de G.

Exemples:
1. $\langle G\rangle = G$.
2. $\langle S\rangle = \mathbb{Z}, S = \{1\}$, doncs per a qualsevol $n \in \mathbb{Z}$:

$$n = \begin{cases}1^n = 1 + 1 + \cdots 1, & n > 0\\ 1^{-n} = -1 - 1 - \cdots 1, & n < 0\end{cases}$$

Nota: recordar que per $\mathbb{Z}$ l'operació és la suma, veure el grup additiu dels enters en 2.1, pàg. 3.

Definició 2.7 Grup finitament generat. Un grup G que té un sistema generador finit es diu finitament generat. Tot grup finit és finitament generat, doncs G és un sistema generador de G. El recíproc no és cert. Per exemple, el grup additiu d'enters té el generador finit $S = \{1\}$ (com s'ha vist en l'exemple anterior), i no és un grup finit.

Teorema 2.6 Sigui G un grup i $a \in G$. Llavors $\langle a\rangle$ és un subgrup de G.

Demostració. Com que $a \in \langle a\rangle$, $\langle a\rangle \neq \emptyset$. Tenim $a^n \in \langle a\rangle$ i $a^n\,(a^n)^{-1} = a^n\,a^{-n} = a^{n-n} = e \in \langle a\rangle$. Per tant, per (2.5) $\langle a\rangle$ és un subgrup de G. □

Corol·lari 2.1 del teorema 2.6. Al ser $\langle a\rangle$ un subgrup de G, per el teorema de Lagrange (veure 4.1, pàg. 13) $\mathrm{o}(\langle a\rangle)$ divideix $\mathrm{o}(G)$.

Definició 2.8 Ordre d'un element a d'un grup G, $\mathrm{o}(a)$ és el menor enter n tal que $a^n = e$. Si no existeix, es diu que l'ordre és infinit, altrament es diu que a és un element de **torsió**. Notar que $\mathrm{o}(a)$ és també l'ordre del subgrup generat per el conjunt $S = \{a\}$, és a dir $\langle a\rangle$. Veure la def. 2.5 de subgrup generat.

Exemple 2.2 (ordre d'un element)
Per el grup quaternió (veure 2.1, pàg. 3):

$$\begin{aligned}\mathrm{o}(-1) &= 2, \text{ doncs } (-1)^2 = 1\\ \mathrm{o}(i) = \mathrm{o}(j) &= \mathrm{o}(k) = 4, \text{ doncs } i^4 = j^4 = k^4 = 1\\ \langle -1\rangle &= \{1 = (-1)^2, -1\}\\ \langle i\rangle &= \{1 = i^4, i, i^2 = -1, i^3 = -i\}\end{aligned}$$

Propietats 2.1 d'un element de torsió a amb $n = \mathrm{o}(a)$:
1. $\mathrm{o}(a)$ és el menor natural $n \geq 1$ tal que $a^n = e$.
2. $\langle a\rangle = \{e,a,a^2,\cdots,a^{n-1}\}$.
3. Si $a^k = e$, llavors k és múltiple de n.
4. $\mathrm{o}(a) = 1$ sii $a = e$.
5. a^{-1} és un element de torsió i $\mathrm{o}(a^{-1}) = \mathrm{o}(a)$.
6. Si $x = a^k \in \langle a\rangle$, llavors x és un element de torsió i $\mathrm{o}(x) = n/\gcd(n,k)$.

Veure la demostració en [3, pàg. 37].

2.1 Grups cíclics

Definició 2.9 Grup cíclic G és un grup cíclic si existeix un **element generador** $a \in G$ tal que

$$G = \langle a\rangle = \{a^n \ : \ n \in \mathbb{Z}\} \tag{2.9}$$

Denotarem un grup cíclic d'ordre n per C_n.

Teorema 2.7 Si $a \in G$ té ordre infinit, aleshores $a^i = a^j$ sii $i = j$. Si a té ordre finit n, aleshores $\langle a\rangle = \{e, a, a^2, \cdots, a^{n-1}\}$ i $a^i = a^j$ sii n divideix $i - j$. Corol·laris: (1) $\mathrm{o}(a) = \mathrm{o}(\langle a\rangle)$. (2) Si $\mathrm{o}(a) = n$ i $a^d = e$, aleshores n divideix d. Veure la demostració en [2, pàg. 73]. (3) Un grup finit G és cíclic sii té un element $a \in G$ tal que $\mathrm{o}(a) = \mathrm{o}(G)$ (doncs $G = \langle a\rangle = \{e, a, a^2, \cdots, a^{n-1}\}$).

Més endavant es veurà que un grup d'ordre un nombre primer és cíclic (veure el corol·lari del teorema de Lagrange 4.1, pàg. 13).

Exemple 2.3 (grup no cíclic)
El grup quaternió Q (veure 2.1, pàg. 3) no és cíclic, doncs $\mathrm{o}(Q) = 8$ i Q no té cap element d'ordre 8 (veure l'exemple 2.2, pàg. 5).

Exemple 2.4 (grup cíclic $\mathbb{Z}$)
El grup additiu dels enters és cíclic amb generadors $\{1\}$ i $\{-1\}$, doncs per $\{1\}$

$$n = \begin{cases} 1^n = 1 + 1 + \cdots 1 & n \geq 0\\ 1^{-n} = -1 - \cdots - 1 & n \leq 0\end{cases}$$

és a dir, $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.

Exemple 2.5 (grup cíclic $\mathbb{Z}_n$)
El grup additiu dels enters mòdul n ($\mathbb{Z}_n = \{0, 1, 2, \cdots (n-1)\}$) és cíclic amb generadors $\{1\}$ i $\{-1\}$, doncs per $\{1\}$

$$n = \begin{cases} 1^n = 1 + 1 + \cdots 1 & n \geq 0, \text{ aritmètica mòdul } n\\ 1^{-n} = -1 - \cdots - 1 & n \leq 0, \text{ aritmètica mòdul } n\end{cases}$$

és a dir, $\mathbb{Z}_n = \langle 1\rangle = \langle -1\rangle$, en aritmètica mòdul n. A diferència de $\mathbb{Z}$, que només té els generadors $\{1\}$ i $\{-1\}$, com es veurà a continuació, $\mathbb{Z}_n$ en pot tenir més. Notar també que -1 és la inversa de 1, és a dir $1 - 1 = 0$. Per tant, $-1 = n - 1$ en aritmètica mòdul n.

Teorema 2.8 Tot grup cíclic és abelià.

Demostració. Si G és cíclic i $x,y \in G$, llavors existeixen els enters n,m tals que $x = a^n$, $y = a^m$. Per tant, $x\,y = a^{m+n} = y\,x$. □

El contrari no és cert (no tot grup abelià és cíclic).

Teorema 2.9 $\mathrm{o}(a) = n \Rightarrow \langle a^d\rangle = \langle a^{\gcd(n,d)}\rangle$ i $\mathrm{o}(a^d) = n/\gcd(n,d)$. Corol·laris: (1) En un grup finit l'ordre d'un element divideix l'ordre del grup. (2) Si $\mathrm{o}(a) = n$, aleshores $\langle a^i\rangle = \langle a^j\rangle$ sii $\gcd(n,i) = \gcd(n,j)$ i $\mathrm{o}(a^i) = \mathrm{o}(a^j)$ sii $\gcd(n,i) = \gcd(n,j)$. (3) Si $\mathrm{o}(a) = n$, aleshores $\langle a\rangle = \langle a^j\rangle$ sii $\gcd(n,j) = 1$ i $\mathrm{o}(a) = \mathrm{o}(a^j)$ sii $\gcd(n,j) = 1$. (4) Un enter $k \in \mathbb{Z}_n$ és un generador de $\mathbb{Z}_n$ sii $\gcd(n,k) = 1$, és a dir, n,k són primers relatius. Veure la definició de primer relatiu en 13.14, pàg. 38. Veure la demostració en [2, pàg. 75].

Exemple 2.6 (Generadors i subgrups de $\mathbb{Z}_8$)
(Veure [2, pàg. 73]) $\mathbb{Z}_8 = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$, doncs els primers relatius de 8 són $\{1, 3, 5, 7\}$. Veure la definició de primer relatiu en 13.14, pàg. 38. Per exemple $\mathbb{Z}_8 = \langle 3\rangle = \{3, 3+3, 3+3+3, \cdots\} = \{3, 6, 9, 12, 15, 18, 21, 24\} = \{3, 6, 1, 4, 7, 2, 5, 0\}$, en aritmètica mòdul 8. A més $\mathrm{o}(1) = \mathrm{o}(3) = \mathrm{o}(5) = \mathrm{o}(7) = 8$. Notar també que $\langle 2\rangle = \{2, 4, 6, 0\}$, $\langle 4\rangle = \{4, 0\}$, $\langle 6\rangle = \{6, 4, 2, 0\} = \langle 2\rangle$. Per tant $\mathrm{o}(2) = 4$, $\mathrm{o}(4) = 2$, $\mathrm{o}(6) = 4$. Veiem doncs que $\mathbb{Z}_8$ té 4 subgrups, els subgrups impropis $\{0\}$ i $\{0,1,\cdots 7\}$ generats per $\{1, 3, 5, 7\}$, i els subgrups propis $\{0, 4\}$ i $\{0, 2, 4, 6\}$ generats per $\{4\}$ i $\{2, 6\}$, respectivament.

Teorema 2.10 Teorema fonamental dels grups cíclics: Tot subgrup d'un grup cíclic, és també cíclic. Si $o(\langle a\rangle) = n$, aleshores l'ordre de qualsevol subgrup de $\langle a\rangle$ és divisor d'n i per cada divisor d de n hi ha exactament un subgrup d'ordre d: $\langle a^{n/d}\rangle$. Veure la demostració en [2, pàg. 77].

Si considerem $\mathbb{Z}_n$ i $a = 1$ en el teorema anterior, obtenim:

Corol·lari 2.2 (subgrups de $\mathbb{Z}_n$) Per cada divisor d de n, $\langle n/d\rangle$ és l'únic subgrup de $\mathbb{Z}_n$ d'ordre d. A més, aquests són els únics subgrups de $\mathbb{Z}_n$.

Teorema 2.11 Si d és un divisor positiu d'n, el nombre d'elements d'ordre d en un grup cíclic d'ordre n és la funció $\phi(n)$ d'Euler. Veure l'apèndix C. Corol·lari: en un grup finit el nombre d'elements d'ordre d és divisible per $\phi(d)$. Veure la demostració en [2, pàg. 79].

Exemple 2.7 (subgrups de $\mathbb{Z}_8$) Els divisors de 8 són $1, 2, 4, 8$. Per tant, del corol·lari 2.2 tenim que els subgrups de $\mathbb{Z}_8$ són:

$$\{\langle 8\rangle, \langle 4\rangle, \langle 2\rangle, \langle 1\rangle\}$$

amb ordres iguals als divisors:

$$o(\langle 8\rangle) = 1, o(\langle 4\rangle) = 2, o(\langle 2\rangle) = 4, o(\langle 1\rangle) = 8.$$

Del teorema 2.11 tenim que el nombre d'elements de $\mathbb{Z}_8$ que generen aquests conjunts són:

$$\begin{aligned}\langle 8\rangle &: \phi(1) = 1\\ \langle 4\rangle &: \phi(2) = 1\\ \langle 2\rangle &: \phi(4) = 2\\ \langle 1\rangle &: \phi(8) = 4\end{aligned}$$

Els subgrups d'ordre 8 són els generadors de $\mathbb{Z}_8$, és a dir, els generats per els primers relatius de 8: $\{1, 3, 5, 7\}$. Deduïm doncs que els 2 elements generadors del subgrup d'ordre 4 són $\{2, 6\}$. Es pot comprovar que aquests resultats coincideixen amb els obtinguts en l'exemple 2.6.

2.2 Propietats dels grups

Definició 2.10 Subgrup conjugat Si G és un grup, H és un subgrup de G i $a \in G$, es diu **subgrup conjugat** de H al conjunt (veure la definició de conjunt conjugat 2.14, pàg. 7):

$$H^a = a^{-1} H a = \{a^{-1} h a : h \in H\}$$

Com és veurà més endavant, H i H^a són isomorfs (teorema 7.6, pàg. 18). Això vol dir que els subgrups H i H^a tenen les mateixes propietats de la teoria de grups. Per exemple, si H és cíclic, llavors H^a també ho és, si H és abelià, llavors H^a també ho és, etc.

Definició 2.11 Centre d'un grup, $Z(G) \subset G$ és el subconjunt d'elements de G que commuten amb tots els elements de G:

$$Z(G) = \{a \in G \ : \ a\,b = b\,a\ \forall b \in G\}. \tag{2.10}$$

Notar que si G és abelià, llavors $Z(G) = G$.

Teorema 2.12 El centre d'un grup, $Z(G)$ és un subgrup. Veure la demostració en [3, pàg. 31].

Exemple 2.8 (centre d'un grup)
Calcular el centre del grup quaternió definit en 2.1, pàg. 3 (exercici 22 [3, pàg 114]).

Solució Els elements i, j, k no commuten però $1, -1$ si. Per exemple, $i\,j = -j\,i$. Per tant. $Z(Q) = \{1, -1\}$. Es pot comprovar que efectivament $Z(Q)$ és un subgrup de Q, a més cíclic, doncs $(-1)^2 = 1$. En l'exemple 2.2, pàg. 5 s'investiguen més propietats d'aquest grup.

Definició 2.12 Centralitzador d'un element a, $C(a) \subset G$ és el subconjunt d'elements de G que commuten amb a:

$$C(a) = \{b \in G \ : \ a\,b = b\,a\}. \tag{2.11}$$

Teorema 2.13 Per a cada $a \in G$, el centralitzador de a és un subgrup.

Definició 2.13 Centralitzador d'un subgrup H de G, $C(H) \subset G$ és el subconjunt d'elements de G que commuten amb tots els elements d'H:

$$C(H) = \{x \in G \ : \ a\,x = x\,a, \forall a \in H\}. \tag{2.12}$$

Teorema 2.14 $C(H)$ és un subgrup de G.

Demostració. Clarament, $1 \in C(H)$. Siguin $x,y \in C(H)$ i $a \in G$. Es té $a\,x = x\,a$ i $a^{-1}\,y = y\,a^{-1}$, per tant:

$$\begin{aligned}&a\,(x\,y^{-1}) = (a\,x)\,y^{-1} = (x\,a)\,y^{-1} = x\,(a\,y^{-1}) =\\ &x\,(y\,a^{-1})^{-1} = x\,(a^{-1}\,y)^{-1} = x\,(y^{-1}\,a) = (x\,y^{-1})\,a\end{aligned}$$

així doncs $x\,y^{-1} \in C(H), \forall x,y \in C(H)$, i per (2.5) $C(H)$ és un subgrup de G. □

Definició 2.14 Conjugat d'un subconjunt S per un element a . Si S és un subconjunt no buit de G i $a \in G$, s'anomena conjugat de S per a al conjunt

$$S^a = \{a^{-1}\, x\, a : x \in S\}$$

Propietats 2.2 Del conjunt conjugat:
1. $S \to S^a : x \to a^{-1}\, x\, a$ és bijectiva.
2. $(S^a)^b = S^{ab}$, $\forall a,b \in G$.
3. $S = S^1$.
4. Si S és un subgrup de G també ho és de S^a.
5. Si $S \subset T$ llavors $S^a \subset T$.

Veure la demostració en [3, pàg. 33].

Definició 2.15 Normalitzador Si S és un subconjunt no buit de G, s'anomena normalitzador de S en G al conjunt

$$N(S) = \{a \in G : S^a = S\} = \{a \in G : a^{-1}\, S\, a = S\} \tag{2.13}$$

Teorema 2.15 $N(S)$ és un subgrup de G.

Demostració. (esbos) Clarament $S^1 = S$ i es pot provar fàcilment que $S^{a\,b^{-1}} = S, \forall a,b \in N(S)$. □

Veure la demostració en [3, pàg. 34].

Teorema 2.16 Si $\{H_i\}$ és una família de subgrups de G, llavors

$$H = \bigcap_i H_i$$

és un subgrup de G. A més, per $a \in G$

$$H^a = \bigcap_i H_i^a.$$

Veure la demostració en [3, pàg. 34].

Definició 2.16 Producte de subgrups.(*internal direct product*) Donats dos subgrups $H,K \subset G$, es defineix:

$$H\,K = \{h\,k : h \in H, k \in K\} \tag{2.14}$$

Notar que $H \subset H\,K$ i $K \subset H\,K$.

Teorema 2.17 $H\,K$ és un subgrup de G sii $H\,K = K\,H$. Veure la demostració en [3, pàg. 34].

2.3 Grup dièdric, D_n

D_n es defineix com el grup de simetries d'un polígon regular d'n vèrtexs $X = \{a_i,\ i = 1,\cdots n\}$. Aquestes es poden obtenir amb (1) n rotacions d'angle $i\frac{2\pi}{n}$, $i = 0,1,\cdots,n-1$ en sentit de les agulles del rellotge, i (2) n reflexions al voltant dels eixos de simetria d'angles $i\frac{2\pi}{n}$, $i = 0,1,\cdots,n-1$, que anomenarem s_i, $i = 1,2,\cdots,n$. Veure la figura 2.1 per D_3.

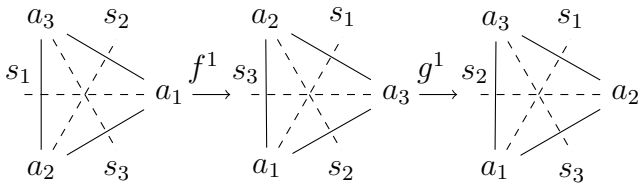


Figura 2.1: Operació $\mathrm{g}^3 = \mathrm{f}^1\,\mathrm{g}^1$ en D_3.

Alternativament es pot definir el grup dièdric com la bijecció $h : X \to X$ tal que $\mathrm{dist}(a,b) = \mathrm{dist}(h(a),h(b))$, $\forall a,b \in X$, on X és el conjunt dels vèrtexs del polígon. És a dir, la bijecció que conserva la distància entre els vèrtexs (això és, rotacions i reflexions).

Fent servir la notació de [3] denotarem les rotacions per el conjunt $\{\mathrm{f}^0, \mathrm{f}^1, \cdots \mathrm{f}^{n-1}\}$, on f^i representa una rotació de $i\frac{2\pi}{n}$, $i = 0,1,\cdots,n-1$ en el sentit de les agulles del rellotge. Les reflexions al voltant dels eixos de simetria s_i, $i = 1,2,\cdots,n$ les denotarem per $\{\mathrm{g}^1, \mathrm{g}^2, \cdots \mathrm{g}^n\}$. veure la figura 2.1. Seguint la notació de [3] denotarem $\mathrm{g} = \mathrm{g}^1$, és a dir, denotarem per g la reflexió al voltant de l'eix de simetria que uneix el centre del polígon amb un dels vèrtexs.

Per exemple, per un triangle equilàter, D_3, hi ha les rotacions $\{\mathrm{f}^0, \mathrm{f}^1, \mathrm{f}^2\}$ i reflexions $\{\mathrm{g}^1, \mathrm{g}^2, \mathrm{g}^3\}$ al voltant dels eixos de simetria s_1, s_2, s_3. Veure la figura 2.1.

Definició 2.17 La **taula de Cayley** 2.1 (o **taula de multiplicació**) mostra les possibles operacions que resulten de les composicions de les bijeccions $h_i\,h_j$, que hi ha en la fila i, columna j. En el proper capítol 3, pàg. 8, es veurà en més detall la composició de bijeccions. Per D_3 es pot comprovar que la taula és tancada amb element neutre $e = \mathrm{f}^0$. Veure la taula 2.1.

	f^0	f^1	f^2	g^1	g^2	g^3
f^0	f^0	f^1	f^2	g^1	g^2	g^3
f^1	f^1	f^2	f^0	g^3	g^1	g^2
f^2	f^2	f^0	f^1	g^2	g^3	g^1
g^1	g^1	g^3	g^2	f^0	f^1	f^2
g^2	g^2	g^1	g^3	f^2	f^0	f^1
g^3	g^3	g^2	g^1	f^1	f^2	f^0

Taula 2.1: Taula de Cayley de D_3.

En general, un grup D_n compleix $\mathrm{f}^i\,\mathrm{f}^j = \mathrm{f}^{i+j}$ en aritmètica mòdul n, i les n reflexions es poden obtenir amb les composicions $\{\mathrm{g}\,\mathrm{f}^0, \mathrm{g}\,\mathrm{f}^1, \cdots \mathrm{g}\,\mathrm{f}^{n-1}\}$. Notar que $\mathrm{g}\,\mathrm{f}^i \neq \mathrm{g}\,\mathrm{f}^j$, per $i \neq j$, $i,j \in \{0,1,\cdots,n-1\}$. Altrament implicaria que $\mathrm{f}^i = \mathrm{f}^j$, $i \neq j$, $i,j \in \{0,1,\cdots,n-1\}$ que no és possible.

Es conclou que un grup dièdric D_n està format per $2\,n$ elements:

$$D_n = \{e, \mathrm{f}^1, \mathrm{f}^2, \cdots \mathrm{f}^{n-1}, \mathrm{g}, \mathrm{g}\,\mathrm{f}^1, \cdots \mathrm{g}\,\mathrm{f}^{n-1}\} \qquad (2.15)$$

on $e = \mathrm{f}^0$. Notar també que D^n no és abelià per $n \geq 3$. Per exemple, de la taula 2.1 tenim $\mathrm{g}^1\,\mathrm{g}^2 = \mathrm{f}^1$ i $\mathrm{g}^2\,\mathrm{g}^1 = \mathrm{f}^2$.

2.4 Producte directe de grups

Definició 2.18 Producte directe de grups (*External Direct Product*): Siguin els grups $G_1, G_2, \cdots G_n$ es defineix el grup denotat per $G_1 \times G_2 \times \cdots G_n$ al conjunt de totes les n-tuples $(g_1, g_2, \cdots g_n)$ on $g_i \in G_i$ i el producte de tuples $(g_1, g_2, \cdots g_n)\,(g'_1, g'_2, \cdots g'_n) = (g_1\,g'_1, g_2\,g'_2, \cdots g_n\,g'_n)$, on el producte $g_i\,g'_i$ és el corresponent al grup G_i.

Teorema 2.18 L'ordre s'un element del producte directe de grups és el mínim comú múltiple dels ordres de les components de l'element:

$$\mathrm{o}((g_1, g_2, \cdots g_n)) = \mathrm{lcm}(\mathrm{o}(g_1), \mathrm{o}(g_2), \cdots \mathrm{o}(g_n)) \qquad (2.16)$$

Demostració. Sigui $s = \mathrm{lcm}(\mathrm{o}(g_1), \mathrm{o}(g_2), \cdots \mathrm{o}(g_n))$, llavors, fent servir el teorema 2.7 tenim:

$$(g_1, g_2, \cdots g_n)^s = (g_1^s, g_2^s, \cdots g_n^s) = (e_1, e_2, \cdots e_n)$$

a més, si $(g_1^t, g_2^t, \cdots g_n^t) = (e_1, e_2, \cdots e_n)$, llavors per 2.7 tenim que t ha de ser un múltiple de $\mathrm{o}(g_i)$, per tant, $s \leq t$. □

Teorema 2.19 Siguin G_1 i G_2 dos grups cíclics finits. Llavors $G_1 \times G_2$ és cíclic sii $\mathrm{o}(G_1)$ i $\mathrm{o}(G_2)$ són primers relatius.

Demostració. Sigui $\mathrm{o}(G_1) = m$ i $\mathrm{o}(G_2) = n$. Llavors $\mathrm{o}(G_1 \times G_2) = m\,n$. Per la primera part hem de demostrar que si $G_1 \times G_2$ és cíclic, llavors $\gcd(m,n) = 1$. Suposem que $\gcd(m,n) = d$ i que (g_1, g_2) és un generador de $G_1 \times G_2$. Això implica $(g_1, g_2)^{m\,n/d} = ((g_1^m)^{n/d}, (g_2^n)^{m/d}) = (e, e)$. Per tant $\mathrm{o}(G_1 \times G_2) = m\,n = \mathrm{o}((g_1, g_2)) \leq m\,n/d \Rightarrow d = 1$.

