

Apunts d'estructures algebraiques

Llorenç Cerdà-Alabern

llorenc@ac.upc.edu

Barcelona, 27 de setembre de 2016

Índex

1	Definicions	1
2	Grups	3
2.1	Grups cíclics	5
2.2	Propietats dels grups	5
2.3	Grup dièdric, D_n	6
2.4	Producte directe de grups	7
3	Grups permutatius	7
3.1	Notació per cicles (<i>cycle notation</i>)	8
4	Teorema de Lagrange	10
4.1	Classe lateral (coset)	10
4.2	Teorema de Lagrange	11
5	Subgrup Normal	12
6	Grup quocient	14
7	Morfismes	15
8	Teoremes de Sylow	18
9	Estructura dels grups abelians finits	19
10	Estructura dels grups abelians finitament generats	20
10.1	Construcció	21
Apèndixs		
A.	Definicions bàsiques	23
B.	Teoremes bàsics	24
C.	Aritmètica modular	24
D.	Funció ϕ d'Euler	24
E.	Notació	25
Referències		25

Índex alfabètic

26

Prefaci

Vaig escriure aquests apunts mentre preparava l'assignatura *Estructuras algebraicas* del curs 2015-16 del grau de matemàtiques de la UNED. Els apunts estan basats fonamentalment en el llibre de l'assignatura [3] Gallian [2] i Schaum [1]. El contingut no és rigorós ni complet, 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 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 $2R4$ ($2R4$ no és correcte), doncs $(2,4) \notin R$.

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

Definició 1.2 Funció (o aplicació, *mapping*)

$$f : A \rightarrow B$$

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 $f : A \rightarrow B$ i $X \subseteq A$ aleshores es defineix

$$f|_X : X \rightarrow B \quad (1.1)$$

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

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

$$(g \circ f)(x) = g f(x) = g(f(x)), x \in A \quad (1.2)$$

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*)

$$\forall (a,b) \in A : f(a) = f(b) \Rightarrow a = b \quad (1.3)$$

És a dir, a iguals imatges, iguals preimatges.

Definició 1.6 Funció surjectiva (*sobrejectiva, onto*)

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

És a dir, tots els elements del codomini tenen una preimatge.

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

$$\begin{aligned} X_i \cap X_j &= \emptyset, \forall i,j \\ \cup_i X_i &= G \end{aligned}$$

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 aR de X donat per:

$$aR = \{b \mid aRb, \forall b \in X\}$$

Exemple 1.2 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:

$$\begin{aligned} 1R &= \{1, 3, 4\} \\ 2R &= \{2\} \\ 3R &= \{3, 1, 4\} \\ 4R &= \{4, 1, 3\} \end{aligned}$$

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

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

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

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 aRb si a i b pertanyen al mateix element de P .

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

¹Alguns 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.

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 Grup¹ és un conjunt G dotat d'una operació binària ab (normalment la multiplicació) que compleix:

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

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

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

$$Q = \{1, -1, i, j, k, -i, -j, -k\} \quad (2.1)$$

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

$$\begin{aligned} i &= jk = -kj \\ j &= ki = -ik \\ k &= ij = -ji \\ i^2 &= j^2 = k^2 = -1. \end{aligned}$$

Per exemple, l'element invers de i és $i^2 i^2 = 1 \rightarrow i i^3 = 1 \rightarrow i^{-1} = i^3$. En els exemples 2.7, pàg. 6 i 2.2, pàg. 4 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:

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

Teorema 2.1 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 $e = e'$. \square

Teorema 2.2 Cancel·lació

$$ba = ca \Rightarrow b = c \quad (2.2)$$

$$ab = ac \Rightarrow b = c. \quad (2.3)$$

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

Demostració.

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= ae a^{-1} \\ &= aa^{-1} \\ &= e \end{aligned} \quad \square$$

Definició 2.2 Subgrup H és un subconjunt de G que és també un grup sota la mateixa operació binària 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

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

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

¹Nota: 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.

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

$$ab^{-1} \in H, \forall a, b \in H. \quad (2.5)$$

$$ab \in H, \forall a, b \in H \text{ i } a^{-1} \in H, \forall a \in H. \quad (2.6)$$

$$H \text{ és finit i tancat sota l'operació binària de } G. \quad (2.7)$$

Definició 2.3 Grup abelià és un grup que a més té la propietat commutativa: $ab = ba$.

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 $(ab)^2 = a^2b^2, \forall a, b \in G$, llavors G és abelià.

Demostració. (1) $a^2 = e \Rightarrow a = a^{-1} \Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. (2) $a(ba)b = (ab)^2 = a^2b^2 = a(ab)b \Rightarrow ab = ba$. \square

Definició 2.4 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

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

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

Definició 2.5 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 2.6 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.

Definició 2.7 Ordre d'un grup $o(G)$ 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 2.8 Ordre d'un element a d'un grup G , $o(a)$ 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 $o(a)$ és també l'ordre del subgrup generat per el conjunt $S = \{a\}$, és a dir $\langle a \rangle$. Veure la def. 2.4, pàg. 4.

Exemple 2.2 Per el grup quaterniò (veure 2.1, pàg. 3):

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

Propietats 2.1 d'un element de torsió a amb $n = o(a)$:

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

Veure la demostració en [3, pàg. 37].

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 . \square

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. 12) $o(\langle a \rangle)$ divideix $o(G)$.

2.1. Grups cíclics

2.1 Grups cíclics

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

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \quad (2.9)$$

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 $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ i $a^i = a^j$ sii n divideix $i - j$. Corol·lari: (1) $o(a) = o(\langle a \rangle)$. (2) Si $o(a) = n$ 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 $o(a) = o(G)$ (doncs $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$).

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. 12).

Exemple 2.3 El grup quaternió Q (veure 2.1, pàg. 3) no és cíclic, doncs $o(Q) = 8$ i Q no té cap element d'ordre 8 (veure l'exemple 2.2, pàg. 4).

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

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

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

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

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

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, $xy = a^{m+n} = ya$. \square

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

Teorema 2.9 $o(a) = n \Rightarrow \langle a^d \rangle = \langle a^{\gcd(n,d)} \rangle$ i $o(a^d) = n / \gcd(n,d)$. Corol·lari: (1) En un grup finit l'ordre d'un element divideix l'ordre del grup. (2) Si $o(a) = n$, aleshores $\langle a^i \rangle = \langle a^j \rangle$ sii $\gcd(n,i) = \gcd(n,j)$ i $o(a^i) = o(a^j)$ sii $\gcd(n,i) = \gcd(n,j)$. (3) Si $o(a) = n$, aleshores $\langle a \rangle = \langle a^j \rangle$ sii $\gcd(n,j) = 1$ i $o(a) = o(a^j)$ 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 10.6, pàg. 24. Veure la demostració en [2, pàg. 75].

Exemple 2.6 (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 10.6, pàg. 24. Per exemple $\mathbb{Z}_8 = \langle 3 \rangle = \{3, 3 + 3, 3 + 3 + 3, \dots\} = \{3, 6, 9, \dots\} = \{3, 6, 1, 4, 7, 2, 5, 0\}$, en aritmètica mòdul 8.

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 : $\langle a^{n/d} \rangle$. Corol·lari: 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 . Veure la demostració en [2, pàg. 77].

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 D. 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].

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. 6):

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

Com es veurà més endavant, H i H^a són isomorfs (teorema 7.6, pàg. 17). 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 :

$$Z(G) = \{a \in G \mid ab = ba \forall b \in G\}. \quad (2.10)$$

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 2.7 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 $1, -1$ sí. Per exemple, $ij = -ji$. 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. 4 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 :

$$C(a) = \{b \in G \mid ab = ba\}. \quad (2.11)$$

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 :

$$C(H) = \{x \in G \mid ax = xa, \forall a \in H\}. \quad (2.12)$$

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 $ax = xa$ i $a^{-1}y = ya^{-1}$, per tant:

$$\begin{aligned} a(xy^{-1}) &= (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = \\ &x(ya^{-1})^{-1} = x(a^{-1}y)^{-1} = x(y^{-1}a) = (xy^{-1})a \end{aligned}$$

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

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

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

Propietats 2.2 Del conjunt conjugat:

1. $S \rightarrow S^a : x \rightarrow a^{-1}xa$ 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 $S^a \subset T^a$.

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

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

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

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

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:

$$HK = \{hk : h \in H, k \in K\} \quad (2.14)$$

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

Teorema 2.17 HK és un subgrup de G sii $HK = KH$. 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 $X = \{a_i, i = 1, \dots, n\}$. Aquestes es poden obtenir amb (1) n rotacions d'angle $i\frac{2\pi}{n}, i = 0, 1, \dots, n-1$ en sentit de les agulles del rellotge, i (2) n reflexions al voltant dels eixos de simetria d'angles $i\frac{2\pi}{n}, i = 0, 1, \dots, n-1$, que anomenarem $s_i, i = 1, 2, \dots, n$. Veure la figura 2.1 per D_3 .

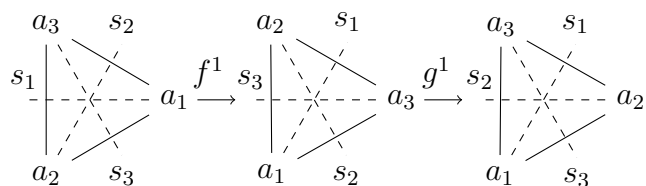


Figura 2.1: Operació $g^3 = f^1 g^1$ en D_3 .