Per la segona part hem de demostrar que si $\gcd(m,n) = 1$, llavors $G_1 \times G_2$ és cíclic. Suposem $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, amb $\gcd(m,n) = 1$. Llavors $\mathrm{o}(G_1 \times G_2) = \mathrm{o}((g_1, g_2)) = \mathrm{lcm}(m,n) = m\,n$. Per tant (g_1, g_2) és un generador de $G_1 \times G_2$. □

Capítol 3
Grups permutatius

Nota: Per a més detalls i demostració dels teoremes veure [2, capítol 5, pàg. 95].

Definició 3.1 Grup permutatiu: És un conjunt de bijeccions d'elements d'un conjunt A en ell mateix, que forma un grup amb l'operació binària composició de funcions. Normalment es considera un conjunt A finit.

Els elements d'un grup permutatiu es representen en forma d'array i s'anomenen **permutacions**. Per exemple, dues permutacions α i β són:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix}$$

On $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\cdots$ i anàlogament per β. La composició de permutacions és:

$$\alpha\,\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

doncs $(\alpha\,\beta)(1) = \alpha(\beta(1)) = 4$, etc.

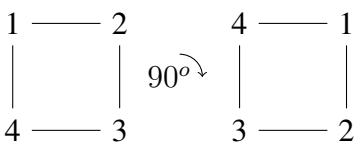
L'element neutre d'un grup permutatiu és la permutació que no canvia cap element, per exemple:

$$e = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

Es pot comprovar fàcilment que per a qualssevol permutació α: $\alpha\,e = e\,\alpha = \alpha$.

Definició 3.2 Grup simètric de grau n, S_n: És el grup format per totes les permutacions de $A = \begin{Bmatrix} 1 & 2 & \cdots & n \end{Bmatrix}$. S_n té $n!$ elements, i es pot provar que per $n \geq 3$ no és Abelià.

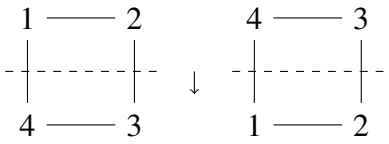
Exemple 3.1 (D_4 és un subgrup de S_4)
En un grup dièdric D_4 podem descriure una rotació de 90^o en sentit de les agulles del rellotge:



amb la permutació:

$$\mathrm{f} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

i la reflexió al voltant de l'eix horitzontal:



amb la permutació:

$$\mathrm{g} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

Els elements f i g generen tot el grup D_4 (tal com es va obtenir en la secció 2.3, pàg. 7). És a dir, qualsevol element de D_4 es pot obtenir d'alguna combinació de f i g. Per exemple, una rotació de 180^o és f^2 (composició de f amb ell mateix). De fet, aplicant (2.15) tenim:

$$D_4 = \{e, \mathrm{f}^1, \mathrm{f}^2, \mathrm{f}^3, \mathrm{g}, \mathrm{g}\,\mathrm{f}^1, \mathrm{g}\,\mathrm{f}^2, \mathrm{g}\,\mathrm{f}^3\}$$

Per tant, D_4 és un subgrup de S_4.

3.1 Notació per cicles (*cycle notation*)

Consisteix en especificar la permutació per els *cicles* que van d'un element a ell mateix. Per exemple:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{bmatrix}$$

s'identificaria per: $\alpha = (1,2,3)(4)(5,6)$, doncs hi ha els cicles $1 \to 2 \to 3 \to 1$, $4 \to 4$ i $5 \to 6 \to 5$. Notar que l'últim element del cicle (que és igual al primer) no es posa en la seqüència. Un altre exemple:

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 1 & 5 \end{bmatrix} = (1,3,6,5)(2,4)$$

Cada expressió de la forma $(a_1,a_2,\cdots,a_n)$ s'anomena cicle de longitud n.

Cada cicle es pot interpretar com una permutació on els elements que no hi ha en el cicle no canvien (equivalent a no afegir els cicles d'un sol element). Per exemple:

$$(1,2,3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{bmatrix}$$

La **multiplicació de cicles** s'interpreta com la permutació que resulta de la composició de les permutacions:

$$(1,2,3)(2,3,5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 3 & 6 \end{bmatrix} = (1,2)(3,5)$$

La composició es pot fer directament tenint en compte les relacions del cicle, i que els elements que no hi ha en el cicle no canvien. Hem de repetir aquestes regles rotant de dreta a esquerra (composició de funcions) fins que es produeix un cicle. Per exemple:

$$(1,3)(3,4,6)(5,3,2) = (1,3,2,5,4,6)$$

doncs l'1 és fix en el tercer factor i el segon, i passa a 3 en el primer. Després el 3 passa a 2 en el primer factor, que és fix en el segon i tercer, i així successivament:

$$\begin{aligned} &1 \to 1 \to 3 \\ &3 \to 2 \to 2 \to 2 \\ &2 \to 5 \to 5 \to 5, \\ &5 \to 3 \to 4 \to 4 \\ &4 \to 4 \to 6 \to 6 \\ &6 \to 6 \to 3 \to 1 \Rightarrow \\ &(1,3,2,5,4,6) \end{aligned}$$

Teorema 3.1 Un cicle de longitud n té ordre n.
Es pot comprovar fàcilment, doncs al rotar n elements, s'obté el mateix element del cicle. Per exemple:

$$(2,4,5)^3 = (2,4,5)(2,4,5)(2,4,5) = (2)(4)(5) = e$$

Teorema 3.2 Tota permutació es pot escriure com el producte de cicles disjunts (amb elements diferents).

Teorema 3.3 Si els cicles α i β són disjunts, aleshores $\alpha\,\beta = \beta\,\alpha$.

Teorema 3.4 L'ordre d'una permutació expressada en cicles disjunts és el mínim comú múltiple de les longituds dels cicles.
Per exemple, considerem S_4, que té $4! = 24$ permutacions. Denotem $(\underline{n})$ un cicle de longitud n. Els possibles cicles disjunts de les permutacions de S_4 tenen longituds:

$$\begin{aligned} &(\underline{4}) \\ &(\underline{3})(\underline{1}) \\ &(\underline{2})(\underline{2}) \\ &(\underline{2})(\underline{1})(\underline{1}) \\ &(\underline{1})(\underline{1})(\underline{1})(\underline{1}) \end{aligned}$$

amb mínims comuns múltiples: $4,3,2,2,1$. Per tant, els ordres de les 24 permutacions de S_4 són $4,3,2,1$.

Teorema 3.5 Qualsevol permutació de S_n, $n > 1$ es pot expressar com el producte de cicles de longitud 2 (*2-cycles*), possiblement no disjunts.
És fàcil de provar, doncs tota permutació es pot expressar com el producte de cicles disjunts, però:

$$(a_1,a_2,\cdots,a_i)\cdots(b_1,b_2,\cdots,b_j) = (a_1,a_i)\cdots(a_1,a_2)\cdots(b_1,b_j)\cdots(b_1,b_2)$$

Per exemple:

$$(1,2,3)(4,5) = (1,3)(1,2)(4,5)$$

Teorema 3.6 El caràcter parell o senar de l'expressió com un producte de *2-cycles* d'una permutació és únic. És a dir, hi pot haver múltiples expressions en productes de *2-cycles* d'una permutació, però totes seran parelles o senars. Això motiva la classificació de les permutacions en *parelles* o *senars*, segons es puguin expressar com el producte d'un nombre parell o senar de *2-cycles*.

Per determinar si una permutació és parella o senar, hi ha una marera més senzilla que fer la descomposició en *2-cycles* (veure [1, pàg. 60]). Donada una seqüència ordenada d'enters, es diu que el **nombre d'inversions** de la seqüència és el nombre d'enters inferiors al primer enter de la seqüència. Per exemple, el nombre d'inversions de $3,2,4,1$ és 2, i escrivim $I(3,2,4,1) = 2$, perquè els elements 2 i 1 són inferiors a 3. Per determinar si una permutació

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$$

és parella o senar, basta calcular si ho són el nombre d'inversions de la permutació:

$$I_\alpha = I(i_1,i_2,\cdots,i_n)+I(i_2,\cdots,i_n)+\cdots+I(i_{n-1},i_n)$$

Per exemple, el nombre d'inversions de la permutació:

$$\alpha = (1,2,3)(4,5) = (1,3)(1,2)(4,5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$$

és $I_\alpha = I(2,3,1,5,4) + I(3,1,5,4) + I(1,5,4) + I(5,4) = 1+1+0+1 = 3$. Per tant, α és una permutació senar.

Teorema 3.7 El conjunt de les permutacions parelles de S_n forma un subgrup de S_n. Notar que no passa el mateix amb les senars, doncs es pot comprovar que la permutació identitat és parella.

Definició 3.3 El subgrup de les permutacions parelles de S_n té el nom de **Grup altern de grau n, A_n**. Com que S_n té $n!$ permutacions, de les quals la meitat són parelles, A_n té ordre $n!/2$.

Exemple 3.2 (permutacions de A_4)
Les permutacions de S_4 que comencen per 1 són:

permutació	Inv.	signe	notació	ordre
1 2 3 4	0	+	e	1
1 2 4 3	1	−	(3,4)	2
1 4 2 3	2	+	(2,4,3)	3
1 4 3 2	3	−	(2,4)	2
1 3 4 2	2	+	(2,3,4)	3
1 3 2 4	1	−	(2,3)	2

Taula 3.1: Permutacions de S_4 que comencen per 1

Intercanviant $1 \leftrightarrow 2$, $1 \leftrightarrow 3$ i $1 \leftrightarrow 4$ s'obtenen les 18 permutacions que falten de S_4.

De la taula 3.1 tenim que les Permutacions de A_4 que comencen per 1 són:

permutació	Inv.	signe	notació	ordre
1 2 3 4	0	+	e	1
1 4 2 3	2	+	$\tau_2 = (2,4,3)$	3
1 3 4 2	2	+	$\tau_1 = (2,3,4)$	3

Taula 3.2: Permutacions d'A_4 que comencen per 1

Intercanviant $1 \leftrightarrow 2$, $1 \leftrightarrow 3$ i $1 \leftrightarrow 4$ en les permutacions senars de la taula 3.1 s'obtenen les 9 permutacions que falten d'A_4 (agafem les senars perquè al fer l'intercanvi canvia el signe de la permutació):

permutació	Inv.	signe	notació	ordre
2 1 4 3	2	+	$\sigma_8 = (1,2)(3,4)$	2
2 4 3 1	4	+	$\tau_5 = (1,2,4)$	3
2 3 1 4	2	+	$\tau_7 = (1,2,3)$	3
3 2 4 1	4	+	$\tau_3 = (1,3,4)$	3
3 4 1 2	4	+	$\sigma_2 = (1,3)(2,4)$	2
3 1 2 4	2	+	$\tau_8 = (1,3,2)$	3
4 2 1 3	4	+	$\tau_4 = (1,4,3)$	3
4 1 3 2	4	+	$\tau_6 = (1,4,2)$	3
4 3 2 1	6	+	$\sigma_5 = (1,4)(2,3)$	2

Taula 3.3: Permutacions d'A_4 que comencen per 2,3,4

En les taules 3.2 i 3.3 s'ha fet servir la mateixa notació que en [1, prob. 5.1, pàg. 131]. Notar que σ_i són permutacions d'ordre 2 i les τ_i són d'ordre 3.

Capítol 4
Teorema de Lagrange

4.1 Classe lateral (coset)

Si G és un grup, H és un subgrup de G, i a és un element de G, llavors els conjunts

$$a\,H = \{a\,h : h \in H\} \tag{4.1}$$
$$H\,a = \{h\,a : h \in H\} \tag{4.2}$$

s'anomenen respectivament classe lateral per l'esquerra i per la dreta (classe esquerra o dreta, per abreujar) de H en G que contenen a (*left and right coset of H in G containing a*).

NOTA: en un grup amb l'operació addició, les classes laterals seran $a + H$ i $H + a$.

Exemple 4.1 (Classes laterals) Sabem que $H = \{0, 4\}$ és un subgrup de $\mathbb{Z}_8 = \{0,1,\cdots 7\}$ (veure l'exemple 2.6, pàg. 5). Les classes laterals generades per H són:

$$\begin{aligned}
0 + H &= \{0, 4\}\\
1 + H &= \{1, 5\}\\
2 + H &= \{2, 6\}\\
3 + H &= \{3, 7\}\\
4 + H &= \{4, 0\} = H\\
5 + H &= \{5, 1\} = 1 + H\\
6 + H &= \{6, 2\} = 2 + H\\
7 + H &= \{7, 3\} = 3 + H
\end{aligned}$$

Definició 4.1 Sigui el grup G i el subgrup H de G. Definim les relacions R^H i R_H (veure [3, pàg. 40]):

$$a\,R^H\,b \text{ si } a^{-1}\,b \in H \tag{4.3}$$
$$a\,R_H\,b \text{ si } a\,b^{-1} \in H \tag{4.4}$$

Exemple 4.2 (classes laterals en C_4)
Donat el subgrup $H = \{e, a^2\}$ de $C_4 = \langle a\rangle$, trobar les classes laterals per la dreta de H en C_4 (grup cíclic d'ordre 4).

$$\begin{aligned}
H\,e &= H = \{e, a^2\}\\
H\,a &= \{a, a^3\}\\
H\,a^2 &= \{a^2, a^4\} = \{a^2, e\} = H\\
H\,a^3 &= \{a^3, a^5\} = \{a^3, a\} = H\,a
\end{aligned}$$

Es pot veure que l'ordre de totes les classes laterals és el mateix, hi ha 2 classes laterals diferents disjuntes i la unió de totes les classes laterals és el grup C_4.

Exemple 4.3 (classes laterals en S_3)
Donat el subgrup $H = \{e, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\}$ de S_3, trobar les classes laterals per la dreta d'H en S_3 (grup simètric de 3 elements). $\mathrm{o}(S_3) = 3! = 6$. Els 6 elements d'S_3 són:

$$\begin{aligned}
e &= \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\\
s_1 &= \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = (2,3)\\
s_2 &= \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = (1,2)\\
s_3 &= \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = (1,3,2)\\
s_4 &= \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = (1,2,3)\\
s_5 &= \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = (1,3)
\end{aligned}$$

Es pot veure que hi ha 3 elements d'ordre 2 (s_1, s_2, s_5) i 2 d'ordre 3 (s_3, s_4). Amb la notació anterior tenim que $H = \{e, s_2\}$. A més:

$$\begin{aligned}
s_2\,s_1 &= (1,2)\,(2,3) = (2,3,1) = (1,2,3) = s_4\\
s_2\,s_2 &= (1,2)\,(1,2) = e\\
s_2\,s_3 &= (1,2)\,(1,3,2) = (1,3) = s_5\\
s_2\,s_4 &= (1,2)\,(1,2,3) = (2,3) = s_1\\
s_2\,s_5 &= (1,2)\,(1,3) = (1,3,2) = s_3
\end{aligned}$$

Per tant, les classes laterals per la dreta són:

$$\begin{aligned}
H\,e &= H\\
H\,s_1 &= \{s_1, s_4\}\\
H\,s_2 &= \{s_2, e\} = H\\
H\,s_3 &= \{s_3, s_5\}\\
H\,s_4 &= \{s_4, s_1\} = H\,s_1\\
H\,s_5 &= \{s_5, s_3\} = H\,s_3
\end{aligned}$$

És a dir, 3 classes laterals diferents d'ordre 2.

Teorema 4.1 R^H i R_H són relacions d'equivalència en el conjunt G. Veure la definició de relació d'equivalència 1.1, pàg. 1.

Demostració. Per R_H (per R^H és anàleg):
1. Per $a \in G$ es té $a\,a^{-1} = e \in H$ (perquè H és subgrup), per tant: $a\,R_H\,a$ (propietat reflexiva).

2. Si $a\,R_H\,b$, $a\,b^{-1} \in H$, llavors $(a\,b^{-1})^{-1} = b\,a^{-1} \in H$, per tant, $b\,R_H\,a$ (propietat de simetria).
3. Si $a\,R_H\,b$ i $b\,R_H\,c$ es té: $a\,b^{-1} \in H$ i $b\,c^{-1} \in H$. Així doncs $(a\,b^{-1})\,(b\,c^{-1}) = a\,c^{-1} \in H$ i, per tant, $a\,R_H\,c$ (propietat transitiva). □

Al ser R^H i R_H relacions d'equivalència en G, generen els conjunts quocients G/R^H i G/R_H. Veure la definició de conjunts quocients 1.11, pàg. 3. Les classes laterals $a\,H$ i $H\,a$ són classes de l'element a generades per les relacions d'equivalència R^H i R_H, respectivament. Veure la def. 1.10, pàg. 2 de classe generada per una relació d'equivalència. És a dir:

$$a\,H = \{a\,h : h \in H\} = \{b \ : \ a\,R^H\,b, \forall b \in G\} \quad (4.5)$$
$$H\,a = \{h\,a : h \in H\} = \{b \ : \ b\,R_H\,a, \forall b \in G\} \quad (4.6)$$

doncs $a\,R^H\,b \Rightarrow a^{-1}\,b = h \in H \Rightarrow b = a\,h \in a\,H$ i $b\,R_H\,a \Rightarrow b\,a^{-1} = h \in H \Rightarrow b = h\,a \in H\,a$.

Teorema 4.2 L'aplicació entre els conjunts quocients

$$G/R_H \to G/R^H : H\,a \to a^{-1}\,H \quad (4.7)$$

és bijectiva.

Demostració. Hem de provar que si $H\,x = H\,y$ haurà de ser $x^{-1}\,H = y^{-1}\,H$. Però si $H\,x = H\,y$ es té $x\,R_H\,y$ Veure el teorema 1.1, pàg. 2. Per tant: $x\,y^{-1} \in H \Rightarrow (x^{-1})^{-1}\,y^{-1} \in H \Rightarrow x^{-1}\,R^H\,y^{-1} \Rightarrow x^{-1}\,H = y^{-1}\,H$. Anàlogament es demostra que si $H\,x \neq H\,y$ llavors $x^{-1}\,H \neq y^{-1}\,H$, que prova la injectivitat. Com que cada element $y\,H$ de G/R^H és la imatge de $H\,y^{-1}$, l'aplicació també és surjectiva. □

Propietats 4.1 De les classes laterals. Si G és un grup, H és un subgrup de G, i a,$b \in G$, llavors

1. $a \in a\,H$.
2. $a\,H = H$ sii $a \in H$ (H *absorbeix* a).
3. $a\,H = b\,H$ sii $a \in b\,H$.
4. $a\,H = b\,H$ sinó és $a\,H \cap b\,H = \emptyset$.
5. $a\,H = b\,H$ sii $a^{-1}\,b \in H$.
6. $\mathrm{o}(a\,H) = \mathrm{o}(b\,H)$.
7. $a\,H = H\,a$ sii $H = a\,H\,a^{-1}$.
8. $a\,H$ és un subgrup de G sii $a \in H$. Això és demostra fàcilment, doncs si H és subgrup ha de tenir e, per tant, de les propietats 2 i 4 $a\,H = e\,H = H$. Notar que aquesta propietat implica que H és l'única classe lateral per l'esquerra de H que conté a que és subgrup de G.

Veure la demostració en [2, pàg. 139].

Les propietats anteriors són anàlogues per a classe lateral per la dreta. Les propietats 1, 4 i 6 impliquen que les classes per l'esquerra d'un subgrup H de G particionen G en subconjunts d'igual mida. Per tant, podem veure les classes per l'esquerra de H com una partició de G en **classes d'equivalència** sota la relació d'equivalència $a\,R^H\,b$ si $a\,H = b\,H$ ($a\,R_H\,b$ si $H\,a = H\,b$ en les classes per la dreta) . De fet, sovint el subgrup H es tria de forma que les classes generades particionen G en alguna forma desitjada.

4.2 Teorema de Lagrange

Teorema 4.3 (Lagrange)
Si G és un grup finit i H és un subgrup de G, llavors $\mathrm{o}(H)$ divideix $\mathrm{o}(G)$. A més, el nombre de classes laterals per l'esquerra (o la dreta) de H en G és $\mathrm{o}(G)/\mathrm{o}(H)$.

Demostració. Siguin $a_i\,H$, $i = 1, \cdots, r$ les r classes per l'esquerra diferents que té H en G. Donat que per algun i: $\forall a \in G$, $a \in a\,H = a_i\,H$ tenim que $G = \cup_{i=1}^{r} a_i\,H$, per tant, $\mathrm{o}(G) = \sum_{i=1}^{r} \mathrm{o}(a_i\,H) = r\,\mathrm{o}(H)$. □

Exemple 4.4 (teorema de Lagrange) $\mathbb{Z}_8$ té 4 subgrups, els subgrups impropis $\{0\}$ i $\{0,1,\cdots 7\}$, i els subgrups propis $\{0,4\}$ i $\{0,2,4,6\}$ (veure l'exemple 2.6, pàg. 5). Podem comprovar que l'ordre dels subgrups: $1, 8, 2, 4$, divideix $\mathrm{o}(\mathbb{Z}_8) = 8$. El nombre de classes laterals de $\{0,4\}$ en $\mathbb{Z}_8$ és $\mathrm{o}(\mathbb{Z}_8)/\mathrm{o}(\{0,4\}) = 8/2 = 4$, tal com s'ha obtingut en l'exemple 4.1, pàg. 11.

Definició 4.2 Índex d'un subgrup H en G, $[G : H]$
És el nombre de classes laterals per l'esquerra d'H en G. Es fa servir la notació $[G\,{:}\,H]$. Amb aquesta notació el teorema de Lagrange es pot enunciar dient que $\mathrm{o}(H)$ divideix $\mathrm{o}(G)$ amb índex $[G\,{:}\,H] = \mathrm{o}(G)/\mathrm{o}(H)$.

Exemple 4.5 (índex en C_4)
En l'exemple 4.2, pàg. 11 tenim $H = \{e, a^2\}$ subgrup de C_4, $\mathrm{o}(H) = 2$. H genera 2 classes laterals diferents de C_4. Com que $\mathrm{o}(C_4) = 4$, comprovem que l'ordre d'H divideix $\mathrm{o}(C_4)$, i que el nombre de classes laterals és $[C_4\,{:}\,H] = \mathrm{o}(C_4)/\mathrm{o}(H) = 2$.

Exemple 4.6 (índex en S_3)
En l'exemple 4.3, pàg. 11 tenim $H = \{e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$ subgrup de S_3, $\mathrm{o}(H) = 2$. H genera 3 classes laterals diferents d'S_3. Com que $\mathrm{o}(S_3) = 6$, comprovem que l'ordre d'H divideix $\mathrm{o}(S_3)$, i que el nombre de classes laterals és $[S_3\,{:}\,H] = \mathrm{o}(S_3)/\mathrm{o}(H) = 3$.

Exemple 4.7 (subgrups propis d'A_4)
[1, Prob. 5.1, pàg. 131] o [3, Prop. 2.10, pàg. 92]. Trobar tots els subgrups propis del grup A_4.

Solució Per el teorema de Lagrange, els subgrups propis han de ser d'ordre 2, 3, 4, 6, doncs han de dividir $\mathrm{o}(A_4) = 4!/2 = 12$.

En les taules 3.2 i 3.3, pàg. 10 hi ha les permutacions d'A_4. N'hi ha 3 d'ordre 2 (σ_2, σ_5, σ_8). Per tant, deduïm que els **subgrups d'ordre 2** són: $\{e, \sigma_2\}$, $\{e, \sigma_5\}$ i $\{e, \sigma_8\}$.

Podem comprovar que per a les permutacions d'ordre 3:

$$\begin{aligned}
\tau_1^2 &= (2,3,4)(2,3,4) = (2,4,3) = \tau_2 \\
\tau_2^2 &= (2,4,3)(2,4,3) = (2,3,4) = \tau_1 \\
\tau_3^2 &= (1,3,4)(1,3,4) = (1,4,3) = \tau_4 \\
\tau_4^2 &= (1,4,3)(1,4,3) = (1,3,4) = \tau_3 \\
\tau_5^2 &= (1,2,4)(1,2,4) = (1,4,2) = \tau_6 \\
\tau_6^2 &= (1,4,2)(1,4,2) = (1,2,4) = \tau_5 \\
\tau_7^2 &= (1,2,3)(1,2,3) = (1,3,2) = \tau_8 \\
\tau_8^2 &= (1,3,2)(1,3,2) = (1,2,3) = \tau_7
\end{aligned}$$

D'on deduïm que hi ha els **subgrups d'ordre 3**: $\{e, \tau_1, \tau_2\}$, $\{e, \tau_3, \tau_4\}$, $\{e, \tau_5, \tau_6\}$, $\{e, \tau_7, \tau_8\}$.