Alternativament es pot definir el grup dièdric com la bijecció $h : X \rightarrow X$ tal que $\text{dist}(a, b) = \text{dist}(h(a), h(b)), \forall a, b \in X$, 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 $\{f^0, f^1, \dots, f^{n-1}\}$, on f^i representa una rotació de $i\frac{2\pi}{n}$, $i = 0, 1, \dots, n-1$ en el sentit de les agulles del rellotge. Les reflexions al voltant dels eixos de simetria s_i , $i = 1, 2, \dots, n$ les denotarem per $\{g^1, g^2, \dots, g^n\}$. veure la figura 2.1. Seguint la notació de [3] denotarem $g = g^1$, 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 $\{f^0, f^1, f^2\}$ i reflexions $\{g^1, g^2, g^3\}$ 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. 7, es veurà en més detall la composició de bijeccions. Per D_3 es pot comprovar que la taula és tancada amb element neutre $e = f^0$. 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 $f^i f^j = f^{i+j}$ en aritmètica mòdul n , i les n reflexions es poden obtenir amb les composicions $\{g f^0, g f^1, \dots, g f^{n-1}\}$. Notar que $g f^i \neq g f^j$, per $i \neq j$, $i, j \in \{0, 1, \dots, n-1\}$. Altrament implicaria que $f^i = f^j$, $i \neq j$, $i, j \in \{0, 1, \dots, n-1\}$ que no és possible.

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

$$D_n = \{e, f^1, f^2, \dots, f^{n-1}, g, g f^1, \dots, g f^{n-1}\} \quad (2.15)$$

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

2.4 Producte directe de grups

Definició 2.18 Producte directe de grups (External Direct Product): Siguin els grups G_1, G_2, \dots, G_n es defineix el grup denotat per $G_1 \times G_2 \times \dots \times G_n$ al conjunt de totes les n -tuples (g_1, g_2, \dots, g_n) on $g_i \in G_i$ i

el producte de tuples $(g_1, g_2, \dots, g_n) (g'_1, g'_2, \dots, g'_n) = (g_1 g'_1, g_2 g'_2, \dots, g_n g'_n)$, 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:

$$o((g_1, g_2, \dots, g_n)) = \text{lcm}(o(g_1), o(g_2), \dots, o(g_n)) \quad (2.16)$$

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

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

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

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

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

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

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 $\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1, \dots$ 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 $A = \{1, 2, \dots, n\}$. S_n té $n!$ elements, i es pot provar que per $n \geq 3$ no és Abelià.

Exemple 3.1 En un grup dièdric D_4 podem descriure una rotació de 90° en sentit de les agulles del rellotge:

$$\begin{array}{ccc} 1 & \text{---} & 2 & & 4 & \text{---} & 1 \\ | & & | & \searrow 90^\circ & | & & | \\ 4 & \text{---} & 3 & & 3 & \text{---} & 2 \end{array}$$

amb la permutació:

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

i la reflexió al voltant de l'eix horitzontal:

$$\begin{array}{ccc} 1 & \text{---} & 2 & & 4 & \text{---} & 3 \\ | & \text{---} & | & \downarrow & | & \text{---} & | \\ 4 & \text{---} & 3 & & 1 & \text{---} & 2 \end{array}$$

amb la permutació:

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

Els elements f i g generen tot el grup D_4 (tal com es va obtenir en la secció 2.3, pàg. 6). És a dir, qualsevol element de D_4 es pot obtenir d'alguna combinació de f i g . Per exemple, una rotació de 180° és f^2 (composició de f amb ell mateix). De fet, aplicant (2.15) tenim:

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

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 $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$, $4 \rightarrow 4$ i $5 \rightarrow 6 \rightarrow 5$. 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, \dots, 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:

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

3.1. Notació per cicles (cycle notation)

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:

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

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 manera 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:

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

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 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

$$aH = \{ah : h \in H\} \tag{4.1}$$

$$Ha = \{ha : h \in H\} \tag{4.2}$$

s'anomenen respectivament classe lateral per l'esquerra i per la dreta (classe esquerra o dreta, per abreviar) 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 $H + a$.

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]):

$$aR^H b \text{ si } a^{-1}b \in H \tag{4.3}$$

$$aR_H b \text{ si } ab^{-1} \in H \tag{4.4}$$

Exemple 4.1 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).

$$He = H = \{e, a^2\}$$

$$Ha = \{a, a^3\}$$

$$Ha^2 = \{a^2, a^4\} = \{a^2, e\} = H$$

$$Ha^3 = \{a^3, a^5\} = \{a^3, a\} = Ha$$

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

Exemple 4.2 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). $o(S_3) = 3! = 6$. Els 6 elements d' S_3 són:

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

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3)$$

$$s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)$$

$$s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2)$$

$$s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

$$s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3)$$

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:

$$s_2 s_1 = (1, 2)(2, 3) = (2, 3, 1) = (1, 2, 3) = s_4$$

$$s_2 s_2 = (1, 2)(1, 2) = e$$

$$s_2 s_3 = (1, 2)(1, 3, 2) = (1, 3) = s_5$$

$$s_2 s_4 = (1, 2)(1, 2, 3) = (2, 3) = s_1$$

$$s_2 s_5 = (1, 2)(1, 3) = (1, 3, 2) = s_3$$

Per tant, les classes laterals per la dreta són:

$$He = H$$

$$Hs_1 = \{s_1, s_4\}$$

$$Hs_2 = \{s_2, e\} = H$$

$$Hs_3 = \{s_3, s_5\}$$

$$Hs_4 = \{s_4, s_1\} = Hs_1$$

$$Hs_5 = \{s_5, s_3\} = Hs_3$$

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):

4.2. Teorema de Lagrange

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). \square

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 aH i Ha 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:

$$aH = \{ah : h \in H\} = \{b \mid aR^H b, \forall b \in G\} \quad (4.5)$$

$$Ha = \{ha : h \in H\} = \{b \mid bR_H a, \forall b \in G\} \quad (4.6)$$

doncs $aR^H b \Rightarrow a^{-1}b = h \in H \Rightarrow b = ah \in aH$ i $bR_H a \Rightarrow ba^{-1} = h \in H \Rightarrow b = ha \in Ha$.

Teorema 4.2 L'aplicació entre els conjunts quocients

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

és bijectiva.

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

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. $a \in aH$.
2. $aH = H$ sii $a \in H$ (H absorbeix a).
3. $aH = bH$ sii $a \in bH$.
4. $aH = bH$ sinó és $aH \cap bH = \emptyset$.
5. $aH = bH$ sii $a^{-1}b \in H$.
6. $o(aH) = o(bH)$.
7. $aH = Ha$ sii $H = aHa^{-1}$.
8. aH és un subgrup de G sii $a \in H$. Això és demostrat fàcilment, doncs si H és subgrup ha de tenir e , per tant, de les propietats 2 i 4 $aH = eH = H$. 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 $aR^H b$ si $aH = bH$ ($aR_H b$ si $Ha = Hb$ 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 Teorema de Lagrange Si G és un grup finit i H és un subgrup de G , llavors $o(H)$ divideix $o(G)$. A més, el nombre de classes laterals per l'esquerra (o la dreta) de H en G és $o(G)/o(H)$.

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

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 $o(H)$ divideix $o(G)$ amb índex $[G : H] = o(G)/o(H)$.

Exemple 4.3 En l'exemple 4.1, pàg. 10 tenim $H = \{e, a^2\}$ subgrup de C_4 , $o(H) = 2$. H genera 2 classes laterals diferents de C_4 . Com que $o(C_4) = 4$, comprovem que l'ordre d' H divideix $o(C_4)$, i que el nombre de classes laterals és $[C_4 : H] = o(C_4)/o(H) = 2$.

Exemple 4.4 En l'exemple 4.2, pàg. 10 tenim $H = \{e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$ subgrup de S_3 , $o(H) = 2$. H genera 3 classes laterals diferents d' S_3 . Com que $o(S_3) = 6$, comprovem que l'ordre d' H divideix $o(S_3)$, i que el nombre de classes laterals és $[S_3 : H] = o(S_3)/o(H) = 3$.

Exemple 4.5 [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 $o(A_4) = 4!/2 = 12$.

En les taules 3.2 i 3.3, pàg. 10 hi ha les permutacions d' A_4 . N'hi ha 3 d'ordre 2 ($\sigma_2, \sigma_5, \sigma_8$). 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. 18, exemple 8.1, es faran servir els teoremes de Sylow per tenir més informació sobre els subgrups d' A_4 .

Exemple 4.6 [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 $\mathbb{Z}/R_H = \{H + 0, H + 1, \dots, H + (m - 1)\}$. 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 $o(G)$ és un nombre primer. Sigui $a \in G$, $a \neq e$. Llavors $o(\langle a \rangle)$ divideix $o(G)$ i $o(\langle a \rangle) \neq 1$. Per tant, ha de ser $o(\langle a \rangle) = o(G)$. \square

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

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

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

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

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

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

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

$$[G : H] = [G : K][K : H] \quad (4.8)$$

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:

$$\text{card}(HK) = \frac{o(H)o(K)}{o(H \cap K)} \quad (4.9)$$

Veure la demostració en [3, pàg. 44].

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

$$a^p \text{ mod } p = a \text{ mod } p.$$

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 $H \triangleleft G$) si

$$aH = Ha, \forall a \in G \quad (5.1)$$

Notar que això vol dir que $\forall a \in G$ i $\forall h \in H$ existeixen $h_1, h_2 \in H$ tals que $ah = h_1 a$ i $ha = a h_2$. També equival a dir que les relacions d'equivalència $R^H = R_H$. Veure la definició en 4.1, pàg. 10. Doncs les classes laterals aH i Ha 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. $ab \in H \Rightarrow ba \in H, \forall a, b \in G.$ Notar però que en general $ab \neq ba.$

Demostració. (esbós, veure la demostració en [3, pàg. 61]).