Es pot comprovar que els productes de permutacions d'ordre 2 també són permutacions d'ordre 2, per exemple: $\sigma_2\,\sigma_5 = (1,3)(2,4)(1,4)(2,3) = (1,2)(3,4) = \sigma_8$. Per tant, hi ha el **subgrup d'ordre 4** $\{e, \sigma_2, \sigma_5, \sigma_8\}$.

Al intentar barrejar permutacions d'ordre 2 i 3 s'acaba obtenint A_4 perquè el subgrup sigui tancat. Per exemple: $\tau_1\,\sigma_2 = (2,3,4)(1,3)(2,4) = (1,3)(2,4) = \sigma_2$, però $\sigma_2\,\tau_1 = (1,3)(2,4)(2,3,4) = (1,3,2) = \tau_8$, etc.

Per tant, ja no hi ha més subgrups d'ordre 4 i tampoc n'hi ha cap d'ordre 6. En el capítol 8, pàg. 20, exemple 8.1, es faran servir els teoremes de Sylow per tenir més informació sobre els subgrups d'A_4.

Exemple 4.8 (índex de $[\mathbb{Z}:m\,\mathbb{Z}]$)
[3, exemple 1.12.5, pàg. 41] El subgrup $H = m\,\mathbb{Z}$ del grup additiu d'enters (veure el teorema 2.4) genera el conjunt quocient $\mathbb{Z}/R_H = \{H+0, H+1, \cdots H+(m-1)\}$. Per tant $[\mathbb{Z}:m\,\mathbb{Z}] = m$.

Corol·laris del teorema de Lagrange:

Corol·lari 4.1 Un grup d'ordre un nombre primer és cíclic.

Demostració. Suposar que $\mathrm{o}(G)$ és un nombre primer. Sigui $a \in G$, $a \neq e$. Llavors $\mathrm{o}(\langle a\rangle)$ divideix $\mathrm{o}(G)$ i $\mathrm{o}(\langle a\rangle) \neq 1$. Per tant, ha de ser $\mathrm{o}(\langle a\rangle) = \mathrm{o}(G)$. □

Corol·lari 4.2 En un grup finit l'ordre de cada element divideix l'ordre del grup.

Demostració. Notar que $\mathrm{o}(a)$ és també l'ordre del subgrup generat per el conjunt $S = \{a\}$. Veure 2.8. Si $n = \mathrm{o}(G)$, del teorema de Lagrange tenim que $n = d\,\mathrm{o}(a)$, $d \in \mathbb{N}$. □

Corol·lari 4.3 En un grup finit G: $\forall a \in G : a^{\mathrm{o}(G)} = e$.

Demostració. Segons el corol·lari 4.2 per algun enter d: $\mathrm{o}(G) = d\,\mathrm{o}(a)$, per tant: $a^{\mathrm{o}(G)} = a^{d\,\mathrm{o}(a)} = e^d = e$. □

Corol·lari 4.4 Si H i K són subgrups finits d'un grup G amb $\mathrm{o}(H) = m$, $\mathrm{o}(K) = n$, i $\gcd(m,n) = 1$, llavors $H \cap K = e$.

Demostració. $H \cap K = e$ és subgrup de H i K. Com que $\mathrm{o}(H \cap K)$ ha de dividir m i n, ha de ser $\mathrm{o}(H \cap K) = 1$. Per tant $H \cap K = e$. □

Corol·lari 4.5 Fórmula de transitivitat de l'índex. Si H i K són subgrups d'un grup G amb $H \subset K$: (1) H és subgrup de K; (2) Si $[G : H]$ és finit, llavors també ho és $[G : K]$ i

$$[G : H] = [G : K]\,[K : H] \tag{4.8}$$

Veure la demostració en [3, pàg. 43].

Corol·lari 4.6 Si H i K són subgrups d'un grup G d'ordre finit. Llavors:

$$\mathrm{card}(H\,K) = \frac{\mathrm{o}(H)\,\mathrm{o}(K)}{\mathrm{o}(H \cap K)} \tag{4.9}$$

Veure la demostració en [3, pàg. 44].

Corol·lari 4.7 Petit teorema de Fermat. Per a cada enter a i nombre primer p:

$$a^p \bmod p = a \bmod p.$$

Veure la demostració en [2, pàg. 143].

Capítol 5
Subgrup Normal

Definició 5.1 Subgrup Normal Si G és un grup i H és un subgrup de G, llavors es diu que H és un subgrup normal de G (i es posa $H \lhd G$) si

$$a\,H = H\,a, \forall a \in G \tag{5.1}$$

Notar que això vol dir que $\forall a \in G$ i $\forall h \in H$ existeixen h_1,$h_2 \in H$ tals que $a\,h = h_1\,a$ i $h\,a = a\,h_2$. També

equival a dir que les relacions d'equivalència $R^H = R_H$. Veure la definició en 4.1, pàg. 11. Doncs les classes laterals $a\,H$ i $H\,a$ són classes de l'element a generades per les relacions d'equivalència R^H i R_H, respectivament. Veure les (4.5) i (4.6). La relació (5.1) en general no es compleix. Aquells subgrups que compleixen (5.1), els subgrups normals, com es veurà a continuació, tenen una especial rellevància.

Teorema 5.1 La condició de normalitat equival a:
1. $H = H^a = a^{-1}\,H\,a,\ \forall a \in G$.
2. $a\,b \in H \Rightarrow b\,a \in H,\ \forall a,b \in G$. Notar però que en general $a\,b \neq b\,a$.

Demostració. (esbós, veure la demostració en [3, pàg. 61]).
1. Si H és normal de G, $\forall a \in G\ \exists h,h' \in H : a\,h = h'\,a$. Llavors $a\,h\,a^{-1} = h' \Rightarrow a\,H\,a^{-1} \subseteq H$. Contràriament, si $a\,H\,a^{-1} \subseteq H$ tenim $a\,H \subseteq H\,a$. Si posem $b = a^{-b}$ s'obté $H\,b \subseteq b\,H$. Per tant $a\,H = H\,a$.
2. $b\,a = a^{-1}\,(a\,b)\,a \in H^a = H$. □

Test de normalitat. Si G és un grup i H és un subgrup de G, llavors la condició del teorema 5.1:

$$H = H^a = a^{-1}\,H\,a,\ \forall a \in G \tag{5.2}$$

es pot fer servir per a determinar si H és un subgrup normal de G, llavors H és un subgrup normal de G.

Exemple 5.1 (subgrups normals de S_3)
Trobar tots els subgrups normals de S_3. En l'exemple 4.3, pàg. 11 s'ha trobat que S_3 té 3 classes laterals per la dreta d'ordre 2 i 2 classes d'ordre 3. Per distingir-les farem servir la notació τ i σ per les d'ordre 2 i 3, respectivament (igual que en l'exemple del Schaum [1, pàg. 57]. En particular:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$$

La taula de Cayley (veure la def. 2.17, pàg. 7) es pot calcular fàcilment, per exemple, $\tau_1\,\tau_2 = (2,3)\,(1,3) = (1,2,3) = \sigma_1$, i resulta la taula 5.1.

	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

Taula 5.1: Taula de Cayley de les permutacions del grup S_3.

Els subgrups $\{e\}$ i G són normals. La taula 5.1 mostra que tots els productes de permutacions d'ordre 2 donen una permutació d'ordre 3. Per tant, no hi pot haver grups normals que només tinguin permutacions d'ordre 2. De fet, es pot veure fàcilment que l'únic grup que té permutacions d'ordre 2 és G. Per exemple, si un subgrup normal H té τ_1, també haurà de tenir $\tau_2\,\tau_1\,\tau_2^{-1} = \sigma_2\,\tau_2 = \tau_3 \in H$. Per tant, $\tau_1\,\tau_3 = \sigma_2 \in H$, etc. i s'obté $H = G$.

Per altra banda, els productes de permutacions d'ordre 3 són tancades, p.e. $\sigma_1^2 = \sigma_2$. De fet, es comprova fàcilment que el subgrup $N = \{e, \sigma_1, \sigma_2\}$ és normal. Doncs, p.e. $\tau_1\,\sigma_1\,\tau_1^{-1} = \tau_2\,\tau_1 = \sigma_2 \in N$.

Nota: en l'exemple del Schaum [1, pàg. 57] la taula és la transposada de la taula 5.1. Això és degut a que en el llibre del Schaum es fa servir la notació contraria per a la composicions de funcions. Veure l'explicació de la notació en la def. 1.4, pàg. 2.

Propietats 5.1 Dels grups normals: (veure [2, pàg 179])
1. Tot subgrup d'un grup abelià és normal. El recíproc és fals, hi ha grups amb tots el subgrups normals que no són abelians. En aquest cas es diuen **hamiltonians**.
2. El centre d'un grup $Z(G)$ és normal. Tots els subgrups de $Z(G)$ també ho són.
3. El grup altern A_n és normal.
4. El subgrup de les rotacions del grup dièdric D_n és normal.
5. El subgrup de les matrius amb determinant 1 de $GL_n(\mathbb{R})$ (matrius reals amb determinant no nul) és normal. Aquest subgrup de $GL_n(\mathbb{R})$ s'anomena **grup especial lineal** i es denota per $SL_n(\mathbb{R})$.

Teorema 5.2 Si H és subgrup de G i $[G : H] = 2$, llavors H és normal. Veure la demostració en [3, pàg. 63].

Exemple 5.2 (subgrup normal d'índex 2)
Com s'ha vist en l'exemple 5.1 $N = \{e, \sigma_1, \sigma_2\}$ és un subgrup de S_3. Com que $\mathrm{o}(N) = 3$ i $\mathrm{o}(S_3) = 3! = 6$, tenim que $[S_3 : N] = 2$, i per el teorema 5.2 tenim que N és subgrup normal de S_3 (tal com es va veure en l'exemple 5.1).

Teorema 5.3 Sigui H un subgrup de G. Llavors:
1. H és subgrup de $N(H)$.
2. H és subgrup normal de $N(H)$.
3. Si K és subgrup de G, $H \subset K$ i H és subgrup normal de K, llavors $K \subset N(H)$.

Veure la demostració en [3, pàg. 66].

Definició 5.2 subgrups conjugats. Si H i K són subgrups de G i $\exists a \in G : K = H^a = a^{-1}\, H\, a$, es diu que K i H són **subgrups conjugats** (doncs també es compleix $\exists b \in G \;:\; H = K^b$). Veure la def. de subgrup conjugat en 2.10.

Teorema 5.4 Si $\mathcal{F}$ és la família de subgrups conjugats de H (diferents) i el normalitzador de H en G és $N = N(H)$ (veure la definició de normalitzador 2.15, pàg. 7), llavors l'aplicació

$$f : G/N \to \mathcal{F} : N\, a \to H^a \tag{5.3}$$

és bijectiva. En particular, si $[G : N]$ és finit, aleshores el nombre de conjugats diferents de H en G és $[G : N]$. Veure la demostració en [3, pàg. 67].

Teorema 5.5 Sigui N un subgrup normal de G i H, K subgrups de G tals que H és subgrup normal de K. Llavors $N\, H$ és subgrup normal de $N\, K$.

Definició 5.3 Un grup G que només té 2 grups normals $\{e\}$ i G es diu **Grup simple**. En particular, si $\mathrm{o}(G)$ és un nombre primer, llavors, per el teorema de Lagrange, només té dos subgrups: $\{e\}$ i G, doncs l'ordre dels subgrups ha de dividir $\mathrm{o}(G)$. Per tant, si $\mathrm{o}(G)$ és un nombre primer, G és simple.

Definició 5.4 Si H és subgrup de G, es diu **Cor** de G a:

$$\mathrm{K}(H) = \bigcap_{a \in G} H^a. \tag{5.4}$$

De (5.4) es té que $\mathrm{K}(H)$ és subgrup de G. A més és subgrup normal de G. Veure la demostració en [3, pàg. 69].

Teorema 5.6 Si $N \subset H$ és subgrup normal de G, llavors $N \subset \mathrm{K}(H)$.

Demostració. Per cada $a \in G$ es té $N = N^a \subset H^a$, per tant $N \subset \cap_{a \in G} H^a = \mathrm{K}(H)$. □

Teorema 5.7 (Poincaré)
Si G té un subgrup d'índex finit, llavors també té un subgrup normal d'índex finit. Veure la demostració en [3, pàg. 69].

Capítol 6
Grup quocient

Teorema 6.1 (Grup quocient (*factor group*))
Sigui G un grup i H **un subgrup normal** de G. Llavors el conjunt de les classes laterals (*cosets*) $G/H = G/R_H = G/R^H = \{a\, H : a \in G\} = \{H\, a : a \in G\}$ és un grup amb l'operació

$$G/H \times G/H \to G/H : (a\, H)\,(b\, H) = a\, b\, H, \tag{6.1}$$

on l'element neutre és $H = e\, H$, doncs $(e\, H)\,(e\, H) = e\, e\, H = e\, H = H$.

És a dir, donat un subgrup normal H, la partició generada per les classes laterals per l'esquerra i per la dreta és la mateixa i, a més, té estructura grup. Recordar que per el grup additiu dels enters $(\mathbb{Z},+)$ l'operació és la suma. És a dir l'operació del grup quocient és $G/H \times G/H \to G/H : (a + H)\,(b + H) = a + b + H$. Veure la demostració en [2, pàg. 180] o [3, pàg. 70].

Notar que els elements de G/H són del tipus $a\, H$, on $a \in G$. Per tant, l'ordre d'un element $a\, H$ de G/H és el mínim natural n tal que $(a\, H)^n = a^n\, H = H$. També, $\langle a\, H\rangle$ és un subgrup de G/H, i si hi ha un $a\, H \in G/H$ tal que $\mathrm{o}(a\, H) = \mathrm{o}(G/H)$, llavors G/H és cíclic.

Exemple 6.1 (grup quocient) En l'exemple 4.1, pàg. 11 hem calculat les classes laterals generades per el subgrup $H = \{0, 4\}$ de $\mathbb{Z}_8 = \{0,1,\cdots 7\}$. Tenim doncs que

$$\mathbb{Z}_8/H = \{\{0, 4\}, \{1, 5\}, \{2, 6\}, \{3, 7\}\}$$

on $e = \{0, 4\}$ i, per exemple,

$$\{0, 4\} + \{2, 6\} = (0 + \{0, 4\}) + (2 + \{0, 4\}) = 2 + \{0, 4\} = \{2, 6\}$$

Teorema 6.2 Un subgrup K de G és normal sii K/H és subgrup normal de G/H. Veure la demostració en [3, pàg. 72].

Teorema 6.3 Si G és cíclic i H és un subgrup normal de G, aleshores G/H també és cíclic.

Demostració. Si $G = \langle a\rangle$, llavors també $G/H = \langle a\, H\rangle$. □

Exemple 6.2 (grup quocient $\mathbb{Z}/m\,\mathbb{Z}$)
El subgrup normal $m\,\mathbb{Z}$ del grup additiu dels enters $\mathbb{Z}$ (és normal doncs $\mathbb{Z}$ és abelià), genera el grup quocient $\mathbb{Z}/m\,\mathbb{Z}$. Veure la definició de $m\,\mathbb{Z}$ en el teorema 2.4, pàg. 4:

$$\begin{aligned}\mathbb{Z}/m\,\mathbb{Z}\times\mathbb{Z}/m\,\mathbb{Z}\to\mathbb{Z}/m\,\mathbb{Z}:\\ (a+m\,\mathbb{Z})\,(b+m\,\mathbb{Z})\to a+b+m\,\mathbb{Z}=\\ \{0+m\,\mathbb{Z},1+m\,\mathbb{Z},\cdots(m-1)+m\,\mathbb{Z}\}=\\ \{\hat{0},\hat{1},\cdots\widehat{m-1}\}\end{aligned}\tag{6.2}$$

on s'ha fet servir la notació $\hat{a}=a+m\,\mathbb{Z}=\{a+m\,x:x\in\mathbb{Z}\}=\{\cdots,a-m\,2,a-m,a,a+m,a+m\,2,\cdots\}$. Notar que amb aquesta notació $\hat{a}\,\hat{b}=(a+m\,\mathbb{Z})\,(b+m\,\mathbb{Z})=a+b+m\,\mathbb{Z}=\widehat{a+b}$.

Notar que $\mathrm{o}(\mathbb{Z}/m\,\mathbb{Z})=m$ i que $\mathbb{Z}/m\,\mathbb{Z}=\langle 1+m\,\mathbb{Z}\rangle=\langle\hat{1}\rangle$ és cíclic, amb element neutre $\hat{0}=\{0+m\,\mathbb{Z}\}$, doncs $(\hat{1})^m=\hat{0}$.

Definició 6.1 Grup multiplicatiu dels enters mòdul n (*Multiplicative group of integers modulo n*). Veure [3, pàg. 73]. El conjunt

$$\mathbb{Z}_m^o=\{a+m\,\mathbb{Z}\in\mathbb{Z}/m\,\mathbb{Z}:\gcd(a,m)=1\}\tag{6.3}$$

amb operació

$$\begin{aligned}\mathbb{Z}_m^o\times\mathbb{Z}_m^o\to\mathbb{Z}_m^o:\\ (a+m\,\mathbb{Z})(b+m\,\mathbb{Z})\to a\,b+m\,\mathbb{Z}\end{aligned}\tag{6.4}$$

és un grup abelià amb ordre $\mathrm{o}(\mathbb{Z}_m^o)=\phi(m)$, on $\phi(m)$ és la funció ϕ d'Euler (veure l'apèndix C), i element neutre $\{1+m\,\mathbb{Z}\}$.

Per exemple, per $m=4$, com que els primers relatius amb 4 són 1,3, es té:

$$\mathbb{Z}_4^o=\{1+4\,\mathbb{Z},3+4\,\mathbb{Z}\}\tag{6.5}$$

Té 2 elements, per tant, és cíclic d'ordre 2. $\mathbb{Z}_m^o$, però, no sempre és cíclic. Veure l'exemple 7.7, pàg. 18.

Notar que en (6.4) es fa servir el producte $(a\,b+m\,\mathbb{Z})$, i no la suma $(a+b+m\,\mathbb{Z})$ com en el grup quocient (6.2) de l'exemple 6.2. Per evitar ambigüitats amb la notació de l'exemple 6.2 ara canviem la notació i definim: $\overline{a}=a+m\,\mathbb{Z}$. Ara $\overline{a}\,\overline{b}=(a+m\,\mathbb{Z})\,(b+m\,\mathbb{Z})=a\,b+m\,\mathbb{Z}=\overline{a\,b}$.

Demostració. Sigui $G=\mathbb{Z}_m^o$.

1. G és tancat: Per $a,b\in G$ tenim $\gcd(a,m)=\gcd(b,m)=1$. Per tant $\gcd(a\,b,m)=1\Rightarrow\overline{a\,b}\in G$.
2. Propietat associativa: $(\overline{a}\,\overline{b})\,\overline{c}=\overline{a\,b\,c}=\overline{a}\,(\overline{b}\,\overline{c})$.
3. Identitat: $\gcd(1,m)=1\in G$, $\overline{1}\,\overline{a}=\overline{a}=\overline{a}\,\overline{1}$.
4. Inversa: Si $\gcd(a,n)=1\Rightarrow\exists s,t:a\,s+n\,t=1$ (veure el teorema 13.9, pàg. 38). Com que $a\,s+n\,t=1\Rightarrow\overline{a\,s}+\overline{n\,t}=\overline{1}$ i $\overline{n\,t}=\overline{0}$, tenim $\overline{a\,s}=\overline{a}\,\overline{s}=\overline{1}\in G$ i es conclou que $a^{-1}=s$. □

Capítol 7
Morfismes

Definició 7.1 Grups homomòrfics (del grec *homo*, "semblant" i *morfic*, "forma"). Un homomorfisme $f:G\to G'$ és una operació (funció) que preserva l'operació del grup:

$$f(a\,b)=f(a)\,f(b),\forall a\,b\in G\tag{7.1}$$

Definició 7.2 Es diu **nucli (*kernel*)** d'un homomorfisme f d'un grup G a

$$\ker f=\{a\in G:f(a)=e'\}\tag{7.2}$$

on e' és l'element identitat de G'. Notar que $f(e)=e'$, per tant, $e\in\ker f$, i el nucli amb el menor nombre d'elements que es pot tenir és $\ker f=\{e\}$.

Exemple 7.1 (kernel) La funció

$$f:\mathbb{Z}\to\mathbb{Z}_n:x\to x\bmod n$$

és un homomorfisme, i el kernel és $\ker f=\langle n\rangle=n\,\mathbb{Z}$. Clarament,

$$\begin{aligned}f(a+b)=(a+b)\bmod n=\\ (a\bmod n)+(b\bmod n)=f(a)+f(b),\forall a,b\in\mathbb{Z}\end{aligned}$$

(l'operació del grup $\mathbb{Z}$ és l'addició). A més

$$f(x)=x\bmod n=f(0)=0,\forall x\in\langle n\rangle.$$

Teorema 7.1 El **nucli (*kernel*)** és un subgrup normal.

Demostració. Per $a,b\in\ker f$ tenim $f(a\,b^{-1})=f(a)\,f(b^{-1})=e'\Rightarrow a\,b^{-1}\in\ker f$, que prova que $\ker f$ és subgrup de G. Per provar que és normal hem de provar que $a\,\ker f\,a^{-1}\subseteq\ker f$, $\forall a\in G$. Veure el teorema 5.2, pàg. 14. Però si $x\in\ker f$, llavors $f(a\,x\,a^{-1})=f(a)\,f(x)\,f(a^{-1})=f(a)\,f(a^{-1})=f(e)=e'\Rightarrow a\,x\,a^{-1}\in\ker f$. □

Teorema 7.2 [3, pàg. 77]. Un homomorfisme f és injectiu (és a dir, és un monomorfisme) sii $\ker f=\{e\}$, on e és l'element identitat de G.

Demostració. Suposem que f és injectiva. Sigui $e' = f(e)$ l'element identitat de G'. Llavors per cada $a \in G$ diferent de e es té

$$f(a) \neq f(e) = e'$$

Per tant $a \notin \ker f$, i es conclou $\ker f = \{e\}$. Per el contrari, suposar que $\ker f = \{e\}$ i $f(a) = f(b)$. Llavors $f(a)\,f(b)^{-1} = e' = f(e) = f(a)\,f(b^{-1}) = f(a\,b^{-1}) \Rightarrow a\,b^{-1} = e \Rightarrow a = b$. □

Una conseqüència d'aquest teorema és que el kernel d'un isomorfisme (veure la definició 7.4, pàg. 18) és el grup trivial $\ker f = \{e\}$, doncs, com es veurà, un isomorfisme és una funció bijectiva (i, per tant, injectiva).

Propietats 7.1 Homomorfismes:

[2, pàg. 202] Sigui $f : G \to G'$ un homomorfisme del grup G al grup G':

1. Si els elements neutres de G i G' són e i e', llavors $e' = f(e)$. Doncs $e'\,f(e) = f(e) = f(e\,e) = f(e)\,f(e)$.
2. $f(a^n) = f(a)^n$, $\forall a \in G$. En cas que l'operació del grup sigui l'addició: $f(n\,a) = n\,f(a)$, $\forall a \in G$.
3. $f(a^{-1}) = f(a)^{-1}$, doncs
$$f(a)\,f(a^{-1}) = f(a\,a^{-1}) = f(e) = e'$$
$$f(a^{-1})\,f(a) = f(a^{-1}\,a) = f(e) = e'.$$
4. Si K és un subgrup de G, llavors $f(K)$ és un subgrup de G'. A més, si K és normal de G, llavors $f(K)$ també ho és de G'.
5. Si H' és un subgrup de G', llavors $f^{-1}(H') = \{x \in G : f(x) \in H'\}$ és un subgrup de G. A més, si H' és normal de G', llavors $f^{-1}(H')$ també ho és de G. Veure la demostració en [3, pàg. 78].
6. Si H és un subgrup de G, llavors
$$f : H \to G : x \to x \tag{7.3}$$
és un homomorfisme injectiu, doncs $f(x\,y) = x\,y = f(x)\,f(y)$.
7. Si $f : G \to G'$ i $g : G \to G'$ i són homomorfismes, també ho és $g \circ f : G \to G'$, doncs $g \circ f(x\,y) = g(f(x\,y)) = g(f(x)\,f(y)) = g(f(x))\,g(f(y)) = (g \circ f(x))\,(g \circ f(y))$.
8. Si $x \in G$ i $\mathrm{o}(x) = m$, llavors
   (a) $\mathrm{o}(f(x))$ divideix m.
   (b) Si f és injectiva, $\mathrm{o}(f(x)) = m$.
   Veure la demostració en [3, pàg. 79].
9. $f(a) = f(b)$ sii $a \ker f = b \ker f$.
10. Si $f(a) = a'$, llavors
$$f^{-1}(a') = \{x \in G : f(x) = a'\} = a \ker f.$$
11. Si f és surjectiva (epimorfisme) i $\ker f = \{e\}$, llavors f és un isomorfisme de G a G'.
12. Si $\mathrm{o}(\ker f) = n$, llavors f és una aplicació n-a-1 (n-*to*-1).