1. Si H és normal de $G, \forall a \in G \exists h, h' \in H : ah = h'a.$ Llavors $aha^{-1} = h' \Rightarrow aHa^{-1} \subseteq H.$ Contràriament, si $aHa^{-1} \subseteq H$ tenim $aH \subseteq Ha.$ Si posem $b = a^{-b}$ s'obté $Hb \subseteq bH.$ Per tant $aH = Ha.$
2. $ba = a^{-1}(ab)a \in H^a = H.$ □

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

$$H = H^a = a^{-1} H a, \forall a \in G \quad (5.2)$$

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 Trobar tots els subgrups normals de $S_3.$ En l'exemple 4.2, pàg. 10 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 $\tau_1,$ 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 contrària 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 Com s'ha vist en l'exemple 5.1 $N = \{e, \sigma_1, \sigma_2\}$ és un subgrup de $S_3.$ Com que $o(N) = 3$

i $o(S_3) = 3! = 6$, 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 $\exists b \in G \mid H = K^b$). 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. 6), llavors l'aplicació

$$f : G/N \rightarrow \mathcal{F} : N a \rightarrow H^a \quad (5.3)$$

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 NH és subgrup normal de NK .

Definició 5.3 Un grup G que només té 2 grups normals $\{e\}$ i G es diu **Grup simple**. En particular, si $o(G)$ 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 $o(G)$. Per tant, si $o(G)$ és un nombre primer, G és simple.

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

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

De (5.4) es té que $K(H)$ 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 $N \subset K(H)$.

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

Teorema 5.7 Teorema de 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) $G/H = G/R_H = G/R^H = \{aH : a \in G\} = \{Ha : a \in G\}$ és un grup amb l'operació

$$G/H \times G/H \rightarrow G/H : (aH)(bH) = abH, \quad (6.1)$$

on l'element neutre és $H = eH$, doncs $(eH)(eH) = eeH = eH = H$.

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 $G/H \times G/H \rightarrow G/H : (a+H)(b+H) = a+b+H$. Veure la demostració en [2, pàg. 180] o [3, pàg. 70].

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

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 $G/H = \langle aH \rangle$. \square

Exemple 6.1 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. 3:

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} : \\ (a+m\mathbb{Z})(b+m\mathbb{Z}) &\rightarrow a+b+m\mathbb{Z} = \\ \{0+m\mathbb{Z}, 1+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}\} &= \\ \{\hat{0}, \hat{1}, \dots, \widehat{m-1}\} &\quad (6.2) \end{aligned}$$

on s'ha fet servir la notació $\hat{a} = a+m\mathbb{Z} = \{a+mx : x \in \mathbb{Z}\} = \{\dots, a-m2, a-m, a, a+m, a+m2, \dots\}$.

Notar que amb aquesta notació $\widehat{a}\widehat{b} = (a + m\mathbb{Z})(b + m\mathbb{Z}) = a + b + m\mathbb{Z} = \widehat{a+b}$.

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

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

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

amb operació

$$\begin{aligned} \mathbb{Z}_m^\circ \times \mathbb{Z}_m^\circ &\rightarrow \mathbb{Z}_m^\circ : \\ (a + m\mathbb{Z})(b + m\mathbb{Z}) &\rightarrow ab + m\mathbb{Z} \end{aligned} \quad (6.4)$$

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

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

$$\mathbb{Z}_4^\circ = \{1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\} \quad (6.5)$$

Té 2 elements, per tant, és cíclic d'ordre 2. \mathbb{Z}_m° , però, no sempre és cíclic. Veure l'exemple 7.6, pàg. 16.

Notar que en (6.4) es fa servir el producte $(ab + m\mathbb{Z})$, i no la suma $(a + b + m\mathbb{Z})$ com en el grup quocient (6.2) de l'exemple 6.1. Per evitar ambigüitats amb la notació de l'exemple 6.1 ara canviem la notació i definim: $\bar{a} = a + m\mathbb{Z}$. Ara $\bar{a}\bar{b} = (a + m\mathbb{Z})(b + m\mathbb{Z}) = ab + m\mathbb{Z} = \overline{ab}$.

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

1. G és tancat: Per $a, b \in G$ tenim $\gcd(a,m) = \gcd(b,m) = 1$. Per tant $\gcd(ab,m) = 1 \Rightarrow \overline{ab} \in G$.
2. Propietat associativa: $(\bar{a}\bar{b})\bar{c} = \overline{ab}c = \bar{a}(\bar{b}\bar{c})$.
3. Identitat: $\gcd(1,m) = 1 \in G$, $\bar{1}\bar{a} = \bar{a} = \bar{a}\bar{1}$.
4. Inversa: Si $\gcd(a,m) = 1 \Rightarrow \exists s, t : as + mt = 1$ (veure el teorema 10.3, pàg. 24). Com que $as + mt = 1 \Rightarrow \bar{a}\bar{s} + \bar{m}\bar{t} = \bar{1}$ i $\bar{m}\bar{t} = \bar{0}$, tenim $\bar{a}\bar{s} = \bar{a}\bar{s} = \bar{1} \in G$ i es conclou que $a^{-1} = s$. \square

Capítol 7 Morfismes

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

$$f(ab) = f(a)f(b), \forall ab \in G \quad (7.1)$$

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

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

on e' és l'element identitat de G' .

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

Demostració. Per $a, b \in \ker f$ tenim $f(ab^{-1}) = f(a)f(b^{-1}) = e'e' \Rightarrow ab^{-1} \in \ker f$, 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. 13. Però si $x \in \ker f$, llavors $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)f(a^{-1}) = f(e) = e' \Rightarrow axa^{-1} \in \ker f$. \square

Teorema 7.2 [3, pàg. 77]. f és injectiva sii $\ker f = \{e\}$, on e és l'element identitat de G .

Demostració. Suposem que f és injectiva. Sigui l'element identitat de G' $e' = f(e)$. 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 $\ker f = \{e\}$. \square

Propietats 7.1 Homomorfismes:

1. Si els elements neutres de G i G' són e i e' , llavors $e' = f(e)$. Doncs $e'f(e) = f(e) = f(ee) = f(e)f(e)$.
2. $f(a^n) = f(a)^n$, $\forall a \in G$. En cas que l'operació del grup sigui l'addició: $f(na) = nf(a)$, $\forall a \in G$.
3. $f(a^{-1}) = f(a)^{-1}$, doncs

$$\begin{aligned} f(a)f(a^{-1}) &= f(aa^{-1}) = f(e) = e' \\ f(a^{-1})f(a) &= f(a^{-1}a) = f(e) = e'. \end{aligned}$$
4. Si $f : G \rightarrow G'$ és un homomorfisme i 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 $f : G \rightarrow G'$ és un homomorfisme i 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

$$f : H \rightarrow G : x \rightarrow x \quad (7.3)$$

és un homomorfisme injectiu, doncs $f(xy) = xy = f(x)f(y)$.

7. Si $f : G \rightarrow G'$ i $g : G \rightarrow G'$ són homomorfismes, també ho és $g \circ f : G \rightarrow G'$, doncs $g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f(x))(g \circ f(y))$.
8. Sigui $f : G \rightarrow F'$ un homomorfisme i $o(x) = m$, llavors
- $o(f(x))$ divideix m .
 - Si f és injectiva, $o(f(x)) = m$.
- Veure la demostració en [3, pàg. 79].

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

$$\pi : G \rightarrow G/N : a \rightarrow aN \quad (7.4)$$

és un homomorfisme sobrejectiu, doncs $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$. Recordar que per el grup quocient es defineix $abH = (aH)(bH)$ (veue 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 $(aH)(bH) = abH$ (veure (6.1)).

Exemple 7.1 (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.

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 7.3 Grup isomòrfic (del grec *iso*, “igual” i *morfic*, “forma”) Un isomorfisme $f : G \rightarrow G'$ és una bijectió que preserva l'operació del grup:

$$f(ab) = f(a)f(b), \forall ab \in G \quad (7.5)$$

Per comprovar que dos grups són isomòrfics 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: $f(ab) = f(a)f(b), \forall a, b \in G$.

Exemple 7.2 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 bijectió $f(x) = 2^x$, doncs

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

Exemple 7.3 La funció $f : \mathbb{R} \rightarrow \mathbb{R} : x \rightarrow x^3$ 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 bijectió $f : G_1 \rightarrow G_2 : f(a^n) = b^n$.

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

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

Exemple 7.5 El Grup additiu dels enters mòdul n ($\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$) és isomorf del grup quocient $\mathbb{Z}/n\mathbb{Z}$ (veure la definició de $\mathbb{Z}/n\mathbb{Z}$ en 6.1, pàg. 14). 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 6.1, pàg. 14, respectivament).

Exemple 7.6 El Grup multiplicatiu dels enters mòdul n (veure 6.1, pàg. 15) és cíclic sii $n = 1, 2, 4, p^k, 2p^k$ on p és un primer major que 2 i k un enter positiu. Com que $o(\mathbb{Z}_n^\circ) = \phi(n)$ (veure D), per els valors p^k es té:

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

Teorema 7.5 Sigui $m = n_1 n_2 \dots n_k$, on n_i són enters positius. Llavors el següent producte directe de grups (veure 2.16, pàg. 6) és una isomorfa sii $n_i, n_j, i \neq j$ són primers relatius

$$\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k} \quad (7.7)$$

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

Demostració. \mathbb{Z}_{n_i} és cíclic (veure l'exemple 2.5, pàg. 5), i el producte directe de grups cíclics és cíclic si els ordres dels grups són primers relatius (veure el teorema 2.19, pàg. 7), \square

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 $f : H \rightarrow H^a = a^{-1} H a : f(h) = a^{-1} h a$. Llavors els grups H i H^a són isomorfs.