La figura 7.1 il·lustra algunes de les propietats anteriors (veure [2, pàg. 205]).

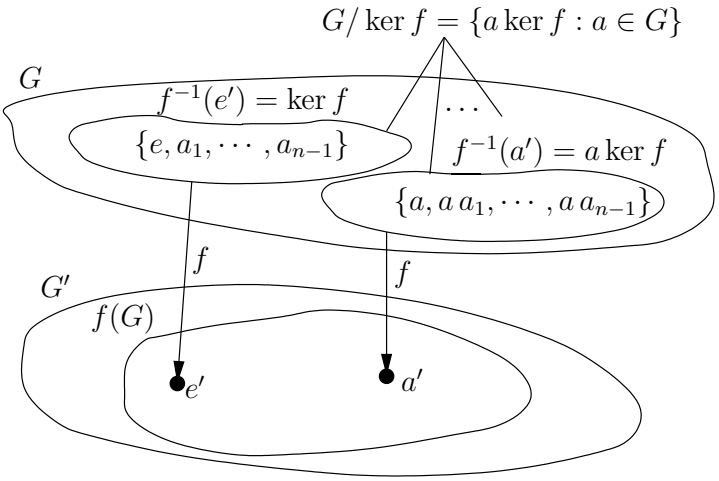


Figura 7.1: Propietats d'un homomorfisme.

Teorema 7.3 (Veure [3, 2.4.8, pàg 78]) Si N **és un subgrup normal** de G, la funció (*mapping*):

$$\pi : G \to G/N : a \to a\,N \tag{7.4}$$

és un homomorfisme sobrejectiu, doncs $\pi(a\,b) = a\,b\,N = (a\,N)\,(b\,N) = \pi(a)\,\pi(b)$. Recordar que per el grup quocient es defineix $a\,b\,H = (a\,H)\,(b\,H)$ (veure el teorema 6.1).

La funció (7.4) s'anomena també **projecció** o **homomorfisme natural** (*natural homomorphism*).

Aquest és un resultat important, doncs implica que si N és un subgrup normal de G, les classes laterals tenen estructura de grup, amb operació $(a\,H)\,(b\,H) = a\,b\,H$ (veure el teorema 6.1).

Exemple 7.2 (grup quocient $\mathbb{Z}/E$)
(Problema 4.64 de [1]). Provar que $\mathbb{Z}/E = C_2$ on E és el conjunt dels enters parells.

Solució Com que $\mathbb{Z}$ és abelià, E és un subgrup normal. Per tant, per el teorema 7.3 es té que $\mathbb{Z}/E$ té estructura de grup. De fet, $\mathbb{Z}/E = \{E, E+1\}$, doncs un enter és parell o senar. L'element neutre és $e = E$, doncs $E+(E+1) = E+1$, i $E+E = E$. A més $E^2 = E+E = E = e$ i $(E+1)^2 = (E+1)+(E+1) = E = e$. Per tant, $\mathbb{Z}/E = \{E, E+1\}$ és un grup cíclic d'ordre 2.

Definició 7.3 (Tipus d'homomorfismes) Existeixen tipus especials d'homomorfismes segons f sigui:

- Surjectiva (*onto*), i es diu **epimorfisme**.
- Injectiva (*one-to-one*), i es diu **monomorfisme**.
- Surjectiva i injectiva (bijectiva), i es diu **isomorfisme**.

El cas d'un isomorfisme és especialment rellevant i s'explica en més detall a continuació.

Definició 7.4 Grup isomorf (del grec *iso*, "igual" i *morfic*, "forma") Un isomorfisme $f : G \to G'$ és una bijecció que preserva l'operació del grup:

$$f(a\,b) = f(a)\,f(b), \forall a\,b \in G \tag{7.5}$$

Si existeix un isomorfisme f entre G i G' es diu que els grups G i G' són isomorfs, i s'escriu $G \cong G'$. Notar que els rols d'un homomorfisme i un isomorfisme són molt diferents. Un homomorfisme pot simplificar un grup, tot i mantenir algunes característiques. Dos grups isomorfs, en canvi, són idèntics des d'un punt de vista algebraic.

Test d'isomorfia Per comprovar que dos grups són isomorfs cal:

1. Definir la funció f entre els grups.
2. Provar que f és injectiva (*one-to-one*).
3. Provar que f és surjectiva (*onto*).
4. Provar que f preserva l'operació:

$$f(a\,b) = f(a)\,f(b), \forall a,b \in G$$

.

Exemple 7.3 (isomorfisme 2^x)
El grup G format per els reals i la suma és un isomorfisme del grup G' format per els reals positius i la multiplicació amb la bijecció $f(x) = 2^x$, doncs

$$f(x+y) = 2^{x+y} = 2^x\,2^y = f(x)\,f(y), \forall x,y \in \mathbb{R}$$

Exemple 7.4 (x^3 no és isomorfisme)
La funció $f : \mathbb{R} \to \mathbb{R} : x \to x^3$ no és un isomorfisme de $G = (\mathbb{R}, +)$ a $G' = (\mathbb{R}, +)$, doncs, tot i que f és bijectiva, $(x+y)^3 \neq x^3 + y^3$, $\forall x,y \in \mathbb{R}$.

Teorema 7.4 Dos grups cíclics $G_1 = \langle a \rangle$, $G_2 = \langle b \rangle$ del mateix ordre són isomorfs amb la bijecció

$$f : G_1 \to G_2 : a^n \to b^n.$$

Demostració. Òbviament f és bijectiva, i $f(a^{n_1}\,a^{n_2}) = f(a^{n_1+n_2}) = b^{n_1+n_2} = b^{n_1}\,b^{n_2} = f(a^{n_1})\,f(a^{n_2})$ □

Exemple 7.5 (isomorfisme dels grups cíclics)
Qualsevol grup cíclic infinit és isomorf del grup $\mathbb{Z}$, doncs la bijecció $a^k \to k$ és un isomorfisme. Igualment, qualsevol grup cíclic $\langle a \rangle$ d'ordre n és isomorf del grup additiu dels enters mòdul n ($\mathbb{Z}_n = \{0, 1, 2, \cdots (n-1)\}$) amb la bijecció $a^k \to k \bmod n$. També és una conseqüència immediata del teorema 7.4.

Exemple 7.6 ($\mathbb{Z}_n \cong \mathbb{Z}/n\,\mathbb{Z}$)
El **Grup additiu dels enters mòdul** n ($\mathbb{Z}_n = \{0, 1, 2, \cdots (n-1)\}$) és isomorf del grup quocient $\mathbb{Z}/n\,\mathbb{Z}$ (veure la definició de $\mathbb{Z}/n\,\mathbb{Z}$ en 6.2, pàg. 16). És una conseqüència immediata del teorema 7.4, doncs $\mathbb{Z}_n$ i $\mathbb{Z}/n\,\mathbb{Z}$ són ambdós cíclics del mateix ordre n (veure 2.5, pàg. 5 i 6.2, pàg. 16, respectivament).

Exemple 7.7 (isomorfisme de $\mathbb{Z}^o_{p^k}$)
El **Grup multiplicatiu dels enters mòdul** n (veure 6.1, pàg. 16) és cíclic sii $n = 1,2,4,p^k,2\,p^k$ on p és un primer major que 2 i k un enter positiu. Com que $\mathrm{o}(\mathbb{Z}^o_n) = \phi(n)$ (veure C), per els valors p^k es té:

$$\mathbb{Z}^o_{p^k} \cong \mathbb{Z}_{\phi(p^k)} = \mathbb{Z}_{p^k(1-1/p)} \tag{7.6}$$

Teorema 7.5 Sigui $m = n_1\,n_2\,\cdots n_k$, on n_i són enters positius. Llavors el següent producte directe de grups (veure 2.16, pàg. 7) és una isomorfia sii n_i,n_j, $i \neq j$ són primers relatius

$$Z_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_k} \tag{7.7}$$

$\mathbb{Z}_{n_i}$ és el grup additiu dels enters mòdul n_i: $\mathbb{Z}_{n_i} = \{0, 1, 2, \cdots (n_i - 1)\}$.

Demostració. $\mathbb{Z}_{n_i}$ és cíclic (veure l'exemple 2.5, pàg. 5), i el producte directe de grups cíclics és cíclic sii els ordres dels grups són primers relatius (veure el teorema 2.19, pàg. 8), □

Teorema 7.6 (Un subgrup i el seu conjugat són isomorfs)
Sigui G un grup, H un subgrup de G i $a \in G$. Definim la funció

$$f : H \to H^a = a^{-1}\,H\,a : h \to a^{-1}\,h\,a.$$

Llavors els grups H i H^a són isomorfs.

Demostració.

1. $h \in \ker f \Rightarrow a^{-1} h\, a = e \Rightarrow h = e$. Per tant $\ker f = \{e\}$, que, per el teorema 7.2, prova que f és injectiva.
2. Sigui $x \in H^a$. Llavors $\exists h \in H : f(x) = a^{-1} h\, a$. Per tant, f és surjectiva.
3. $f(h_1\, h_2) = a^{-1}\,(h_1\, h_2\, a) = (a^{-1}\, h_1\, a)\,(a^{-1}\, h_2)\, a = f(h_a)\, f(h_2)$. Per tant, f preserva l'operació. □

Veure la definició de subgrup conjugat en 2.10, pàg. 6.

Propietats 7.2 Dels isomorfismes

1. Les mateixes que les dels homomorfismes 7.1, doncs un isomorfisme també es homomorfisme.
2. f^{-1} és un isomorfisme de G' a G. Per aixo es diu simplement que G i G' són **grups isomorfs** i es denota per $G \cong G'$.
3. Dos grups isomorfs tenen les mateixes propietats (de la teoria de grups). En particular:
4. Si a,$b \in G$ son commutatius, també ho són $f(a)$,$f(b) \in G'$. Per tant, si G és abelià, també ho és G'.
5. $G = \langle a \rangle$ sii $G' = \langle f(a) \rangle$. Per tant, si G és cíclic, també ho és G'.
6. $\mathrm{o}(G) = \mathrm{o}(G')$ i $\mathrm{o}(a) = \mathrm{o}(f(a))\ \forall a \in G$.
7. Les equacions $x^k = a$ en G tenen el mateix nombre de solucions que $x^k = f(a)$ en G'.
8. Per a grups finits G i G' tenen el mateix nombre d'elements de cada ordre.
9. Si X i Y són dos conjunts finits amb n elements, llavors $Biy(X)$ i $Biy(Y)$ són isomorfs.

Veure les demostracions en [2, pàg. 128] i [3, pàg. 81].

Teorema 7.7 Sigui G un grup amb $\mathrm{o}(G) = 2\,p$, on p és un nombre primer major de 2. Llavors G és isomorf de $\mathbb{Z}_{2p}$ o D_p. Per exemple, S_3, amb ordre $3! = 6$, és isomorf de D_3.

Teorema 7.8 (Cayley)
Tot grup és isomorf d'un grup permutatiu.

Definició 7.5 Es diu **imatge de** f a:

$$\mathrm{im}\, f = \{f(x) : x \in G\} = f(G) \tag{7.8}$$

$\mathrm{im}\, f$ és un subgrup de G, doncs si $a = f(x)$, $b = f(y)$, llavors $a\, b^{-1} = f(x)\, f(y)^{-1} = f(x)\, f(y^{-1}) = f(x\, y^{-1}) \in \mathrm{im}\, f$.

Teorema 7.9 (Primer teorema d'isomorfia)
Si $f : G \to G'$ és un homomorfisme, llavors $G/\ker f$ és isomorf de $\mathrm{im}\, f = f(G)$. Notar que això implica que $\mathrm{o}(G/\ker f) = \mathrm{o}(f(G))$. La figura 7.1, pàg. 17 il·lustra aquest teorema.

Demostració. (esbós) Recordar del teorema 7.1 que $\ker f$ és un subgrup normal de G. A més, per el teorema 7.3 es té que $G/\ker f$ té estructura de grup i és un isomorfisme de G. Per a més detalls, veure la demostració en [3, pàg. 82]. □

Exemple 7.8 (homomorfisme injectiu $f : S_3 \to A_4$?)
[3, prob. 26.a, pàg. 114] Existeix un homomorfisme injectiu $f : S_3 \to A_4$?

Solució Si f és injectiva llavors $\ker f = \{e\}$ (teorema 7.2, pàg. 16). Per el primer teorema d'isomorfia (teorema 7.9) tenim $S_3/\ker f = S_3 \cong f(S_3)$. Per tant, $f(S_3)$ seria un subgrup d'A_4 amb $\mathrm{o}(f(S_3)) = \mathrm{o}(S_3) = 3! = 6$. Però això no és possible, perquè, tal com s'ha vist en l'exemple 4.7, pàg. 13, A_4 no té cap subgrup d'ordre 6.

Exemple 7.9 (homomorfismes entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$)
[3, ex. 2.9.4, pàg 84] Calcular els homomorfismes entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.

Solució (veure [3, pàg 86]) Els homomorfismes entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$ són del tipus:

$$f_k : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \to k\, x + n\mathbb{Z}$$
$$k = i\,\frac{n}{d},\ i = 0, \cdots d-1,\ d = \gcd(m,n). \tag{7.9}$$

Per tant, hi ha $d = \gcd(m,n)$ homomorfismes diferents.

Exemple 7.10 (monomorfismes entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$)

[3, ex. 2.9.4, pàg 87] Calcular els homomorfismes injectius (monomorfismes) entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.

Solució (veure [3, pàg 88]) Sigui $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
Si f és injectiva llavors $\ker f = \{e\}$ (teorema 7.2, pàg. 16). Per el primer teorema d'isomorfia (teorema 7.9) tenim $(\mathbb{Z}/m\mathbb{Z})/\ker f = \mathbb{Z}/m\mathbb{Z} \cong \mathrm{im}\, f = f(\mathbb{Z}/m\mathbb{Z})$, que ha de ser un subgrup de $\mathbb{Z}/n\mathbb{Z}$. Tenim doncs $\mathrm{o}(f(\mathbb{Z}/m\mathbb{Z})) = m$ que ha de dividir $\mathrm{o}(\mathbb{Z}/n\mathbb{Z}) = n$, per teorema de Lagrange. Tenint en compte l'exemple 7.9, es conclou que els monomorfismes són de la forma:

$$f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \to k\, x + n\mathbb{Z}$$
$$k = i\,\frac{n}{m},\ i = 0, \cdots m-1,\ \gcd(i,m) = 1. \tag{7.10}$$

Per tant, el nombre de monomorfismes és la funció $\phi(m)$ d'Euler. Veure l'apèndix C.

Exemple 7.11 (epimorfismes entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$) [3, ex. 2.9.4, pàg 88] Calcular els d'homomorfismes surjectius (epimorfismes) entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.

Solució (veure [3, pàg 88]) Sigui $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Si f és surjectiva llavors $\operatorname{im} f = f(\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. Per tant $(\mathbb{Z}/m\mathbb{Z})/\ker f \cong \operatorname{im} f \cong \mathbb{Z}/n\mathbb{Z} \Rightarrow [\mathbb{Z}/m\mathbb{Z} : \ker f] = n$ i, per el teorema de Lagrange, $m/\mathrm{o}(\ker f) = n$. És a dir, m és un múltiple de n. Tenint en compte l'exemple 7.9, es conclou que els epimorfismes són de la forma:

$$f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \to k\,x + n\mathbb{Z}$$
$$k = i,\ i = 0, \cdots n-1,\ \gcd(i,n) = 1. \quad (7.11)$$

Per tant, el nombre d'epimorfismes és la funció $\phi(n)$ d'Euler. Veure l'apèndix C.

Exemple 7.12 (primer teorema d'isomorfia) (Veure [3, 2.96, pàg. 91] per a més detalls) Sigui

$$\epsilon : S_n \to U_2 = \{1, -1\} :$$
$$\alpha \to \epsilon(\alpha) = \begin{cases} 1, & \alpha \text{ és una permutació parella,} \\ -1, & \alpha \text{ és una permutació senar.} \end{cases} \quad (7.12)$$

Veure la definició de permutació parella i senar en el teorema 3.6, pàg. 10. Llavors, el grup altern A_n (veure la definició en 3.3, pàg. 10) és:

$$A_n = \ker \epsilon = \{\alpha \in S_n : \epsilon(\alpha) = 1\} \quad (7.13)$$

A_n és un grup normal de S_n. Llavors, per el primer teorema d'isomorfia: $S_n/\ker\epsilon = S_n/A_n \cong U_2$. Per tant $[S_n : A_n] = \mathrm{o}(S_n/A_n) = \mathrm{o}(U_2) = 2$. Per el teorema de Lagrange tenim $\mathrm{o}(S_n)/\mathrm{o}(A_n) = 2$. com que $\mathrm{o}(S_n) = n!$ es conclou que $\mathrm{o}(A_n) = n!/2$, tal com es va deduir en la definició de grup altern 3.3, pàg. 10.

Teorema 7.10 (Segon teorema d'isomorfia)
Siguin N i H subgrups normals d'un grup G tals que $N \subset H$. Llavors H/N és subgrup normal de G/N i

$$(G/N)\,(H/N) \cong G/H \quad (7.14)$$

Veure la demostració en [3, pàg. 98].

Teorema 7.11 (Tercer teorema d'isomorfia)
Siguin N i H subgrups d'un grup G, N subgrup normal de G. Llavors H/N és subgrup normal de G/N i

1. $H \cap N$ és subgrup normal d'H.
2. $H\,N$ és subgrup de G.
3. N és subgrup normal de $H\,N$.
4. $(H\,N)/N \cong H/(H \cap N)$.

Veure la demostració en [3, pàg. 99].

Teorema 7.12 (Quart teorema d'isomorfia)
Siguin H_1 i H_2 subgrups d'un grup G, N_1 subgrup normal de H_1 i N_2 subgrup normal de H_2. Llavors

1. $N_1\,(H_1 \cap H_2)$ i $N_2\,(H_1 \cap H_2)$ són subgrups de H_1 i H_2, respectivament.
2. $N_1\,(H_1 \cap N_2)$ és subgrup normal de $N_1\,(H_1 \cap H_2)$ i $N_2\,(N_1 \cap H_2)$ és subgrup normal de $N_2\,(H_1 \cap H_2)$.
3. $(H_1 \cap N_2)\,(N_1 \cap H_2)$ és subgrup normal de $(H_1 \cap H_2)$.
4. $$N_1\,(H_1 \cap H_2)/N_1\,(H_1 \cap N_2) \cong$$
$$N_2\,(H_1 \cap H_2)/N_2\,(N_1 \cap H_2) \cong$$
$$(H_1 \cap H_2)/(H_1 \cap N_2)(N_1 \cap H_2)$$

Veure la demostració en [3, pàg. 101].

Capítol 8
Teoremes de Sylow

Teorema 8.1 (Primer teorema de Sylow)
Sigui G un grup finit, p un nombre primer i p^k la major potència de p que divideix $\mathrm{o}(G)$. Llavors hi ha al menys un subgrup de G d'ordre p^k. Si H és un subgrup de G d'ordre p^k, llavors H es diu un **p-subgrup de Sylow** de G. En general, un grup d'ordre igual a una potència d'un nombre primer p es diu un **p-grup**. Així, un p-subgrup de Sylow H d'un grup G és el **p-grup maximal** en G. Veure la demostració del teorema en [1, pàg. 130], [2, pàg. 407] o [3, pàg. 175].

Teorema 8.2 (Segon teorema de Sylow)
Sigui G un grup finit, si H és un subgrup de G i $\mathrm{o}(H)$ és la potència d'un nombre primer p (és a dir, H és un p-grup), llavors H està contingut en algun p-subgrup de Sylow de G. Veure la demostració del teorema en [1, pàg. 131], [2, pàg. 408] o [3, pàg. 175].

Teorema 8.3 (Tercer teorema de Sylow)
Sigui G un grup finit, p un nombre primer i $\mathrm{o}(G) = m\,p^k$, tal que p no divideix m. Llavors el nombre n_p de p-subgrups de Sylow de G compleix: (1) n_p divideix m i (2) $n_p - 1$ és un múltiple de p. Notar que $n_p = 1 + k\,p$, per algun enter k, i en aritmètica mòdul p es té $(1 + k\,p) \bmod p = 1$. Per això també es diu que n_p és congruent a 1 en aritmètica mòdul p, o

simplement, 1 en mòdul p. A més, si H i K són p-subgrups de G, llavors H i K són conjugats, és a dir, $\exists a \in G : K = H^a = a^{-1} H\, a$. Recíprocament, si H és un p-subgrup de G, llavors $H^a\ \forall a \in G$ també és un p-subgrup de G. Per tant, el nombre de n_p de p-subgrups de G és $n_p = [G : N(H)]$. Veure la def. de subgrups conjugats en 5.2 i el normalitzador $N(H)$ en 2.15. Veure la demostració del teorema en [1, pàg. 131], [2, pàg. 408] o [3, pàg. 175].

Teorema 8.4 Sigui G un grup finit i H un p-subgrup de G. H és un subgrup normal sii el nombre de p-subgrups $n_p = 1$ (és a dir, si H és l'únic p-subgrup de G). Veure la demostració en [2, pàg. 410] o [3, pàg. 177].

Exemple 8.1 (primer teorema de Sylow)
Per el grup A_4, $\mathrm{o}(A_4) = 4!/2 = 12$. Tenim els nombres primers 2 i 3 que divideixen 12. Per tant, per el primer teorema de Sylow, tenim que hi ha 2-subgrups i 3-subgrups de Sylow.

El 2-subgrup maximal que divideix 12 és $2^2 = 4$. Per tant, per el primer teorema de Sylow hi ha, al menys 1 2-subgrup de Sylow d'ordre 4. Com que $3 \cdot 2^2 = 12$, del tercer teorema de Sylow tenim que hi pot haver 1 o 3 2-subgrups de Sylow d'A_4, doncs 1 i 3 divideixen $m = 3$, i $1 = 1 + k\,2$ per $k = 0$, $3 = 1 + k\,2$ per $k = 1$. Tal com es va obtenir en l'exemple 4.7, pàg. 13, només hi ha 1 2-subgrup de Sylow (curiosament, en l'exemple 4.7 s'-ha obtingut que n'hi ha 3 d'ordre 2). Com que només hi ha 1 2-subgrup de Sylow, per el teorema 8.4 podem afirmar que és un subgrup normal.

El 3-subgrup maximal que divideix 12 és 3^1. Per tant, per el primer teorema de Sylow hi ha, al menys 1 3-subgrup de Sylow d'ordre 3. Com que $4 \cdot 3^1 = 12$, del tercer teorema de Sylow tenim que només hi pot haver 4 3-subgrups de Sylow d'A_4, doncs 4 divideixen $m = 4$, i $4 = 1 + k\,3$ per $k = 1$. Tal com es va obtenir en l'exemple 4.7, efectivament hi ha 4 3-subgrup de Sylow d'ordre 3. Per el tercer teorema de Sylow tenim que els 4 3-subgrups de Sylow d'A_4 són conjugats.

Capítol 9

Estructura dels grups abelians finits

Lema 9.1 Sigui G un grup abelià finit i $x \in G$ un element d'ordre màxim. Llavors per a cada $y \in G$, $\mathrm{o}(y)$ divideix $\mathrm{o}(x)$. Veure la demostració en [3, pàg. 104].

Lema 9.2 Sigui G un grup i H, K subgrups normals de G tals que $H \cap K = \{e\}$. Llavors $H\,K$ i $H \times K$ són isomorfs. És a dir:

$$f : H \times K \to H\,K : (h, k) \to h\,k.$$

és un isomorfisme. Veure la demostració en [3, pàg. 105].