Demostració.

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

Veure la definició de subgrup conjugat en 2.10, pàg. 5.

Propietats 7.2 Dels isomorfismes

- Les mateixes que les dels homomorfismes 7.1, doncs un isomorfisme també es homomorfisme.
- f^{-1} és un isomorfisme de G' a G . Per això es diu simplement que G i G' són **grups isomorfs** i es denota per $G \cong G'$.
- Dos grups isomorfs tenen les mateixes propietats (de la teoria de grups). En particular:
- 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' .
- $G = \langle a \rangle$ sii $G' = \langle f(a) \rangle$. Per tant, si G és cíclic, també ho és G' .
- $o(G) = o(G')$ i $o(a) = o(f(a)) \forall a \in G$.
- Les equacions $x^k = a$ en G tenen el mateix nombre de solucions que $x^k = f(a)$ en G' .
- Per a grups finits G i G' tenen el mateix nombre d'elements de cada ordre.
- 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 $o(G) = 2p$, on p és un nombre primer major de 2. Llavors G és isomòrfic de \mathbb{Z}_{2p} o D_p . Per exemple, S_3 , amb ordre $3! = 6$, és isomòrfic de D_3 .

Teorema 7.8 Teorema de Cayley. Tot grup és isomòrfic d'un grup permutatiu.

Definició 7.4 Es diu **imatge de f** a:

$$\text{im } f = \{f(x) : x \in G\} = f(G) \quad (7.8)$$

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

Teorema 7.9 Primer teorema d'isomorfia Si $f : G \rightarrow G'$ és un homomorfisme, llavors $G/\ker f$ i $\text{im } f = f(G)$ són isomorfs. Notar que això implica que $o(G/\ker f) = o(f(G))$.

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]. \square

Exemple 7.7 ([3, prob. 26.a, pàg. 114]) Existeix un homomorfisme injectiu $f : S_3 \rightarrow A_4$?

Solució Si f és injectiva llavors $\ker f = \{e\}$ (teorema 7.2, pàg. 15). 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 $o(f(S_3)) = o(S_3) = 3! = 6$. Però això no és possible, perquè, tal com s'ha vist en l'exemple 4.5, pàg. 11, A_4 no té cap subgrup d'ordre 6.

Exemple 7.8 [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:

$$f_k : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \rightarrow kx + n\mathbb{Z}$$

$$k = i \frac{n}{d}, i = 0, \dots, d-1, d = \text{gcd}(m, n). \quad (7.9)$$

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

Exemple 7.9 [3, ex. 2.9.4, pàg 87] Calcular els d'homomorfismes injectius entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.

Solució (veure [3, pàg 88]) Sigui $f : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$.

Si f és injectiva llavors $\ker f = \{e\}$ (teorema 7.2, pàg. 15). Per el primer teorema d'isomorfia (teorema 7.9) tenim $\mathbb{Z}/m\mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} \cong \text{im } f = f(\mathbb{Z}/m\mathbb{Z})$, que ha de ser un subgrup de $\mathbb{Z}/n\mathbb{Z}$. Tenim doncs $o(\text{im } f) = m$ que ha de dividir $o(\mathbb{Z}/n\mathbb{Z}) = n$, per teorema de Lagrange. Tenint en compte l'exemple 7.8, es conclou que els homomorfismes injectius són de la forma:

$$f : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \rightarrow kx + n\mathbb{Z}$$

$$k = i \frac{n}{m}, i = 0, \dots, m-1, \gcd(i, m) = 1. \quad (7.10)$$

Per tant, el nombre d'homomorfismes injectius és la funció $\phi(m)$ d'Euler. Veure l'apèndix D.

Exemple 7.10 [3, ex. 2.9.4, pàg 88] Calcular els d'homomorfismes surjectius entre $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.

Solució (veure [3, pàg 88]) Sigui $f : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. Si f és surjectiva llavors $\text{im } f = f(\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. Per tant $\mathbb{Z}/m\mathbb{Z}/\ker f \cong \text{im } f \cong \mathbb{Z}/n\mathbb{Z} \Rightarrow [\mathbb{Z}/m\mathbb{Z} : \ker f] = n$ i, per el teorema de Lagrange, $m/o(\ker f) = n$. És a dir, m és un múltiple de n . Tenint en compte l'exemple 7.8, es conclou que els homomorfismes injectius són de la forma:

$$f : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \rightarrow kx + n\mathbb{Z}$$

$$k = i, i = 0, \dots, n-1, \gcd(i, n) = 1. \quad (7.11)$$

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

Exemple 7.11 (Veure [3, 2.96, pàg. 91] per a més detalls) Sigui

$$\epsilon : S_n \rightarrow U_2 = \{1, -1\} :$$

$$\alpha \rightarrow \epsilon(\alpha) = \begin{cases} 1, & \alpha \text{ és una permutació parella,} \\ -1, & \alpha \text{ és una permutació senar.} \end{cases}$$