Lema 9.3 ([2, Ex. 11, pàg. 226]) El producte de potències de nombres primers (no necessàriament iguals) es pot expressar com el producte d'enters positius $m_1\, m_2 \cdots m_r$ tals que m_i divideix m_{i-1}, $i = 2, \cdots, r$; i que els factors que formen cada m_i siguin nombres primers relatius.

Demostració. Agafar les potències majors de tots els primers diferents i formar m_1 com el producte de totes elles. Això garanteix que els factors que formen m_1 són primers relatius. Repetir el mateix amb els factors que queden i així successivament fins acabar. Per exemple:

$$\begin{aligned} 125 \times 25 \times 27 \times 3 \times 4 \times 2 \times 2 = \\ 5^3 \times 5^2 \times 3^3 \times 3 \times 2^2 \times 2 \times 2 = \\ (5^3 \times 3^3 \times 2^2)(5^2 \times 3 \times 2)(2) = \\ m_1 \times m_2 \times m_3 \end{aligned}$$

□

La utilitat d'aquest lema és la següent. Suposem que tenim grups cíclics d'ordre igual a les potències dels nombres primers. Seguint l'exemple anterior: $G_1 = \mathbb{Z}_{125} \times \mathbb{Z}_{25} \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Notar que G_1 no seria cíclic, doncs els ordres dels grups $\mathbb{Z}_i$ no són primers relatius (veure el teorema 2.19). Però agrupant els factors de forma que siguin primers relatius, com s'ha fet abans, obtenim els grups cíclics $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \mathbb{Z}_{m_3}$. El producte directe d'aquests grups $G_2 = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3}$ serà abelià i tindrà els elements amb mateix ordre que G_1 (veure les propietats dels isomorfismes 7.2, pàg. 19). Per tant, G_1 i G_2 seran isomorfs.

Teorema 9.1 Teorema d'estructura de grups abelians finits.

Tot grup abelià finit G és el producte directe de grups cíclics d'ordre potències de nombres primers (no necessàriament diferents). A més, el nombre de termes i els ordres dels grups cíclics és únic per a cada G. Veure [2, teorema 11.1, pàg. 218]

Com que un grup cíclic d'ordre n és isomorf a $\mathbb{Z}_n$ (veure l'exemple 7.5, pàg. 18), i tenint el compte el lema 9.3, el teorema es pot reformular així (veure [2, pàg. 222] o [3, proposició 2.2.1, pàg. 106]):

Sigui G un grup abelià finit, llavors existeixen enters positius $m_1, m_2, \cdots m_r$ tals que

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \mathbb{Z}_{m_r} \tag{9.1}$$

on cada m_i divideix m_{i-1}. A més, els nombres $r, m_1, m_2, \cdots m_r$ són únics i $\mathrm{o}(G) = m_1\, m_2 \cdots m_r$. Els

nombres $m_1, m_2, \cdots m_r$ es diuen **coeficients de torsió** de G. El càlcul de l'equació (9.1) té l'avantatge que els grups que s'obtenen no són isomorfs entre ells, doncs el resultats dels productes (9.1) donarà lloc a grups amb elements d'ordre diferent. Per tant, calculant tots els possibles coeficients de torsió diferents, per a cada possible r, s'obtenen tots els grups no isomorfs entre ells, i amb producte igual a G.

Veure la demostració en [2, pàg. 223] i [3, pàg. 106]. Veure la definició de producte directe de grups en 2.18, pàg. 8. Nota: en [3] es fa servir $\mathbb{Z}/m_i\,\mathbb{Z}$ en comptes de $\mathbb{Z}_{m_i}$ (notació que es fa servir en [2]). Ambdues són equivalents, doncs $\mathbb{Z}/m_i\,\mathbb{Z}$ i $\mathbb{Z}_{m_i}$ són isomorfs (veure l'exemple 7.6, pàg. 18).

Exemple 9.1 (grups abelians d'ordre 36)
[3, ex. 2.21.2, pàg. 110] Calcular els grups abelians, no isomorfs entre ells, d'ordre 36.

Solució. Del teorema 9.1 hem de buscar les tuples $r, m_1, m_2, \cdots m_r$ tals que $m_1\, m_2 \cdots m_r = 36$ i m_i divideix m_{i-1}.

1. Per $r = 1$ tenim $m_1 = 36$. Llavors $G_1 = \mathbb{Z}_{36}$.
2. Per $r = 2$ tenim

$$\begin{aligned} &m_1 = 18,\ m_2 = 2, \text{ Llavors } G_2 = \mathbb{Z}_{18} \times \mathbb{Z}_2,\\ &m_1 = 12,\ m_2 = 3, \text{ Llavors } G_3 = \mathbb{Z}_{12} \times \mathbb{Z}_3,\\ &m_1 = 6,\ m_2 = 6, \text{ Llavors } G_4 = \mathbb{Z}_6 \times \mathbb{Z}_6 \end{aligned}$$

3. Per $r \geq 3$ ja no hi ha més productes tals que m_i divideix m_{i-1}.

Notar que dels grups anteriors només G_1 és cíclic, doncs $G_1 \times G_2$ és cíclic sii $\mathrm{o}(G_1)$ i $\mathrm{o}(G_2)$ són primers relatius (veure el teorema 2.19). Notar també que hi ha altres productes dels grups $\mathbb{Z}_i$ d'ordre 36, però seran isomorfs d'algun grup anterior. Per exemple, del teorema 2.19 tenim que $\mathbb{Z}_9 \times \mathbb{Z}_4 \cong \mathbb{Z}_{36} = G_1$, doncs 9 i 4 són primers relatius. Igualment, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_2 \times \mathbb{Z}_{18} \cong \mathbb{Z}_{18} \times \mathbb{Z}_2 = G_2$ (doncs per el teorema 2.19 $\mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_{18}$), etc.

Capítol 10

Estructura dels grups abelians finitament generats

Definició 10.1 Subgrup de torsió. Sigui G un grup, definim:

$$T(G) = \{g \in G : \mathrm{o}(g) \text{ és finit}\}. \tag{10.1}$$

Si G és abelià, llavors T és un subgrup de G i el denominarem el **subgrup de torsió** de G. En general, si G no és abelià, $T(G)$ no és un subgrup de G.

Propietats 10.1 Del subgrup de torsió

1. Si G és abelià, llavors $G/T(G)$ no té torsió.
2. El grup $G = \underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{n}$, que denotarem per $\mathbb{Z}^n$, no té torsió.
3. Si G és finit, llavors $T(G) = G$. El recíproc és fals.
4. Si G és abelià i $K \subset G$, llavors $T(K) = K \cap T(G)$. D'on es dedueix $T(T(G)) = T(G)$.
5. Sigui

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_r\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{s}$$

tenim

$$T(G) = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_n\mathbb{Z} \times \underbrace{\emptyset \times \cdots \emptyset}_{r} = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_r\mathbb{Z} \tag{10.2}$$

doncs ningun element $x = (a_1 + m_1\mathbb{Z}, \cdots a_r + m_n\mathbb{Z}, b_1, \cdots b_r)$ amb $b_i \neq 0$ té ordre finit.

6. Sigui

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_n\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{r}$$

tenim

$$G/T(G) = \underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{s}$$

Veure les demostracions en [3, pàg. 326].

Teorema 10.1 (d'estructura de grups abelians finitament generats)
Sigui G un grup abelià finitament generat. Llavors existeixen els enters no negatius n i r, i si $n \neq 0$ enters positius $m_1, \cdots m_n$, tals que:

1. $$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_n\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{r} \tag{10.3}$$
2. m_i divideix m_{i-1}, $i = 2, \cdots n$.
3. $$T(G) \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_n\mathbb{Z} \tag{10.4}$$

   i $r = \beta(G)$ és el **nombre de Betti**.
4. $G \cong T(G) \times G/T(G)$

Veure les demostracions en [3, pàg. 331].

10.1 Construcció

Veure [3, pàg. 337]. Sigui G un grup abelià finitament generat i

$$S = \{x_1, \cdots x_n\} \tag{10.5}$$

un **sistema generador** de G (veure la definició 2.6, pàg. 4). Denotem

$$\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{n} \tag{10.6}$$

i definim l'homomorfisme

$$\begin{aligned} f_s : \mathbb{Z}^n &\to G : \\ (m_1, \cdots m_n) &\to x_1\, m_1 + \cdots x_n\, m_n \end{aligned} \tag{10.7}$$

Notar que

$$\begin{aligned} f_s((m_1, \cdots m_n) + (g_1, \cdots g_n)) = \\ x_1\,(m_1 + g_1) + \cdots x_n\,(m_n + g_n) = \\ (x_1\, m_1 + \cdots x_n\, m_n) + (x_1\, g_1 + \cdots x_n\, g_n) = \\ f_s(m_1, \cdots m_n) + f_s(g_1, \cdots g_n), \end{aligned}$$

i definim el **subgrup de les relacions de G respecte d'S**:

$$R(S) = \ker f_s. \tag{10.8}$$

Notar que $(m_1, \cdots m_n) \in R(S) = \ker f_s$ equival a la relació entre els generadors d'$S = \{x_1, \cdots x_n\}$:

$$m_1\, x_1 + \cdots m_n\, x_n = 0 \tag{10.9}$$

Veure la definició de $\ker f$ 7.2, pàg. 16. En el que que segueix es farà servir el terme **relació** per referir-se a la tupla $(m_1, \cdots m_n) \in R(S)$, o a l'expressió (10.9) a la que es es refereix. Utilitzant el teorema 9.1 tenim que existeixen els enters no negatius j, k tals que

$$R(S) = \mathbb{Z}/q_1\,\mathbb{Z} \times \mathbb{Z}/q_j\,\mathbb{Z} \times \mathbb{Z}^k \tag{10.10}$$

De la propietat 10.1.5 tenim

$$T(R(S)) = \mathbb{Z}/q_1\mathbb{Z} \times \cdots \mathbb{Z}/q_j\mathbb{Z}$$

i de 10.1.4

$$T(R(S)) = R(S) \cap T(\mathbb{Z}^k)$$

com que $T(\mathbb{Z}^k) = \{e\}$ tenim

$$T(R(S)) = \mathbb{Z}/q_1\mathbb{Z} \times \cdots \mathbb{Z}/q_j\mathbb{Z} \cong \{e\}$$

i, substituint en (10.10):

$$R(S) \cong \{e\} \times \mathbb{Z}^k = \mathbb{Z}^k$$

on $k = \beta(R(S)) \leq \beta(\mathbb{Z}^n) = n$ és el **nombre de Betti**. Per el primer teorema d'isomorfia (veure 7.9, pàg. 19):

$$\mathbb{Z}^n/R(S) \cong G. \tag{10.11}$$

Definició 10.2 Sigui G un grup abelià finitament generat i S un sistema generador finit de G. Tenim $R(S) = \ker f_s = \mathbb{Z}^k$.

1. Es diu **sistema complet de relacions de G respecte** S a qualsevol sistema generador minimal R del subgrup $R(S)$. Notar que la relació $(m_1, \cdots m_n) \in R(S) = \ker f_s$ entre els generadors $S = \{x_1, \cdots x_n\}$ de G equival a l'equació (10.9).
2. Una **presentació de G mitjançant generadors i relacions** és una tupla (S,R) on S és un sistema generador de G i R un sistema complet de relacions de G respecte S (definit en el punt anterior).

Veure [3, def.7.11, pàg. 338]. Nota: Per a representar la presentació anterior es farà servir la notació:

$$G = \langle x_1, \cdots x_n : m_1\, x_1 = \cdots m_n\, x_n = 0 \rangle \tag{10.12}$$

Proposició 10.1 Càlcul dels coeficients de torsió i del nombre de Betti Sigui G un grup abelià finit amb la presentació de G mitjançant generadors i relacions, amb

$$\begin{aligned} S &= \{x_1, \cdots x_n\} \\ R &= \{r_1, \cdots r_k\} \\ r_i &= (0, \cdots, m_i, \cdots, 0) \end{aligned}$$

on m_{i+1} divideix m_i, $i = 1, \cdots (k-1)$. Amb la notació (10.13):

$$G = \langle x_1, \cdots x_n : m_1\, x_1 = \cdots m_k\, x_k = 0 \rangle \tag{10.13}$$

Llavors el grup

$$G = \mathbb{Z}/m_1 \times \cdots \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^{n-k}$$

on $m_1, \cdots m_k$ són els coeficients de torsió, i el nombre de Betti és $\beta(G) = n - k$. Veure la demostració en [3, pàg. 344].

Exemple 10.1 (coef. de torsió i nombre de Betti) [3, ex. 7.11.3, pàg. 340]. El grup

$$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$

té un sistema generador

$$\begin{aligned} S &= \{x_1, x_2\} \\ x_1 &= (1 + 3\mathbb{Z},\, 0 + 12\mathbb{Z}) \\ x_2 &= (0 + 3\mathbb{Z},\, 1 + 12\mathbb{Z}) \end{aligned}$$

doncs qualsevol $x = (a + 3\mathbb{Z},\ b + 12\mathbb{Z}) \in G$ es pot escriure com:

$$x = (a + 3\mathbb{Z},\, b + 12\mathbb{Z}) = \\ a\,(1 + 3\mathbb{Z},\, 0 + 12\mathbb{Z}) + b\,(0 + 3\mathbb{Z},\, 1 + 12\mathbb{Z}) = \\ a\,x_1 + b\,x_2$$

Per altra banda, $r = (m_1,\, m_2) \in R(S)$ sii:

$$m_1\,x_1 + m_2\,x_2 = 0 \Rightarrow \\ (m_1 + 3\mathbb{Z},\, m_2 + 12\mathbb{Z}) = (0 + 3\mathbb{Z},\, 0 + 12\mathbb{Z}) \Rightarrow \\ m_1 \in 3\mathbb{Z},\, m_2 \in 12\mathbb{Z}$$

D'on, per exemple, tenim el conjunt de relacions de $R(S)$:

$$R = \{r_1, r_2\} \\ r_1 = (3,\, 0) \\ r_2 = (0,\, 12)$$

Fent servir la notació (10.13):

$$G = \langle x_1, x_2 : 3\,x_1 = 12\,x_2 = 0\rangle$$

De la proposició 10.1 tenim que els coeficients de torsió de G són $3, 12$ i el nombre de Betti $\beta(G) = n - k = 2 - 2 = 0$.

En general, els generadors i relacions de G no estaran en la forma de la proposició 10.1. A continuació veurem un mètode per aconseguir-ho. Primer, però, veiem quines transformacions podem fer amb els sistema generador.

Proposició 10.2 Sigui G un grup abelià finitament generat amb

$$S = \{x_1, \cdots x_n\}$$

1. Canviant x_i per $-x_i$ s'obté un conjunt generador de G.
2. Siguin $\lambda_2, \cdots \lambda_n$ nombres enters. Canviant x_1 per

$$y_1 = x_1 + \lambda_2\,x_2 + \cdots + \lambda_n\,x_n \tag{10.14}$$

s'obté un nou conjunt generador de G.

Veure la demostració en [3, pàg. 345].

Proposició 10.3 Algorisme per a calcular el nombre de Betti i els coeficients de torsió [3, pro. 7.14, pàg. 347].

Sigui G un grup abelià finitament generat i (S,R) una presentació de G mitjançant un sistema de generadors i un sistema complert de relacions:

$$S = \{x_1, \cdots x_n\} \\ R = \{r_1, \cdots r_k\} \\ r_i = (a_{i1}, \cdots a_{in}),\ i = 1, \cdots k.$$

Definim la **matriu de G respecte la presentació** (S,R)

$$M(S,R) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix} \tag{10.15}$$

Es tracta de transformar la matriu (10.15) en una matriu:

$$M(S',R') = \begin{bmatrix} m_1 & \cdots & 0 & 0 & \cdots 0 \\ 0 & \cdots & 0 & 0 & \cdots 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & m_k & 0 & \cdots 0 \end{bmatrix} \tag{10.16}$$

on m_i divideix m_{i+1}, $i = 1, \cdots (k-1)$, aplicant els canvis de la proposició 10.2. Llavors, els generadors S' que resulten amb les relacions $r_i = (0, \cdots, m_i, \cdots, 0)$ generen G. Per tant, de la proposició 10.1, $m_1, \cdots m_k$ són els coeficients de torsió, i el nombre de Betti és $\beta(G) = n - k$.

1. Permutar les columnes (equival a renombrar els generadors) i canviar x_1 per $-x_1$, és a dir, canviar el signe dels elements de la primera columna (si cal) per tenir $a_{11} > 0$. A continuació posem els coeficients a_{1j}, $j = 2, \cdots n$ en la forma:

$$a_{1j} = \lambda_j\,a_{11} + b_{1j},\ j = 2, \cdots n,\ 0 \le b_{1j} < a_{11} \tag{10.17}$$

Si a_{1j} ja és múltiple de a_{11} ($b_{1j} = 0$), aquest pas és innecessari. Tenint en compte la proposició 10.2.2 tenim que $y_1 = x_1 + \lambda_2\,x_2 + \cdots \lambda_n\,x_n$ és un generador, per tant:

$$a_{11}\,y_1 + b_{12}\,x_2 + \cdots b_{1n}\,x_n = 0$$

Per actualitzar les altres relacions amb el nou sistema de generadors haurem de canviar $a_{ij} = \lambda_j\,a_{i1} + b_{ij}$, d'on $b_{ij} = \lambda_j\,a_{i1} - a_{ij}$. Així obtenim la matriu:

$$M(S',R') = \begin{bmatrix} a_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

on s'ha restat a columna j λ_1 vegades la columna 1. Després agafem la columna j que té el menor b_{1j} en valor absolut, diferent de 0 (és a dir $0 < b_{1j} < a_{11}$) i permutem les columnes 1 i j (equival a renombrar els generadors). Si b_{1j} divideix els altres elements de la fila 1, continuem amb el següent pas, altrament repetint el procés.

2. Ara repetim el procés anterior, però per la primera columna. És a dir, posem els coeficients $a_{i1},\ j = 2,\cdots k$ en la forma (notar que per simplificar la notació, denotem els elements de M després del pas anterior per a_{ij}):

$$a_{i1} = \lambda_i\, a_{11} + c_{i1},\ i = 2,\cdots k,\ 0 \leq c_{i1} < a_{11} \tag{10.18}$$

És a dir, restar a la fila i λ_i vegades la fila 1. Si c_{i1} ja és múltiple de a_{11} ($c_{i1} = 0$), aquest pas és innecessari. Tenint en compte la proposició 10.2.2 tenim que

$$\begin{aligned} r'_1 &= r_1 \\ r'_i &= r_i - \lambda_i\, r_1,\ i = 2,\cdots k \end{aligned}$$

és un sistema generador minimal de $R(S)$. Ara continuem igual que el pas anterior per aconseguir que $a_{i1},\ i = 2,\cdots k$ sigui un múltiple de a_{11}, és a dir $a_{i1} = \mu_i\, a_{11},\ i = 2,\cdots k$. Això ho podem fer permutant les files (equival a renombrar els generadors i relacions). Com que de la proposició 10.2.2 es té que

$$\begin{aligned} r'_1 &= r_1 \\ r'_i &= r_i - \mu_i\, r_1,\ i = 2,\cdots k \end{aligned}$$

és un sistema generador, apliquem aquestes operacions per deixar:

$$M(S',R') = \begin{bmatrix} a_{11} & b_{12} & \cdots & b_{1n} \\ 0 & b_{k2} & \cdots & b_{kn} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

i a continuació retem múltiples de la primera columna de les altres per aconseguir:

$$M(S',R') = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

3. Ara hem d'aconseguir que a_{11} en la matriu anterior divideixi tots els altres elements no nuls de la matriu. Per exemple, si a_{11} no divideix b_{22}, llavors apliquem el mètode del primer pas agafant els elements $(a_{11}, b_{22}, \cdots b_{2,k})$.

4. Repetim els passos anteriors a la submatriu:

$$\begin{bmatrix} b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots \\ b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

5. Reiterem el procés anterior fins aconseguir la forma (10.16) desitjada.

Resumint l'algorisme anterior, es tracta d'aconseguir la forma desitjada (10.16) amb les operacions: canvi de signe dels elements d'una columna, permutació de files o columnes, i resta de múltiples de files a altres files, o columnes a altres columnes.

Exemple 10.2 (coef. de torsió i nombre de Betti) [3, ex. 7.14.4, pàg. 353] Donat el grup amb presentació:

$$\begin{aligned} G = \langle x_1,x_2,x_3,x_4 : \\ 6\,x_2 - 9\,x_3 - 3\,x_4 &= \\ 12\,x_1 + 24\,x_2 + 9\,x_3 + 9\,x_4 &= \\ 30\,x_1 + 42\,x_2 + 45\,x_3 + 27\,x_4 &= 0 \rangle \end{aligned}$$

Calcular els coef. de torsió i el nombre de Betti.

Solució Aplicant el mètode anterior tenim:

$$\begin{bmatrix} 12 & 24 & 9 & 9 \\ 30 & 42 & 45 & 27 \\ 0 & 6 & -9 & -3 \end{bmatrix} \to \begin{bmatrix} 3 & 15 & 0 & 9 \\ 3 & -3 & 18 & 27 \\ 3 & 15 & -6 & -3 \end{bmatrix} \to \begin{bmatrix} 3 & 15 & 0 & 9 \\ 0 & -18 & 18 & 18 \\ 0 & 0 & -6 & -12 \end{bmatrix} \to \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & -18 & 0 & 0 \\ 0 & 0 & -6 & -12 \end{bmatrix} \to \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 18 & 0 \end{bmatrix}$$

D'on tenim:

$$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}$$

amb coeficients de torsió 3,6,18 i nombre de Betti $\beta(G) = 1$.

Capítol 11
Anells

Definició 11.1 Anell (*ring*) és un conjunt A amb 2 operacions (suma i producte) que compleixen:

1. Amb la suma A es un grup commutatiu. L'element neutre de la suma es 0 i denotarem $A^* = A \setminus \{0\}$.

2. El producte té la propietat associativa.

3. El producte té la propietat distributiva sobre la suma. És a dir, $(x + y)\, z = x\, z + y\, z,\ \forall x,y,z \in A$.

Si el producte té la propietat commutativa es diu **Anell commutatiu**.

Definició 11.2 Anell unitari (*unitary ring*) És un anell A en el que el producte té element neutre (*unity*) en A^*. L'element neutre el denotarem per 1.

Definició 11.3 Unitat (*unit*) d'un anell unitari A és un element $x \in A$ que té element invers $y = x^{-1} \in A$ respecte el producte. És a dir, $x\,y = 1$. Notar que, en cas d'existir, l'invers d'un element és únic. El conjunt de totes les unitats de A es denota per $U(A)$ i és un grup per el producte.

Exemple 11.1 (anells) [2, pàg 238]

- $\mathbb{Z}$ és un anell commutatiu unitari amb l'addició i multiplicació amb unitats 1 i -1.
- $\mathbb{Z}_n$ és un anell commutatiu unitari amb l'addició i multiplicació mòdul n.
- $\mathbb{Z}[x]$ (polinomis de coeficients enters i variable real) és un anell commutatiu unitari amb l'addició i multiplicació de polinomis amb unitat $f(x) = 1$.
- El conjunt $M_2(\mathbb{Z})$ de les matrius 2×2 d'enters és un anell (no commutatiu) amb unitat $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- $2\,\mathbb{Z}$ (conjunt dels enters parells) és un anell commutatiu sense unitats.
- **Anell d'enters de Gauss (*ring of Gaussian integers*)** $\mathbb{Z}[i]$ és l'anell commutatiu unitari amb element neutre del producte igual a 1 format per el nombres complexes $a + b\,i$, on $a,b \in \mathbb{Z}$. Les unitats són 1 i -1.
- $A = C(\mathbb{R},\mathbb{R})$ de funcions continues reals de variable real és un anell commutatiu unitari amb element neutre del producte igual a la funció constant $f(x) = 1$. Les operacions són $(f + g)(x) = f(x) + g(x)$ i $(f\,g)(x) = f(x)\,g(x)$.

Definició 11.4 Subanell (*subring*) [2, pàg. 240] és un subconjunt S d'un anell A tal que és anell amb les mateixes operacions que A.

Test de subanell [2, pàg. 240] Un subconjunt no buit S d'un anell A és subanell si és tancat amb l'operació resta i multiplicació. És a dir $a - b \in S$, $a\,b \in S$ $\forall a,b \in S$.

Notar que $\{0\}$ i A són subanells d'un anell A.

Exemple 11.2 (subanell de $\mathbb{Z}_{12}$)
$\{0, 3, 6, 9\}$ és un subanell de $\mathbb{Z}_{12}$:

$$\begin{aligned}
0 - 3 = -3 = 9 \quad &(\mathrm{mod}\,12),\\
0 - 6 = -6 = 6 \quad &(\mathrm{mod}\,12),\\
0 - 9 = -9 = 3 \quad &(\mathrm{mod}\,12),\\
3 - 6 = -3 = 9 \quad &(\mathrm{mod}\,12),\\
3 - 9 = -6 = 6 \quad &(\mathrm{mod}\,12),\\
6 - 9 = -3 = 9 \quad &(\mathrm{mod}\,12),\\
3 \cdot 3 = 9 \quad &(\mathrm{mod}\,12),\\
3 \cdot 6 = 18 = 6 \quad &(\mathrm{mod}\,12),\\
3 \cdot 9 = 27 = 3 \quad &(\mathrm{mod}\,12),\\
6 \cdot 6 = 36 = 0 \quad &(\mathrm{mod}\,12),\\
6 \cdot 9 = 54 = 6 \quad &(\mathrm{mod}\,12),\\
9 \cdot 9 = 81 = 9 \quad &(\mathrm{mod}\,12).
\end{aligned}$$

Propietats 11.1 dels anells

Sigui l'anell A i a,b,$c \in A$

1. $a\,0 = 0\,a = 0$
2. $a\,(-b) = (-a)\,b = -(a\,b)$
3. $(-a)\,(-b) = a\,b$
4. $a\,(b - c) = a\,b - a\,c$ i $(a - b)\,c = a\,c - b\,c$

Si A és unitari:

5. $(-1)\,a = -a$
6. $(-1)\,(-1) = 1$

Demostració. [2, pàg. 239] $0 + a\,0 = a\,0 = a\,(0 + 0) = a\,0 + a\,0$ i per el teorema de cancel·lació (veure 2.2, pàg. 3) $0 = a\,0$. □

Definició 11.5 Cos és un anell K tal que K^* amb el producte és un grup. Amb altres paraules, un cos és un anell unitari K on tot element no zero és unitat, és a dir $U(K) = K^*$.

Normalment ens interessarem per un **cos commutatiu**, que coincideix amb la definició de *field*, definit a continuació.

Definició 11.6 *Field* [2, pàg. 250] és un anell unitari commutatiu on tot element no zero és unitat, és a dir $U(K) = K^*$. Per exemple, els conjunts Q, $\mathbb{R}$, $\mathbb{C}$ dels racionals, reals i complexes, són cossos commutatius (*fields*).

NOTA: alguns autors defineixen *cos* afegint a la definició 11.5 la condició d'anell commutatiu. En aquest cas, cos coincideix amb la definició de *field*.

Definició 11.7 Divisor de zero (*zero-divisor*) És un element $x \neq 0$, $x \in A^*$ tal que $x\,y = 0$ per algun $y \neq 0$, $y \in A^*$.

Definició 11.8 Domini d'integritat (*integral domain*) És un anell unitari i commutatiu que no té divisors de zero.
Una propietat fonamental d'un domini d'integritat és la cancel·lació (veure el teorema 2.2, pàg. 3). És a dir: $b\,a = c\,a \Rightarrow b = c$.

Demostració. $b\,a = c\,a \Rightarrow (b-c)\,a = 0 \Rightarrow b = c$ perquè a no és divisor de 0. □

Exemple 11.3 ($\mathbb{Z}_n$) $\mathbb{Z}_n$ és un anell commutatiu unitari amb l'addició i multiplicació mòdul n amb unitats:

$$U(\mathbb{Z}_n) = \{0 < k < n \ : \ \gcd(k,n) = 1\} \qquad (11.1)$$

Clarament, si $\gcd(k,n) = 1$ llavors existeixen $a,b \in \mathbb{Z}$ tals que $k\,a + n\,b = k\,a = 1 \pmod n$. Per tant, k és unitat. Notar que $\mathrm{o}(U(\mathbb{Z}_n)) = \phi(n)$ (veure la definició de $\phi(n)$ en l'apèndix C, pàg. 38)). Deduïm, doncs, que només en cas que n sigui primer tots els elements de $\mathbb{Z}_n$ seran unitats i, per tant, $\mathbb{Z}_n$ serà un domini d'integritat.
Si n no és primer, tots els elements de $\mathbb{Z}_n$ que no són unitats són divisors de zero. Clarament, si $\gcd(k,n) = d$, $d > 1$ llavors $k = s\,d$ i $k\,(n/d) = s\,d\,(n/d) = s\,n = 0 \pmod n$.

Definició 11.9 producte d'anells Siguin els anells A, B anells unitaris commutatius. Llavors $C = A \times B$ és un anell unitari commutatiu amb les operacions

$$(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1,b_1)\,(a_2,b_2) = (a_1\,a_2, b_1\,b_2)$$

i $0_C = (0_A,0_b)$, $1_C = (1_A,1_B)$. El producte d'anells sempre té divisors de zero, doncs $(a,0)\,(0,b) = (0,0)$, amb $a \neq 0$, $b \neq 0$.
Una propietat del producte d'anells és

$$U(C) = U(A) \times U(B) \qquad (11.2)$$

on $U(A)$ és el conjunt de les unitats d'A (veure la def. 11.3).

Teorema 11.1 Un domini d'integritat finit és un cos commutatiu (*field* [2, pàg. 251]). Esborrany de la demostració: Al ser finit hi ha d'haver $a^i = a^j$ per $i > j$. Per tant, a^{i-j-1} és l'element invers d'a, doncs $a^{i-j-1}\,a = 1$. Notar que un domini d'integritat infinit no és necessàriament un cos.

Corol·lari 11.1 Per a un nombre primer p, $\mathbb{Z}_p$ és un cos commutatiu (*field*).

Demostració. Per el teorema 11.1 basta provar que $\mathbb{Z}_p$ és un domini d'integritat (no té divisors de zero). Si $a,b \in \mathbb{Z}_p$ amb $a\,b = 0$, llavors $a\,b = k\,p$ per algun enter k. Llavors, per el lema d'Euclidi (veure l'apèndix 13.10, pàg. 38), p dividiex a, o b, que no és possible. Per tant, $a = 0$ o $b = 0$. Corroborem així el que ja havíem obtingut en l'exemple 11.3. □

Definició 11.10 Cos de fraccions d'un domini d'integritat És un anell unitari i commutatiu que no té divisors de zero.

Definició 11.11 Característica d'un anell, $\mathrm{char}\,A$. Sigui un anell A. És el menor enter n tal que $n\,x = x \overset{n}{\cdots} + x = 0$, $\forall x \in A$. Si no existeix, es diu que la característica de A és 0.

Exemple 11.4 (característica d'un anell) Per el subanell $A = \{0,3,6,9\}$ de $\mathbb{Z}_{12}$ es té $4\,x = 0\ \forall x \in A$. Per tant, $\mathrm{char}\,A = 4$.
Anàlogament, $\mathrm{char}\,\mathbb{Z} = 0$ i $\mathrm{char}\,\mathbb{Z}_n = n$.

Teorema 11.2 (Característica d'un anell unitari) Sigui un anell unitari A. Si 1 té ordre infinit respecte l'addició, aleshores la característica de A és 0. Altrament, si l'ordre és n, la característica és n.

Demostració. Si 1 té ordre n per a l'addició es té $1 \overset{n}{\cdots} + 1 = 0$. Per tant:

$$\begin{aligned} n\,x &= x \overset{n}{\cdots} + x = \\ &= 1\,x \overset{n}{\cdots} + 1\,x = \\ &= (1 \overset{n}{\cdots} + 1)\,x = \\ &= (0)\,x = 0 \end{aligned}$$

□

Teorema 11.3 (Caract. d'un domini d'integritat) La característica d'un domini d'integritat és 0 o un nombre primer.

Demostració. Suposem que 1 té ordre n on n no és primer. Aleshores $n = s\,t$, $1 < s \leq t < n$, i $0 = n\,1 = (s\,t)\,1 = (s\,1)\,(t\,1)$. Això implica que $s\,1 = 0$ o $t\,1 = 0$. Però això no és possible perquè n és el menor enter tal que $n\,1 = 0$. Per tant, $n = s\,t$, $1 < s \leq t < n$, no és possible, és a dir, n és primer. □

Veure més exemples d'anells i propietats en la taula 13.2 de [2, pàg 254].

11.1 Ideals

Motivació: Els ideals són l'equivalent als conjunts normals dels grups (veure el capítol 5, pàg. 13) per als anells. Això permet definir el grup quocient d'un grup (*factor group*, veure el capítol 6, pàg. 15), per als anells (anomenat anell quocient, *factor ring*, que es veu més abaix).

Definició 11.12 [2, pàg. 262] **Ideal** (*ideal*) és un subanell I d'un anell A tal que per $\forall r \in A$ i $\forall s \in I$ es té $r\,s \in I$ i $s\,r \in I$. És a dir, un ideal absorbeix els elements d'A: $\forall r \in A$: $r\,I \subseteq I$, $I\,r \subseteq I$.

En [4, pàg. 25] es defineix ideal amb la definició equivalent: Sigui A un anell commutatiu unitari. Un ideal és un subconjunt $I \subset A$ tal que:
1. I és subgrup de A per a la suma (en particular $0 \in I$),
2. $\forall r \in A$ i $\forall s \in I$ es té $r\,s \in I$.

Notar que
- I és un subgrup normal d'A (veure 5.1, pàg. 13).
- $\{0\}$ i A són ideals d'un anell A. $\{0\}$ s'anomena l'**ideal trivial**.
- A s'anomena l'**ideal impropi**.
- Es diu que un ideal I és propi d'un anell A, si és un subanell diferent d'A.
- En general, no és cert que $s\,r \in I \Rightarrow s \in I$ o $r \in I$. Si es compleix aquesta condició es diu que I és un ideal primer (veure la definició d'ideal primer 11.18, pàg. 29).

Test d'ideal [2, pàg. 262] Un subconjunt no buit I d'un anell A és un ideal si
1. $a - b \in I, \forall a, b \in I$. Aquesta condició és anàloga a $a + b \in I, \forall a, b \in I$, doncs $-b = (-1)\,b \in I$, perquè $-1 \in A$ i $b \in I$.
2. $r\,a \in I, a\,r \in I, \forall r \in I, \forall a \in A$.

Teorema 11.4 (si $1 \in I$ llavors $I = R$) Sigui I un ideal d'un anell R i $1 \in I$. Llavors $I = R$.

Demostració. Si $1 \in I$ llavors $\forall r \in R$ tenim $1\,r \in I \Rightarrow r \in I \Rightarrow I = R$. □

Operacions amb Ideals. Siguin I, J ideals d'un anell unitari commutatiu A. Les següent operacions també donen un ideal d'A.
- Suma: $I + J = \{x + y \ : \ x \in I, y \in J\}$. Notar que $I + J = I \cup J$.
- Producte: $I\,J = \{x\,y \ : \ x \in I, y \in J\}$.
- Intersecció: $I \cap J$.

Definició 11.13 ideal finitament generat Sigui A un anell commutatiu unitari i $L = \{x_1, \cdots x_r\} \subset A$. S'anomena l'ideal I generat per L a

$$I = A\,x_1 + \cdots A\,x_r = \left\{ \sum_{i=1}^{r} a_i\,x_i \ : \ a_i \in A \right\}. \quad (11.3)$$

En el llibre de l'UNED es fa servir la notació $I = (x_1, \cdots x_r)$ (veure la definició [4, def 1.18, pàg 27]). Si $r = 1$ s'anomena **ideal principal**. Degut a la seva importància es defineix a continuació.

Definició 11.14 ideal principal Sigui A un anell commutatiu unitari i $a \in A$. El conjunt:

$$a\,A = \{r\,a \ : \ r \in A\} \quad (11.4)$$

és un ideal de A anomenat l'ideal principal d'A generat per a.
NOTA: En el llibre de l'UNED es fa servir la notació $I = (a)$. En aquests apunts, però, es farà servir la notació del Gallian $I = \langle a \rangle$ per referir-se a l'ideal principal generat per a [2, pàg 263], per evitar confusions amb els parèntesi. Notar que la notació $\langle a \rangle$ també es fa servir per el grup cíclic generat per a (veure la definició D, pàg. 39). Tanmateix el significat d'$\langle a \rangle$ s'entén sempre del context.

Exemple 11.5 (ideal principal $\langle x \rangle$) Sigui $\mathbb{R}[x]$ el conjunt de tots el polinomis amb coeficients reals. sigui I el subconjunt d'$\mathbb{R}[x]$ amb el terme constant igual a zero. Llavors I és un ideal d'$\mathbb{R}[x]$ amb $I = \langle x \rangle$. Clarament, per a qualsevol polinomi $p(x) \in \mathbb{R}[x]$, $x\,p(x) \in I$.

Exemple 11.6 (ideal principal $\langle x,2 \rangle$) Sigui I el conjunt de $\mathbb{Z}[x]$ format per els polinomis que tenen el terme constant igual a un nombre parell. Llavors I és l'ideal generat per $I = \langle x,2 \rangle$. Clarament, per a qualssevol polinomis $p(x)$,$g(x) \in \mathbb{Z}[x]$, $x\,p(x) + 2\,g(x) \in I$.

Exemple 11.7 (ideal $m\,\mathbb{Z}$) Per a qualsevol enter m, $\langle m \rangle = m\,\mathbb{Z} = \{m\,x \ : \ x \in \mathbb{Z}\} = \{\cdots, -2\,m, -m, 0, m\,2, m, \cdots\}$ és un ideal principal de $\mathbb{Z}$. Com que m i $-m$ generen el mateix ideal, es pot establir una bijecció entre els ideals de $\mathbb{Z}$ i els enters no negatius. En el llibre de l'UNED [4] es fa servir la notació: $J_m = (m) = m\,\mathbb{Z}$.

Proposició 11.1 (ideals d'un cos) [4, pàg 28] En un cos K només hi ha els ideals $\{0\}$ i K. Recíprocament, si un anell només té els ideals $\{0\}$ i K, aleshores K és un cos.

Definició 11.15 Anell quocient (factor ring) Sigui A un anell unitari commutatiu i $I \subset A$ un ideal propi d'A. Definim (veure el teorema 6.1, pàg. 15):

$$A/I = \{a+I : a \in A\},\ a+I = \{a+r : r \in I\} \quad (11.5)$$

que és un anell commutatiu amb les operacions:

$$I_1 + I_2 = \{r_1 + r_2 \ : \ r_1 \in I_1, r_2 \in I_2\} \quad (11.6)$$
$$I_1 \cdot I_2 = \{r_1 \cdot r_2 \ : \ r_1 \in I_1, r_2 \in I_2\} \quad (11.7)$$

on l'element neutre de la suma és $0 + I$, i del producte $1 + I$.

Relació d'equivalència Notar que un Ideal I permet definir la relació d'equivalència (veure la definició 1.1, pàg. 1):

$$a \equiv b \text{ sii } a - b \in I \quad (11.8)$$

El conjunt $a + I = \{a + r \ : \ r \in I\}$ és una relació d'equivalència de l'element $a \in A$. Per aquesta relació d'equivalència també es fa servir la notació

$$a \bmod I = a + I = \{a + r : r \in I\}. \quad (11.9)$$

Per això, l'anell A/I s'anomena **anell de classes de restes mòdul** I [4, pàg 26]. Notar que:

$$I_1 = a_1 + I = \{a_1 + r : r \in I\}$$
$$I_1 + I_2 = (a_1 + I) + (a_2 + I) = (a_1 + a_2) + I = \{a_1 + a_2 + r : r \in I\}$$
$$I_1\, I_2 = (a_1 + I)\,(a_2 + I) = (a_1\, a_2) + I = \{a_1\, a_2 + r : r \in I\}$$

Definició 11.16 (representants de les classes) (*coset representatives*) Sigui A un anell unitari commutatiu i $I \subset A$ un ideal propi d'A. Els **representants de l'anell quocient** A/I és el conjunt d'elements $a_i \in A$ que donen lloc a diferents elements de $A/I = \{a_i + I : a_i \in A\},\ a_i + I = \{a_i + r : r \in I\}$.

Exemple 11.8 (representants d'un anell quocient) [2, ex. 11, pàg 265] Considerar l'anell $A = \mathbb{Z}[i]/\langle 2-i\rangle$, on $\mathbb{Z}[i]$ és l'anell d'enters de Gauss (veure la definicio 11.1) i $\langle 2-1\rangle$ l'ideal principal generat per $2-i$ (veure la definició 11.14). Hem de buscar els elements (representants) $a + b\,i \in \mathbb{Z}[i]$ tals que donin lloc a conjunts $a + b\,i + \langle 2 - i\rangle$ diferents. El fet de que $2 - i + \langle 2 - i\rangle = 0 + \langle 2 - i\rangle$ implica que, pel que fa els representats, $2 - i = 0$. És a dir, $2 = i \Rightarrow 4 = -1 \Rightarrow 5 = 0$. Es conclou doncs, que els elements de $A = \mathbb{Z}[i]/\langle 2 - i\rangle$ seran de la forma $a + \langle 2 - i\rangle$, on a és un enter. En particular: $A = \mathbb{Z}[i]/\langle 2 - i\rangle = \{0+\langle 2-i\rangle, 1+\langle 2-i\rangle, 2+\langle 2-i\rangle, 3+\langle 2-i\rangle, 4+\langle 2-i\rangle\}$. És a dir, $A = \mathbb{Z}[i]/\langle 2 - i\rangle$ és isomorf amb l'anell $\mathbb{Z}_5$.

Definició 11.17 Ideal maximal [4, pàg. 29] Sigui A un anell unitari commutatiu i $I \in A$ un ideal. I és maximal si compleix qualsevol de les següents condicions equivalents:

1. A/I és un cos.
2. I és un ideal propi i no hi ha altre ideal propi que el conté.

Definició 11.18 Ideal primer Sigui A un anell unitari commutatiu i $I \in A$ un ideal. I és primer si compleix qualsevol de les següents condicions equivalents:

1. A/I és un domini d'integritat.
2. I és un ideal propi i $\forall x,y \in A$, si $x\,y \in I$ llavors $x \in I$ o $y \in I$.

Demostració. Si $x\,y \in I \Rightarrow x\,y + I = I = 0 + I = (x + I)\,(y + I)$. Per tant, pel que fa els representats, $x\,y = 0$. Al ser A/I un domini d'integritat, o bé $x = 0 \Rightarrow x + I = 0 + I \Rightarrow x \in I$, o bé $y = 0 \Rightarrow y + I = 0 + I \Rightarrow y \in I$. □

Teorema 11.5 (R/I DI sii I primer) [2, pàg. 268] Sigui R un anell commutatiu amb unitat i I un ideal d'R. Llavors R/I és un domini d'integritat (DI) sii I és un ideal primer.

Demostració. Sigui D/I DI amb $a\,b \in I$. Llavors $(a + I)(b + I) = a\,b + I = I$, l'element 0 d'$R/I$. Per tant, o bé $a + I = I$ o $b + I = I$, és a dir, o bé $a \in I$ o $b \in I$. Així doncs, I és primer. Per provar el contrari, s'ha de provar que si I és primer, R/I no té divisors de 0. Però si $(a+I)(b+I) = I$, o bé $a+I = I$ o $b+I = I$. Per tant, $(a + I)$ o bé $(b + I)$ és l'element 0 d'R/I. □

Teorema 11.6 (R/I és un cos commutatiu sii I maximal) [2, pàg. 268] Sigui R un anell commutatiu amb unitat i I un ideal d'R. Llavors R/I és un cos commutatiu (*field*) sii I és un ideal maximal.

11.2 Homomorfismes

Definició 11.19 Homomorfisme entre anells De forma semblant a l'homomorfisme entre grups (veure la definició 7.1, pàg. 16) un homomorfisme $f : A \to B$ entre dos anells unitaris commutatius A i B és una aplicació que compleix $\forall a,b \in A$:

1. $f(a + b) = f(a) + f(b)$
2. $f(a\,b) = f(a)\,f(b)$
3. $f(1_A) = 1_B$

Definició 11.20 (nucli d'un homomorfisme) Sigui $f : A \to B$ un homomorfisme entre anells unitaris commutatius. De forma anàloga al nucli d'un homomorfisme entre grups (veure la definició en 7.2, pàg. 16), es defineix el **nucli de l'homomorfisme entre anells** (*kernel*) i es denota per $\ker f$ a l'ideal:

$$\ker f = \{x \in A \ : \ f(x) = 0\}. \tag{11.10}$$

Com que ha de ser $f(0) = 0$, es té, $0 \in \ker f$, i el nucli amb el menor nombre d'elements que es pot tenir és $\ker f = \{0\}$.

Definició 11.21 (imatge d'un homomorfisme) Sigui $f : A \to B$ un homomorfisme entre anells unitaris commutatius. S'anomena **imatge de l'homomorfisme entre anells** i es denota per $\operatorname{im} f$ a l'anell:

$$\operatorname{im} f = \{y \in B \ : \ \exists x \in A \text{ amb } y = f(x)\} \tag{11.11}$$

Igual que en l'homomorfisme entre grups es defineixen els següents tipus d'homomorfismes:

Definició 11.22 (Tipus d'homomorfismes) Existeixen tipus especials d'homomorfismes segons f sigui:

- Injectiva (*one-to-one*), i es diu **monomorfisme**.
- Surjectiva (*onto*), i es diu **epimorfisme**.
- Injectiva i surjectiva (bijectiva), i es diu **isomorfisme**.

Notar que entre homomorfisme i isomorfisme hi ha diferències importants. Un homomorfisme pot simplificar un anell, mantenint algunes característiques, mentre dos anells isomòrfics són essencialment el mateix, des del punt de vista algebraic.

Teorema 11.7 ($\ker f$ és un ideal propi)
[4, pàg. 33]. Sigui $f : A \to B$ un homomorfisme entre anells unitaris commutatius. Com que $f(1_A) = 1_B \neq 0$, $\ker f$ **és un ideal propi d'**A (és a dir, $\ker f \subset A$, $\ker f \neq A$). Veure la figura 11.1, i comparar amb la figura 7.1, pàg. 17.

A més, es verifica que f és injectiu (és a dir, és un monomorfisme) sii $\ker f = \{0\}$. La demostració és anàloga el teorema equivalent per monomorfisme entre grups (veure el teorema 7.2, pàg. 16).

Una conseqüència d'aquest teorema és que si $f : K \to B$ és un homomorfisme entre anells unitaris i K és un cos, llavors f és un necessàriament un monomorfisme, doncs $\ker f$ és un ideal propi de K, i K només té els ideals $\{0\}$ i K (veure la proposició 11.1). Per tant, ha de ser $\ker f = \{0\}$.

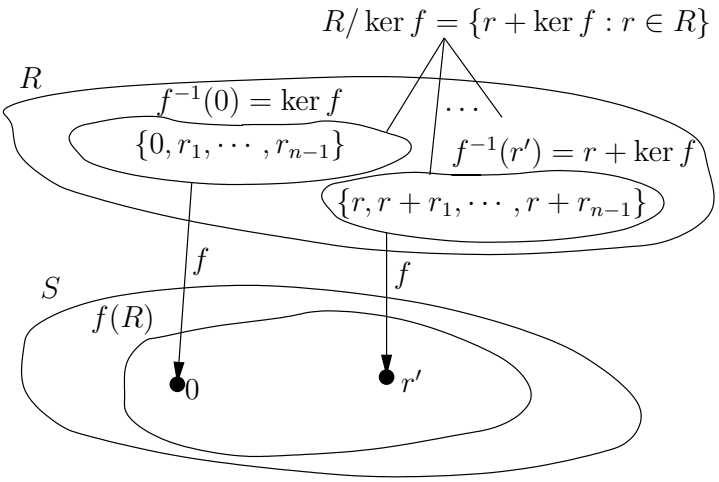


Figura 11.1: Propietats d'un homomorfisme entre anells.

Propietats 11.2 dels monomorfismes entre anells

[2, pàg. 283] Sigui $f : A \to B$ un homomorfisme entre anells unitaris commutatius.

1. $f(n\,a) = n\,f(a)$, $a \in A$, $n \in \mathbb{Z}$.
2. Si S és un subanell de A, llavors $f(S)$ és un subanell de B.
3. Si I és un ideal de A i f és surjectiva (epimorfisme), llavors $f(I)$ és un ideal de B.
4. Si I_B és un ideal de B, llavors $f^{-1}(B)$ és un ideal de A.
5. Si A és commutatiu, llavors $f(B)$ també ho és.
6. Si A té unitat 1, $B \neq \{0\}$ i f és surjectiva (epimorfisme), llavors $f(1)$ és la unitat de B.
7. f és un isomorfisme sii és surjectiva (epimorfisme) i $\ker f = \{0\}$.

Teorema 11.8 (primer teoria d'isomorfia per anells)
Sigui $f : R \to S$ un homomorfisme entre anells. Llavors l'aplicació:

$$r + \ker f \to f(r) \tag{11.12}$$

és un isomorfisme, és a dir, $R/\ker f \cong \operatorname{im} f = f(R)$. Veure la figura 11.1.

Teorema 11.9 (els ideals són kernel)
Tot ideal I d'un anell R és el kernel d'un homomorfisme entre anells d'R. En particular, ho és de l'**homomorfisme natural**:

$$f : R \to R/I : r \to r + I \tag{11.13}$$

Clarament, $\forall a \in I \ : \ a + I = I$. Per tant, pel que fa els representants, $\forall a \in I \ : \ a = 0$, d'on $\ker f = I$.

Exemple 11.9 (homomorfisme) [2, pàg. 284] L'aplicació

$$f : \mathbb{Z}[x] \to \mathbb{Z} : p(x) \to p(0)$$

és un homomorfisme entre anells amb

$$\ker f = \{p(x) \in \mathbb{Z}[x] \ : \ f(0) = 0\} = \langle x \rangle$$

(veure l'exemple 11.5, pàg. 28). Del teorema 11.8 tenim $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$. Com que $\mathbb{Z}$ és un domini d'integritat, però no un cos, dels teoremes 11.5 i 11.6 tenim que $\langle x \rangle$ és un ideal primer però no maximal en $\mathbb{Z}[x]$.

Teorema 11.10 (homomorfisme de $\mathbb{Z}$ en un anell) [2, pàg. 284] Sigui R un anell unitari $1 \in R$. L'aplicació:

$$f : \mathbb{Z} \to R : n \to 1\, n \tag{11.14}$$

és un homomorfisme entre anells.

Teorema 11.11 (un anell unitari conté $\mathbb{Z}$ o $\mathbb{Z}_n$) [2, pàg. 284] Sigui R un anell unitari $1 \in R$ amb característica $n > 0$. Llavors R conté un subanell isomorf a $\mathbb{Z}_n$. Si la característica és 0, llavors conté un subanell isomorf a $\mathbb{Z}$.

Demostració. Sigui $\operatorname{char} R = n$, $1 \in R$ i $S = k\,1 \ : \ k \in \mathbb{Z}\}$. Del teorema 11.10 tenim que $f(k) = k\,1$ és un homomorfisme. Com que $\ker f = \langle n \rangle$, on n és l'ordre d'1 amb l'addició i $\mathbb{Z}/\ker f = \mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n \cong S$, per el teorema 11.2, pàg. 27 tenim que també és la característica d'R. Si R té característica 0, llavors $S \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$. □

Teorema 11.12 (F conté $\mathbb{Z}_p$ o Q) [2, pàg. 285] Sigui F un cos commutatiu (*field*). Llavors si la característica d'F és p, F conté un subcos isomorf a $\mathbb{Z}_p$. Altrament, si la característica és 0, F conté un subanell isomorf al cos dels racionals, Q.

Tot i que $\mathbb{Z}$ no és un cos commutatiu, del teorema anterior tenim que està contingut en el cos commutatiu dels racionals. Això motiva el següent teorema:

Definició 11.23 (cos commutatiu quocient) [2, pàg. 286] Sigui D un domini d'integritat. Llavors existeix un cos commutatiu F anomenat **cos quocient** que conté un subanell isomorf a D.

Demostració. (esborrany) Definim

$$F = \{a/b \ : \ a,b \in D, b \neq 0\} \tag{11.15}$$

amb operacions: $a/b + c/d = (a\,d + b\,c)/(b\,d)$ i $(a/b)\,(c/d) = (a\,c)/(b\,d)$. Llavors F és un cos commutatiu. □

Exemple 11.10 (cos quocient) El cos quocient de $\mathbb{Z}[x]$ és:

$$F(x) = \{\frac{f(x)}{g(x)} \ : \ f(x),g(x) \in \mathbb{Z}[x], g(x) \neq 0\}. \tag{11.16}$$

La notació estàndard per aquest cos és $F(x)$.

11.3 Divisibilitat en un anell

En tota aquesta secció es considera un anell A que és domini d'integritat.

Definició 11.24 (Divisibiliat en un anell) Siguin $x,y \in A$ amb $x \neq 0$. Es diu que x divideix y, o que y és divisible per x, o que x és divisor o factor de y, o que y és un múltiple de x, i s'escriu $x \,|\, y$ si existeix $a \in A$ tal que

$$y = a\,x,\ a \in A. \tag{11.17}$$

Propietats 11.3 de la divisibilitat en un anell

1. $x \,|\, y$ sii $y \in \langle x \rangle$, o equivalentment $\langle y \rangle \subset \langle x \rangle$.
2. $\langle x \rangle = \langle y \rangle \Rightarrow$ existeix una unitat $a \in U(A)$ tal que $y = a\,x$.

   Demostració. $\langle x \rangle = \langle y \rangle \Rightarrow y \in \langle x \rangle$ i $x \in \langle y \rangle \Rightarrow y = a\,x$, $x = b\,y \Rightarrow y = a\,b\,y \Rightarrow a\,b = 1$, doncs A és un domini d'integritat. Per tant, a és unitat. □
3. Si un element no nul $y \in A$ no és unitat, denotem $\operatorname{div}(y)$ al conjunt de tots els divisors de y. Tenim que $U(A) \in \operatorname{div}(y)$ i $y\,U(A) \in \operatorname{div}(y)$, doncs si x és unitat:

   $$y = (y\,x^{-1})\,x = a\,x,\ a = y\,x^{-1} \in A,\ x \in U(A),$$
   $$y = x^{-1}\,(y\,x) = a\,(y\,x),\ a = x^{-1} \in A,\ (y\,x) \in y\,U(A).$$

Definició 11.25 (gcd, lcm) (veure la definició per els enters en l'apèndix A) Per $x,y \in A^*$ definim:

- **Màxim comú divisor** (*Greatest Common Divisor,* gcd) $d = \gcd(x,y)$ si $d \,|\, x$, $d \,|\, y$ i d és múltiple de qualsevol altre divisor de x,y.
- **Mínim comú múltiple** (*Least Common Multiple,* lcm): $z = \operatorname{lcm}(x,y)$ si z és múltiple de x i y, i divideix qualsevol altre múltiple de x i y.

Propietats 11.4 del gcd i lcm [4, pàg. 40]

Per un DIP A (veure la definició 11.29), $\forall x,y \in A^*$:

1. $z = \operatorname{lcm}(x,y) \Rightarrow \langle z \rangle = \langle x \rangle \cap \langle y \rangle$.
2. $z = \operatorname{lcm}(x,y) \Rightarrow t = x\,y/z = \gcd(x,y)$.
3. $d = \gcd(x,y) \Rightarrow \langle d \rangle = \langle x \rangle + \langle y \rangle$.

4. Per a un domini d'integritat A

$$\forall x,y \in A^* \ : \ \gcd(x,y) \cdot \operatorname{lcm}(x,y) = x\,y.$$

Definició 11.26 (element irreductible) Si un element no nul $y \in A$ no és unitat i els únics divisors de y són $\operatorname{div}(y) = U(A) \cup y\,U(A)$, es diu que y és **irreductible**.

Definició 11.27 (element primer) Si un element no nul $y \in A$ no és unitat i per $a,b \in A$, $y \,|\, a\,b \Rightarrow y \,|\, a$ o $y \,|\, b$ (és a dir, y genera un ideal primer $\langle y \rangle$, veure la definició d'ideal primer 11.18, pàg. 29), es diu que y és **primer**.

Teorema 11.13 (en un DI primer implica irreductible)
En un domini d'integritat tot element primer és irreductible.

Demostració. Suposar que y és primer i $y = a\,b$. Hem de provar que a o b és una unitat. Com que y és primer, $y \,|\, a$ o $y \,|\, b$. Suposem que $y \,|\, a \Rightarrow a = k\,y = k\,a\,b \Rightarrow 1 = k\,b$, per tant, b és unitat. □

En el cas dels enters les definicions d'element irreductible i primer són equivalents, però veurem que hi poden haver anells irreductibles que no són primers.

Definició 11.28 (domini euclidi) Es diu que un domini d'integritat A és un **domini euclidi, DE** si existeix una aplicació (anomenada *mesura*):

$$\|\cdot\| : A \to \mathbb{N} \tag{11.18}$$

tal que:
1. $\|x\| = 0$ sii $x = 0$.
2. $\|x\,y\| = \|x\|\,\|y\|$.
3. Per $x,y \in A^* \exists r \in A \ : \ y\,|(x - r)$ i $\|r\| < \|y\|$.

Aquesta definició segueix la definicio de la divisió entera, r s'anomena reste i $q \in A \ : \ x - r = q\,y$ quocient.

Proposició 11.2 [4, prop. 2.8, pàg. 38]
Si A és un domini euclidi:

$$U(A) = \{x \in A \ : \ \|x\| = 1\} \tag{11.19}$$

Exemple 11.11 ($\|\cdot\|$)

1. Per $A = \mathbb{Z}$

$$\|k\| = |k| = \begin{cases} k, & \text{si } k \geq 0 \\ -k, & \text{si } k < 0 \end{cases} \tag{11.20}$$

2. Per $A = \mathbb{Z}[i]$ [4, exemple 2.7.2, pàg. 37]

$$\|a + b\,i\| = a^2 + b^2 \tag{11.21}$$

Definició 11.29 (domini d'ideals principals, DIP) És un domini d'integritat on tots els ideals tenen la forma $\langle a \rangle$, és a dir, són ideals principals (veure la definició d'ideal principal en 11.14, pàg. 28).

Teorema 11.14 (en un DIP irreductible ⇒ primer)
En un domini d'ideals principals, DIP, un element és irreductible sii és primer. Veure la demostració en [2, pàg. 324].

Teorema 11.15 (ED ⇒ PID)
[2, pàg. 333] Tot domini Euclidi (ED) és un domini d'ideals principals (PID).

Proposició 11.3 (identitat de Bezout) Si $x,y \in A^*$ generen un ideal principal (per exemple, si A és un DIP), aleshores existeix $d = \gcd(x,y)$ i

$$d = a\,x + b\,y,\ a,b \in A$$

Teorema 11.16 (factors irreductibles)
[4, pàg. 42] Sigui A un domini d'ideals principals, DIP. Per cada $x \in A^*$ que no és unitat existeixen els elements irreductibles únics (anomenats factors irreductibles) $a_1, \cdots a_r$ primers relatius, i els enters únics $n_1, \cdots n_r$ tals que

$$x = a_1^{n_1} \cdots a_r^{n_r} \tag{11.22}$$

Definició 11.30 (domini de factorització única, DFU) és un domini d'integritat que compleix:
1. tot element irreductible és primer,
2. tot element no nul que no sigui unitat és el producte d'elements irreductibles.

Teorema 11.17 (PID ⇒ DFU)
[2, pàg. 329] Tot domini d'ideals principals (DIP) és un domini de factorització única (DFU).
Notar que DE ⇒ DIP ⇒ DFU. Però DFU ⇏ DIP ⇏ DE.

En un DFU sempre existeixen:
- gcd = producte dels factors irreductibles comuns elevats al menor exponent,
- lcm = producte dels factors irreductibles comuns i no comuns elevats al major exponent.

11.3.1 Equacions diofàntiques

Amb dues incògnites són les solucions de [4, pàg. 50]:

$$a\,x + b\,y = c, \quad a,b,c,x,y \in A \tag{11.23}$$

Resolució: Suposem que es compleix una identitat de Bezout:

$$d = \gcd(a,b) = \alpha\, a + \beta\, b, \quad d,\alpha,\beta \in A \tag{11.24}$$

L'equació (11.23) només té solució si $d \mid c$, i podem escriure (11.23) i (11.24) com:

$$a'\, x + b'\, y = c' \tag{11.25}$$
$$\alpha\, a' + \beta\, b' = 1 \tag{11.26}$$

on:

$$a' = a/d,\ b' = b/d,\ c' = d/d$$

Multiplicant (11.25) per α i substituint $\alpha\, a' = 1 - \beta\, b'$, i multiplicant (11.25) per β i substituint $\beta\, b' = 1 - \alpha\, a'$, tenim, respectivament:

$$x = \alpha\, c' + b'(\beta\, x - \alpha\, y)$$
$$y = \beta\, c' - a'(\beta\, x - \alpha\, y)$$

d'on deduïm que les solucions són de la forma:

$$\begin{aligned} x &= \alpha\, c' + b'\, t \\ y &= \beta\, c' - a'\, t \end{aligned} \quad t \in A \tag{11.27}$$

Nota Si A és un subanell de B, les solucions de l'equació (11.24) en B serien simplement:

$$\begin{aligned} u &= \alpha\, c' + b'\, t \\ v &= \beta\, c' - a'\, t \end{aligned} \quad t \in B \tag{11.28}$$

Algorisme d'Euclidi Per a calcular $d = \gcd(a,b)$ l'algorisme (13.9), pàg. 38 es pot generalitzar a un anell A on hi ha definida una aplicació (és un DE) $\|\cdot\| : A \to \mathbb{N}$ com la definida en (11.18). Sigui $a,b \in A$ on $\|a\| > \|b\|$. Posant $x_0 = a$, $x_1 = b$, amb $\|\|$ podem calcular la successió:

$$\begin{aligned} x_0 &= y_1\, x_1 + x_2 \\ x_1 &= y_2\, x_2 + x_3 \\ &\vdots \\ x_{r-2} &= y_{r-1}\, x_{r-1} + x_r \\ x_{r-1} &= y_r\, x_r \end{aligned}$$

d'on és veu que x_r divideix a tots els anteriors x_i. Per tant $\gcd(a,b) = x_r$, és a dir, l'últim reste no nul. És convenient posar els resultats en forma de taula:

	y_1	y_2	$\cdots$	y_{r-1}	y_r
$a = x_0$	$b = x_1$	x_2	$\cdots$	x_{r-1}	x_r
	x_2	x_3	$\cdots$	x_r	

Coeficients de la identitat de Bezout es poden obtenir amb l'algorisme d'Euclidi anterior posant:

$$\begin{aligned} x_2 &= a - y_1\, b \\ x_3 &= x_1 - y_2\, x_2 = \\ &\quad b - y_2(a - y_1\, b) = -y_2\, a + (1 + y_1\, y_2)b \\ &\vdots \\ x_r &= d = \alpha\, a + \beta\, b \end{aligned}$$

11.4 Congruències

Propietats 11.5 de l'anell $\mathbb{Z}$ [4, pàg. 56]:

1. Un enter p és irreductible sii és primer.
2. $\mathbb{Z}$ és un domini de factorització única (veure la definició 11.30).
3. El conjunt dels nombres primers és ∞.
4. $\mathbb{Z}/\langle n\rangle$, $n > 1$ s'anomena **anell de restes mòdul** n. Es denota:

   $$[k] = [k]_n = k + \langle n\rangle = \{k + q\, n \ :\ q \in \mathbb{Z}\} \tag{11.29}$$

   Es fa servir $[k]$ si no hi ha confusió. Notar que un altre representant de $[k]$ és $k = r + q\, n$ on r és el reste per defecte si $k > 0$ o per excés si $k < 0$. És a dir $[k] = [r]$. Per tant, cada classe d'equivalència de $\mathbb{Z}/\langle n\rangle$ està determinada per un representant $0 \le r < n$, i:

   $$\mathbb{Z}/\langle n\rangle = \{[0], [1], \cdots, [n-1]\} \tag{11.30}$$

   $[0]$ i $[1]$ són, respectivament, el 0 i 1 de l'anell $\mathbb{Z}/\langle n\rangle$. Per referir-se als representants de $\mathbb{Z}/\langle n\rangle$ es fan servir les notacions:

   $$k = l \bmod n = l \ (\mathrm{mod}\, n) \tag{11.31}$$

   i es diu que k i l són congruents mòdul n.
5. Dels resultats anteriors tenim que els ideals d'un anell de restes mòdul n estan en bijecció amb els ideals $I \subset \mathbb{Z}$ que contenen $\langle n\rangle$.

Teorema 11.18 (xinès del reste)
Si a, b són primers relatius existeix un isomorfisme d'anells unitaris:

$$f : \mathbb{Z}/\langle a\, b\rangle \to \mathbb{Z}/\langle a\rangle \times \mathbb{Z}/\langle b\rangle :$$
$$[k]_{ab} \to ([k]_a, [k]_b) \tag{11.32}$$

Proposició 11.4 (unitats dels anells de restes)
(veure [4, pàg. 61]) Si $n > 1$ i $k \in \mathbb{Z}$ les següents condicions són equivalents:

- $[k] \in U(\mathbb{Z}/\langle n\rangle)$.
- $\gcd(k,n) = 1$.

- $[k] \neq 0$ i no és divisor de zero en $\mathbb{Z}/\langle n\rangle$

Teorema 11.19 (Euler)
Si $n > 1$ i k són primers relatius, llavors:

$$k^{\phi(n)} = 1 \pmod n \tag{11.33}$$

on $\phi(n)$ és la funció d'Euler. Veure l'apèndix C. Per exemple, $\phi(10) = 10(1-1/2)(1-1/5) = 4$. Per tant $7^{\phi(10)} = 7^4 = 2401 = 1 \pmod{10}$, doncs $\gcd(7,10) = 1$.

Teorema 11.20 (petit teorema de Fermat)
Si p és primer i $n \in \mathbb{Z}$ llavors:

$$n^p = n \pmod p. \tag{11.34}$$

equivalentment: $n^{p-1} = 1 \pmod p$.

Teorema 11.21 (de Wilson)
Si p és primer, llavors

$$(p-1)! = -1 = p-1 \pmod p \tag{11.35}$$

Per exemple $4! = 24 = 4 \pmod 5$.

Capítol 12
Anells de Polinomis

Definició 12.1 (polinomi) Sigui un anell commutatiu A, s'anomena **anell de polinomis** en una indeterminada x a:

$$A[x] = \{a_n\, x^n + \cdots + a_1\, x + a_0 \ : \ a_i \in A, n \in \mathbb{Z}^+\} \tag{12.1}$$

Nota: en el llibre de l'UNED [4, pàg. 107] es considera més d'una indeterminada:

$$A[x] = \sum_\nu a_\nu\, x_1^{\nu_1} \cdots x_n^{\nu_n}. \tag{12.2}$$

Si $f(x),g(x) \in A$:

$$f(x) = a_n\, x^n + \cdots + a_1\, x + a_0$$
$$g(x) = b_m\, x^m + \cdots + b_1\, x + b_0$$

es defineix la suma i producte com:

$$f(x) + g(x) = (a_s + b_s)\, x^s + \cdots + (a_1 + b_1)\, x + (a_0 + b_0), \quad s = \max(n,m)$$
$$f(x)\, g(x) = c_{n+m}\, x^{n+m} + \cdots + c_1\, x + c_0$$

on $c_k = a_k\, b_0 + \cdots + a_0\, b_k$, $k = 0, \cdots, n+m$.
Si $f(x)$ té l'**element director** $a_n \neq 0$ es diu que té **grau** n i es denota per $\partial f = n$ (fent servir la notació de [4]). Per conveniència definim:

$$\partial 0 = -\infty. \tag{12.3}$$

En cas de tenir un polinomi amb varies indeterminades es defineix el grau total i parcial com:

$$\partial f(x) = \max d \ : \ a_\nu \neq 0, \nu_1 + \cdots + \nu_n = d \tag{12.4}$$
$$\partial_i f(x) = \max d \ : \ a_\nu \neq 0, \nu_i = d \tag{12.5}$$

Si $a_n = 1$ es diu que és un **polinomi mònic**, i si només hi ha un sumand es diu **monomi**.

Propietats 12.1 d'un anell de polinomis
1. $A[x]$ és un domini d'integritat (DI) sii A ho és [2, pàg. 296].
2. Si A és un DI llavors $U(A) = U(A[x])$.

Teorema 12.1 (algorisme de divisió)
[2, pàg. 296] Sigui F un cos commutatiu (*field*) amb $f(x),g(x) \in F$, $g(x) \neq 0$. Llavors existeixen els polinomis únics $q(x),r(x) \in F$ (quocient i reste, respectivament) tals que

$$f(x) = g(x)\, q(x) + r(x) \tag{12.6}$$

on $r(x) = 0$ o $\partial r(x) < \partial g(x)$.

Teorema 12.2 (regla de Ruffini)
Per a cada $f(x) \in A[x]$ existeix $q(x) \in A[x]$ tal que:

$$f(x) = q(x)\,(x-a) + f(a) \tag{12.7}$$

i $x - a \mid f(x)$ sii $f(a) = 0$.

Corol·lari 12.1 Un polinomi no nul $f \in A[x]$ té com a molt $p = \partial f$ zeros diferents en A.

Teorema 12.3 (DIP)
Sigui F un cos commutatiu (*field*). Llavors $F[x]$ és un domini d'ideals principals (DIP). És a dir, tots els ideals d'$F[x]$ són de la forma $\langle f(x)\rangle = \{f(x)\, g(x) \ : \ g(x) \in F[x]\}$ (veure la definició de DIP en 11.29, pàg. 32).

Teorema 12.4 (criteri per un ideal d'$F[x]$)
[2, pàg. 300] Sigui F un cos commutatiu (*field*), i I un ideal no nul d'$F[x]$. Llavors $I = \langle f(x)\rangle$ sii $f(x)$ és un polinomi no nul de grau mínim en I (és a dir, un polinomi de menor grau no nul).

Exemple 12.1 ($I = \langle f(x)\rangle$) [2, ex. 3, pàg. 300] Considerar l'homomorfisme

$$\phi : \mathbb{R}[x] \to \mathbb{C} : f(x) \to f(i)$$

és a dir, avaluar $f(x)$ en i. Llavors $x^2 + 1 \in \ker\phi$ i és un polinomi de grau mínim de $\ker\phi$. Per tant, del teorema 12.4 tenim $\ker\phi = \langle x^2+1\rangle$ i per el primer teorema d'isomorfia (veure 7.9, pàg. 19) $\mathbb{R}[x]/\langle x^2+1\rangle$ és isomorf amb $\operatorname{im}\mathbb{R}[x] = \mathbb{C}$.

12.1 Factorització de polinomis

Definició 12.2 (irreductibilitat) [2, pàg. 305] Sigui D un domini d'integrigat. Un element $f(x) \in D[x]$ no nul ni unitat és irreductible si per a qualsevol factorització $f(x) = g(x)\,h(x)$, $g(x)$,$h(x) \in D$, llavors $g(x)$ o $h(x)$ és una unitat de $D[x]$.

Exemple 12.2 (irreductibilitat) $f(x) = 2\,x^2 + 4$ és irreductible en $\mathbb{R}[x]$, doncs, per exemple $f(x) = 2(x^2+2)$ i $h(x) = 2$ és unitat amb $h^{-1}(x) = 2^{-1}$. Igualment per a qualsevol factorització d'$f(x)$. En canvi $f(x)$ és reductible en $\mathbb{C}$, doncs $f(x) = (2\,x+\sqrt{-2})(2\,x-\sqrt{-2})$ i cap dels factors és una unitat de $\mathbb{C}[x]$.

Definició 12.3 (contingut i polinomi primitiu)
S'anomena **contingut d'un polinomi** $f(x) = a_n\,x^n + \cdots + a_1\,x + a_0$ a $c(f) = \gcd(a_n, \cdots, a_0)$.
S'anomena **polinomi primitiu** a un polinomi amb $c(f) = 1$.

Teorema 12.5 (lema de Gauss)
[2, pàg. 307] El producte de 2 polinomis primitius és primitiu.

Teorema 12.6 (irreductibilitat en $A[x]$ i $K[x]$)
[4, pàg. 130] Si $f(x) \in A[x]$ amb $\partial[A] > 0$ és irreductible en $A[x]$, llavors $c(f) = 1$ i també és irreductible en el cos de fraccions $K[x]$ de $A[x]$.

Teorema 12.7 (les arrels divideixen $f(0)$)
[4, pàg. 142] Sigui $f(x) = a_n\,x^n + \cdots + a_1\,x + a_0 \in A[x]$ amb $a_n \in U(A)$. Llavors, tota arrel d'$f(x)$ en A divideix $a_0 = f(0)$.

12.1.1 Teoremes d'irreductibilitat

Veure [2, pàg. 307].

Teorema 12.8 (irreductibilitat)
[2, pàg. 306] Sigui F un cos commutatiu (*field*) i $f(x) \in F[x]$ amb grau 2 o 3. Llavors $f(x)$ és reductible en $F[x]$ sii $f(x)$ té un zero en F.

Exemple 12.3 (teorema irreductibilitat) En l'exemple 12.8 $f(x) = 2\,x^2 + 4$ té els zeros $\pm\sqrt{-2} \in \mathbb{C}$. Per tant, és reductible en $\mathbb{C}$, però no en $\mathbb{R}$, doncs no té zeros en $\mathbb{R}$.

Teorema 12.9 (reductibilitat en Q)
Sigui $f(x) \in \mathbb{Z}[x]$. Si f és reductible en Q, llavors és reductible en $\mathbb{Z}$.

Teorema 12.10 (test d'irreductibilitat $\bmod p$)
Sigui p primer i $f(x) \in \mathbb{Z}[x]$, $\partial f \geq 1$. Sigui $\hat{f}(x) \in \mathbb{Z}_p[x]$ el polinomi obtingut reduint els coeficients $f \bmod p$. Llavors, si $\hat{f}$ és irreductible en $\mathbb{Z}_p$ i $\partial\hat{f} = \partial f$, també ho és f en Q.

Teorema 12.11 (criteri d'Eisenstein)
Sigui

$$f(x) = a_n\,x^n + \cdots + a_1\,x + a_0 \in \mathbb{Z}[x]$$

si hi ha un primer p tal que

$$p \nmid a_n,\ p \mid a_{n-a}, \cdots, p \mid a_0,\ \text{ i } p^2 \nmid a_0$$

llavors f és irreductible en Q.

Teorema 12.12 (polinomi ciclotomic)
Sigui p primer. Llavors el **polinomi ciclotomic**

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \quad (12.8)$$

és irreductible en Q.

Teorema 12.13 (ideal maximal en $F[x]$)
Sigui F un cos commutatiu (*field*) i $f(x) \in F[x]$. Llavors $\langle f(x)\rangle$ és un ideal maximal en $F[x]$ sii f és irreductible en F (veure la definició d'ideal maximal en 11.17, pàg. 29).

Teorema 12.14 (cos commutatiu)
Sigui F un cos commutatiu (*field*) i $f(x) \in F[x]$ un polinomi irreductible en F. Llavors $F[x]/\langle f(x)\rangle$ és un cos commutatiu (*field*).

Teorema 12.15 ($f(x) \mid a(x)\,b(x)$)
Sigui F un cos commutatiu (*field*), $f(x)$,$a(x)$,$b(x) \in F[x]$ i $f(x) \in F[x]$ un polinomi irreductible en F. Si $f(x) \mid a(x)\,b(x)$, llavors $f(x) \mid a(x)$ o $f(x) \mid b(x)$.

Teorema 12.16 (factorització)
Qualsevol polinomi $f(x) \in \mathbb{Z}[x]$ diferent de zero o la unitat es pot factoritzar de forma única com:

$$f(x) = b_1 \cdots b_s\,p_1(x) \cdots p_m(x) \quad (12.9)$$

on b_i i $p_i(x)$ són polinomis irreductibles amb $\partial b_i = 0$ i $\partial p_i(x) \geq 1$.

Proposició 12.1 (DE) [4, pàg. 126] Sigui F un cos commutatiu (*field*). Llavors $F[x]$ és un domini Euclidi (DE) amb:

$$\|f(x)\| = 2^{\partial f(x)} \quad (12.10)$$

Veure la definició de DE en 11.28, pàg. 32. Nota: en el Gallian es defineix $\|f(x)\| = \partial f(x)$.

Teorema 12.17 (DFU)
Sigui F un cos commutatiu (*field*). Llavors $F[x]$ és un domini de factorització única (veure la definició 11.30, pàg. 32).

Teorema 12.18 (F cos, $F[x]$ DE, $F[x]$ DIP)
[4, pàg. 127] Les següents afirmacions són equivalents:
- F és un cos,
- $F[x]$ és un domini euclidi (DE),
- $F[x]$ és un domini d'ideals principals (DIP).

Teorema 12.19 (Gauss: implicació UFD)
[2, pàg. 334] i [4, pàg. 127] Sigui D un domini de factorització única (DFU). Llavors $D[x]$ també és un DFU.

$\mathbb{Z}$	$\mathbb{Z}[x]$
$a_n\,10^n + \cdots + a_1\,10 + a_0$	$a_n\,x^n + \cdots + a_1\,x + a_0$
Unitat $\|a\| = 1$	$\partial f(x) = 0$
$a = b\,q + r$	$f(x) = g(x)\,q(x) + r(x)$
primer	irreductible
ED: $\|a\| = \|a\|$	$\|f(x)\| = 2^{\partial f(x)}$
DIP: $I = \langle a\rangle$	$I = \langle f(x)\rangle$
DFU: producte primers	producte irreductibles

Taula 12.1: Analogia entre els anells $\mathbb{Z}$ i $\mathbb{Z}[x]$ [2, pàg. 332].

Capítol 13
Extensió de cossos

13.1 Espais vectorials

Definició 13.1 (espai vectorial) [2, pàg. 345] Un conjunt V es diu espai vectorial sobre un cos commutatiu (*field*) F si V és un grup abelià amb l'addició i per a cada $a \in F$ i $v \in V$ hi ha un element $a\,v \in V$; i es compleixen el següent per tot $a,b \in F$ i $u,v \in V$:
1. $a(u+v) = a\,u + a\,v$
2. $(a+b)v = a\,v + b\,v$
3. $a(b\,v) = (a\,b)v$
4. $1\,v = v$.

Els elements d'F s'anomenen **escalars** i els d'V **vectors**.

Definició 13.2 (subespai vectorial) Sigui V un espai vectorial sobre F. $U \subset V$ és un subespai de V si també és espai vectorial sobre F amb les mateixes operacions que V.

Definició 13.3 (independència linial) Un conjunt de vectors S es diuen linealment dependents en F si hi ha uns vectors $v_1, \cdots v_n \in S$ i escalars $a_1, \cdots a_n \in F$ tals que $a_1\,v_1 + \cdots + a_n\,v_n = 0$. Altrament es diuen linealment independents.

Definició 13.4 (base d'un espai vectorial) Sigui V un espai vectorial en F. Un conjunt de vectors $B \in V$ es diu **base** de V si B és linealment independent i qualsevol vector de V és una combinació lineal d'elements de B.
El nombre de vectors d'una base és invariant (és a dir, la mateix per a qualsevol base d'V) i s'anomena **dimensió** de V.

13.2 Extensió de cossos

Definició 13.5 (extensió d'un cos) (*extension field*) [4, pàg. 247] Siguin K,E cossos. Es diu que E és una **extensió d'un cos** K, i s'escriu E/K, si existeix un homomorfisme $f : K \to E$. Com que K és un cos, f és un monomorfisme (veure el teorema 11.7, pàg. 30), per tant, K és isomorf a la seva imatge $f(K) \subseteq E$ (notar que al ser injectiva, f serà una bijecció entre K i $f(K)$).
En el Gallian [2, pàg. 345] es dóna una definició més senzilla: E és un cos commutatiu $K \subseteq E$ on les operacions de K són les de E restringides a K.

Teorema 13.1 (Kronecker)
Sigui F un cos commutatiu (*field*) i $f(x) \in F[x]$ amb $\partial f > 0$. Llavors existeix una extensió E on $f(x)$ té un zero.

Definició 13.6 (tipus d'extensions) [2, pàg. 370] Sigui E una extensió del cos commutatiu F i $a \in E$. Una extensió d'F de la forma $F(a)$, on

$$F(x) = \{f(x)/g(x) \;:\; f(x),g(x) \in F[x],\, g(x) \neq 0\} \tag{13.1}$$

s'anomena **extensió simple** d'F.

Definició 13.7 (subextensió d'un cos) L'extensió simple definida anteriorment es defineix en [4, pàg. 252] de la següent manera. Sigui E/F i $A = \{a_1, \cdots a_n\} \in E$ (on n pot ser ∞). Es denota $F(A)$ a la intersecció de tots els subcossos $K \subset E$ que contenen F i A. El cos $F(A)$ s'anomena **extensió generada per** A **sobre** F. El cos $F(A)$ també es pot descriure de la següent manera: $x \in E$ està en $F(A)$ si existeixen els elements $A = \{a_1, \cdots a_n\} \in E$ i els polinomis $f,g \in F[x_1, \cdots x_n]$ amb n indeterminades tals que

$$g(a_1, \cdots a_n) \neq 0,\; x = f(a_1, \cdots a_n)/g(a_1, \cdots a_n) \tag{13.2}$$

Es diu que el cos $L = F(A)$ està generat per A sobre F. Si A té un nombre finit d'elements, llavors es diu que L està finitament generat. Si A té un sol element, es diu que és una **extensió simple**.

Per a 2 conjunts A, B es té:

$$F(A)(B) = F(A \cup B) \tag{13.3}$$

Definició 13.8 (homomorfisme d'avaluació) [4, pàg. 255] Sigui E una extensió del cos commutatiu F i $a_1, \cdots a_n \in E$. Es defineix l'**homomorfisme d'avaluació**:

$$F[x_1, \cdots x_n] \to E : f(x_1, \cdots x_n) \to f(a_1, \cdots a_n) \tag{13.4}$$

Llavors es diu que $a_1, \cdots a_n$ són **algebraicament independents** si $\ker f = \{0\}$. És a dir, no hi ha un polinomi no nul tal que $f(a_1, \cdots a_n) = 0$. Altrament, si existeix un polinomi no nul tal que $f(a_1, \cdots a_n) = 0$, es diu que $a_1, \cdots a_n$ són **algebraicament dependents**.

Si $a_1, \cdots a_n$ són **algebraicament independents** es un isomorfisme entre anells:

$$F[x_1, \cdots x_n] \cong F[a_1, \cdots a_n] \subset E$$

i entre cossos:

$$F(x_1, \cdots x_n) \cong f(a_1, \cdots a_n) \subset E$$

Si $n = 1$ i a_1 és **algebraicament independent** sobre F, llavors es diu que a_1 és **transcendent** sobre F. Altrament, si a_1 és **algebraicament dependent** sobre F, llavors es diu que a_1 és **algebraic** sobre F, i es té l'isomorfisme:

$$F[x_1]/\ker f \cong F[a_1] \subset E \tag{13.5}$$

A més, com que E és un cos, no té divisors de zero. Per tant, tampoc els té $F[x_1]/\ker f$ i $\ker f$ és un ideal primer $\ker f \neq \{0\}$. Com que $F[x_1]$ és un DIP, $\ker f$ serà maximal, i $F[x_1]/\ker f$ un cos. Per tant, de l'isomorfirme anterior tenim que $F[a_1]$ també és un cos i $F[a_1] = F(a_1)$.

Definició 13.9 (tipus d'extensions) La definició anterior d'element algebraic i transcendent en [2, pàg. 370] es resumeixen així: Sigui E una extensió del cos commutatiu F i $a \in E$. Es diu que a és **algebraic** en F si és el zero d'un polinomi d'$F[x]$. Altrament es diu que a és **transcendent** en F.

L'extensió E es diu algebraica en F si tots els elements d'E són algebraics en F. Altrament es diu que E és una extensió transcendent en F.

Teorema 13.2 (espai vectorial) [4, pàg. 249] Sigui E/F. Llavors E té una estructura d'espai vectorial sobre F.

Definició 13.10 (grau d'una extensió) Sigui E una extensió del cos commutatiu F i $a \in E$. Es diu que el **grau de l'extensió** E és n i s'escriu $[E : F] = n$ si E té dimensió n com a espai vectorial en F. Si el grau és finit, es diu que E és una **extensió finita**. En particular, si $[E : F] = 1$, llavors $E = F$.

Per exemple, $\mathbb{C}$ té grau 2 en $\mathbb{R}$, doncs $\{1, i\}$ és una base de $\mathbb{C}$.

Teorema 13.3 (extensió finita) Sigui E/F i F/K. Llavors són equivalents

1. E/F i F/K són finites,
2. E/K és finit.

A més, si són finites es té: $[E : K] = [E : F]\,[F : K]$.

Teorema 13.4 (unicitat) Si a és algebraic en F, llavors hi ha un polinomi mònic únic en $F[x]$ tal que $p(a) = 0$.

Teorema 13.5 (divisibilitat) Si a és algebraic en F i $p(x)$ un polinomi de grau mínim per a en F. Llavors si $f(x) \in F[x]$ i $f(a) = 0$, $p(x)$ divideix a $f(x)$ en $F[x]$.

13.3 Extensions simples

Teorema 13.6 (caracterització d'extensions) [2, pàg. 371] i [4, pàg. 257] Sigui E una extensió del cos commutatiu F i $a \in E$. Es compleix que:

- **Si a és transcendent en F**, llavors $F(a)$ és isomorf a $F(x)$.
- **Si a és algebraic en F**, llavors $f : F(x) \to F(a) = E : x \to a$ és un epimorfisme i E un anell de polinomis en a. Es diu que E/F és una **extensió simple algebraica**. Si $f(x)$ és un polinomi irreductible tal que $f(a) = 0$, llavors

$$\ker f = \langle f(x) \rangle \tag{13.6}$$

doncs $f(a) = 0$, i $f(a)\,g(a) = 0$. Per tant, $\langle f(a) \rangle = \{f(a)\,g(a) \ : \ g(x) \in F[x]\} \subseteq \ker f$. Al ser $f(x)$ irreductible, $\langle f(x) \rangle$ és un ideal maximal (veure el teorema 12.13, pàg. 35) i, per tant , $\ker f = \langle f(x) \rangle$. D'aquí tenim que per el primer teorema d'isomorfia,

$$F[x]/\langle f(x) \rangle = F[x]/\ker f \cong \operatorname{im} f = F(a) \tag{13.7}$$

Per a que el polinomi sigui únic es tria mònic i s'anomena **polinomi mínim de a sobre F**. Amb la notació de [4, pàg. 257] el polinomi mínim es denota per $P(a, F)$. És a dir, $P(a, F)$ és un polinomi irreductible mònic $f(x) \in F[x]$, tal que $f(a) = 0$.

Teorema 13.7 (element primitiu)
Sigui E/F una extensió finita de cossos de característica 0. Llavors és simple, algebraica i $E = F(a)$ per algun $a \in E$. L'element a es diu element primitiu de l'extensió.

Apèndixs

A. Divisibilitat en els enters

Definició 13.11 Divisor Es diu que l'enter d divideix l'enter a (o que a és divisible per d, o que d és divisor o factor de a) si a és un múltiple de d, i s'escriu $d|a$:

$$d|a \Rightarrow a = q\,d,\ q \in \mathbb{N}. \tag{13.8}$$

Definició 13.12 Màxim comú divisor (*Greatest Common Divisor,* gcd): Per a qualssevol enters a,b, amb a,$b \neq 0$, $\gcd(a,b)$ és el major de tots els divisors comuns de a,b. Es compleix $\gcd(a,b) = \gcd(a, a \bmod b)$. Per a calcular-ho és convenient l'**algorisme d'Euclidi**:

$$\gcd(a,b) = \begin{cases} a, & a = b \\ \gcd(a-b,b), & a > b \\ \gcd(a,b-a), & b > a \end{cases} \tag{13.9}$$

Definició 13.13 Mínim comú múltiple (*Least Common Multiple,* lcm): Per a qualssevol enters a,b, amb a,$b > 0$, $\operatorname{lcm}(a,b)$ és el menor enter positiu que és múltiple de a,b.

Definició 13.14 Nombres primers relatius: Dos nombres n,m són primers relatius si l'únic factor comú que tenen és l'1. És a dir, $\gcd(n,m) = 1$.

Teorema 13.8 De la divisió entera
Per a qualssevol enters D (dividend) i d (divisor), amb $d > 0$ existeixen els enters únics q (quocient) i r (reste) tals que

$$D = d\,q + r,\ 0 \leq r < d \tag{13.10}$$

Veure la demostració en [2, pàg. 3].

Teorema 13.9 gcd és una combinació lineal
Per a qualssevol enters a,b, amb a,$b \neq 0$, existeixen els enters s, t tals que

$$\gcd(a,b) = a\,s + b\,t. \tag{13.11}$$

Corol·lari: Si a,b són primers relatius ($\gcd(a,b) = 1$), aleshores existeixen els enters s, t tals que

$$a\,s + b\,t = 1. \tag{13.12}$$

Veure la demostració en [2, pàg. 5].

Teorema 13.10 Lema d'Euclidi Per a qualssevol enters a,b, si p és un nombre primer que divideix $a\,b$, aleshores p divideix a o divideix b. Veure la demostració en [2, pàg. 6].

Teorema 13.11 Teorema fonamental de l'aritmètica Qualsevol enter a es pot representar de forma única com a producte de potències de nombres primers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i} \tag{13.13}$$

on $p_1 < p_2 < \cdots p_k$ són nombres primers i $\alpha_i \in \mathbb{N}$. Veure la demostració en [2, pàg. 6].

B. Aritmètica modular

Per a qualssevol enters a,n, el mòdul $a \bmod n$ es defineix com el reste de la divisió entera de a entre n.

Propietats

$$a \bmod n \in \mathbb{Z}_n = \{0, 1, \cdots, n-1\} \tag{13.14}$$

$$(a \bmod n) \bmod n = a \bmod n \tag{13.15}$$

$$(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n \tag{13.16}$$

$$a\,b \bmod n = ((a \bmod n)\,(b \bmod n)) \bmod n \tag{13.17}$$

$$a^b \bmod n = a^{b \bmod \phi(n)} \bmod n \tag{13.18}$$

on $\phi(n)$ és la funció d'Euler (veure l'apèndix C).

Definició 13.15 Congruència Qualssevol enters a,b són congruents respecte $\bmod n$ si

$$a \bmod n = b \bmod n \tag{13.19}$$

Teorema 13.12 Si dos enters a,b són congruents respecte $\bmod n$, aleshores $a - b$ és un múltiple de n (és a dir $a - b$ divideix n).

Teorema 13.13 Si escrivim $a \sim_n b$ quan a,b són congruents $\bmod n$, aleshores, si $a_1 \sim_n b_1$ i $a_2 \sim_n b_2$, llavors

$$a_1 + a_2 \sim_n b_1 + b_2 \tag{13.20}$$

$$a_1 - a_2 \sim_n b_1 - b_2 \tag{13.21}$$

$$a_1\,a_2 \sim_n b_1\,b_2 \tag{13.22}$$

C. Funció ϕ d'Euler

(Euler's totient function) $\phi(n) \geq 1$ compte quants nombres enters positius menors que n són primers relatius amb n. Per tant, $\phi(n)$ és el nombre d'enters k, $1 \leq k < n$, tals que $\gcd(n.k) = 1$. Per exemple, $\phi(9) = 6$, doncs $1, 2, 4, 5, 7, 8$ són primers relatius de 9. Notar que per un nombre primer p, $\phi(p) = p - 1$.

Propietats

1. Per a qualssevol nombres $n.m$ primers relatius ($\gcd(n.m) = 1$):

$$\phi(m\,n) = \phi(m)\,\phi(m) \tag{13.23}$$

2. Per a qualsevol nombre primer p i enter $k \geq 1$:

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}) \tag{13.24}$$

3. Donada la descomposició d'un enter en factors primers (13.13) i aplicant reiteradament (13.23) i (13.24) es té:

$$\begin{aligned}\phi(a) = \phi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = \\ \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\cdots\phi(p_k^{\alpha_k}) = \\ p_1^{\alpha_1}(1-\frac{1}{p_1})p_2^{\alpha_2}(1-\frac{1}{p_2})\cdots p_k^{\alpha_k}(1-\frac{1}{p_k}) = \\ p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k}) = \\ a\,(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})\end{aligned} \tag{13.25}$$

D. Notació

gcd	*greatest common divisor*.
lcm	*least common multiple*.
$d\|a$	d divideix a.
$S \subseteq T$	$S \subset T$ o $S = T$.
$S \subset T$	$S \subset T$ i $S \neq T$.
X/R	Partició generada per la relació d'equivalència R d'un conjunt X. Veure el teorema 1.1, pàg. 2.
$G \cong G'$	Grups isomorfs. Veure la def. 7.4, pàg. 18.
A_n	Grup altern de grau n. Veure la def. 3.3, pàg. 10.
$Biy(X)$	[3, pàg. 20] Grup format per les aplicacions bijectives del conjunt no buit $X \to X$, on l'operació és la composició de funcions. Notar que els elements de $Biy(X)$ són funcions, i la funció $h : X \to X, h(x) = (f \circ g)(x)$, on f,$g \in Biy(X)$ compleix $h(X) = f(g(X)) = f(X) = X$. Per tant, $h \in Biy(X)$[1].
C_n	Grup cíclic d'ordre n. Veure la definició .
D_n	Grup dièdric d'ordre n. Veure la secció 2.3, pàg. 7.
$N(S)$ o $N_G(S)$	normalitzador de S en G. Veure la def. 2.15, pàg. 7.
$\mathrm{o}(G)$	Ordre del grup G. Veure la def. 2.4, pàg. 4.
$\mathrm{o}(a)$	Ordre de l'element a. Veure la def. 2.8, pàg. 5.
S_n	Grup simètric de grau n. Veure la def. 3.2, pàg. 8. Quan X és un grup finit, es fa servir la notació S_n en comptes de $Biy(X)$.
S^a	Conjugat de S per a. Veure la def. 2.14, pàg. 7.
GL_n	Grup de les matrius no singulars d'ordre n, amb operació producte de matrius.
$U(n)$	Conjunt dels enters positius menors que n i primers relatius amb n. També es fa servir aquesta notació per referir-se al grup format per aquest conjunt i l'operació mòdul n. L'ordre $\mathrm{o}(U(n)) = \phi(n)$. Veure la funció ϕ d'Euler, apèndix C. Notar que per un nombre primer p, $U(p) = \{1, 2, \cdots, p-1\}$.

Conjunts/Grups

$\mathbb{C}$	Conjunt dels complexes.
$\mathbb{N}$	Conjunt dels naturals (enters positius).
Q	Conjunt dels racionals.
Q^+	Conjunt dels racionals positius.
$\mathbb{R}$	Conjunt dels reals.
$\mathbb{R}^+$	Conjunt dels reals positius.
$\mathbb{Z}$	Conjunt dels enters.
$\mathbb{Z}^+$	Conjunt dels enters positius.
$\mathbb{Z}_n$	Conjunt $\{0, 1, \cdots, n-1\}$ i grup amb l'addició mòdul n.
$m\,\mathbb{Z}$	Conjunt dels múltiples de m: $\{m\,x : x \in \mathbb{Z}\} = \{\cdots, -2\,m, -m, 0, m\,2, m, \cdots\}$ i grup amb l'operació d'addició. Veure el teorema 2.4, pàg. 4.
$\mathbb{Z}_m^o$	Grup multiplicatiu dels enters mòdul n. Veure la def. 6.1, pàg. 16.

Referències

[1] Benjamin Baumslag i Bruce Chandler. *Schaum's outline of theory and problems of group theory*. McGraw-Hill, 1968.

[1] Notar que es fa servir la notació $f(X)$ per representar el conjunt que s'obté al aplicar la funció f a tots els elements del conjunt X. Veure la def. 1.7, pàg. 2.

[2] Joseph Gallian. *Contemporary abstract algebra*. 7a ed. Cengage Learning, 2010.

[3] Emilio Bujalante García, José Javier Etayo Gordejuela i José Manuel Gamboa Mutuberría. *Teoría elemental de grupos*. 3a ed. UNED, 2012.

[4] José Manuel Gamboa Mutuberría y Jesús M. Ruiz Sancho. *Anillos y cuerpos conmutativos*. UNED, 2002.

Índex alfabètic