(7.12)

Veure la definició de permutació parella i senar en 3.6, pàg. 9. Llavors, el grup altern A_n (veure la definició en 3.3, pàg. 9) 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 $[S_n : A_n] = o(S_n/A_n) = o(U_2) = 2$. Per el teorema de Lagrange tenim $o(S_n)/o(A_n) = 2$. com que $o(S_n) = n!$ es conclou que $o(A_n) = n!/2$, tal com es va deduir en la definició de grup altern 3.3, pàg. 9.

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/N .
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. $N_1(H_1 \cap H_2)$ 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. $(H_1 \cap H_2)(N_1 \cap H_2)$ és subgrup normal de $(H_1 \cap H_2)$.
- 4.

$$N_1(H_1 \cap H_2)/N_1(H_1 \cap H_2) \cong$$

$$N_2(H_1 \cap H_2)/N_2(N_1 \cap H_2) \cong$$

$$(H_1 \cap H_2)/(H_1 \cap H_2)(N_1 \cap H_2)$$

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 $o(G)$. 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 $o(H)$ 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 $o(G) = mp^k$, 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 $n_p = 1 + kp$, per algun enter k , i en aritmètica mòdul p es té $(1 + kp) \bmod p = 1$. 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 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 Per el grup A_4 , $o(A_4) = 4!/2 = 12$. 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 $1 = 1 + k \cdot 2$ per $k = 0$, $3 = 1 + k \cdot 2$ per $k = 1$. Tal com es va obtenir en l'exemple 4.5, pàg. 11, només hi ha 1 2-subgrup de Sylow (curiosament, en l'exemple 4.5 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 $4 = 1 + k \cdot 3$ per $k = 1$. Tal com es va obtenir en l'exemple 4.5, 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 $y \in G$, $o(y)$ divideix $o(x)$. 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 HK i $H \times K$ són isomorfs. És a dir:

$$f : H \times K \rightarrow HK : (h, k) \rightarrow hk.$$

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} , $i = 2, \dots, r$; 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. 17). 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 7.4, pàg. 16), 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, \dots, m_r tals que

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r} \quad (9.1)$$

on cada m_i divideix m_{i-1} . A més, els nombres r, m_1, m_2, \dots, m_r són únics i $o(G) = m_1 m_2 \dots m_r$. Els nombres m_1, m_2, \dots, 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 resultat 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. 7. 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 7.5, pàg. 16).

Exemple 9.1 [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, \dots, m_r tals que $m_1 m_2 \dots m_r = 36$ 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

$$m_1 = 18, m_2 = 2, \text{ Llavors } G_2 = \mathbb{Z}_{18} \times \mathbb{Z}_2,$$

$$m_1 = 12, m_2 = 3, \text{ Llavors } G_3 = \mathbb{Z}_{12} \times \mathbb{Z}_3,$$

$$m_1 = 6, m_2 = 6, \text{ Llavors } G_4 = \mathbb{Z}_6 \times \mathbb{Z}_6$$

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 $o(G_1)$ i $o(G_2)$ 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:

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

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 $G = \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_n$, 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

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_s$$

tenim

$$T(G) = \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z} \times \underbrace{\emptyset \times \dots \times \emptyset}_r = \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z} \quad (10.2)$$

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

6. Sigui

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_r$$

tenim

$$G/T(G) = \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_s$$

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

Teorema 10.1 Teorema 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, \dots, m_n , tals que:

1.
$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_r \quad (10.3)$$

2. m_i divideix m_{i-1} , $i = 2, \dots, n$.

3.
$$T(G) \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \quad (10.4)$$

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

$$S = \{x_1, \dots, x_n\} \quad (10.5)$$

un **sistema generador** de G (veure la definició 2.5, pàg. 4). Denotem

$$\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_n \quad (10.6)$$

i definim l'homomorfisme

$$f_s : \mathbb{Z}^n \rightarrow G : \\ (m_1, \dots, m_n) \rightarrow x_1 m_1 + \cdots + x_n m_n \quad (10.7)$$

Notar que

$$f_s((m_1, \dots, m_n) + (g_1, \dots, g_n)) = \\ x_1(m_1 + g_1) + \cdots + x_n(m_n + g_n) = \\ (x_1 m_1 + \cdots + x_n m_n) + (x_1 g_1 + \cdots + x_n g_n) = \\ f_s(m_1, \dots, m_n) + f_s(g_1, \dots, g_n),$$

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

$$R(S) = \ker f_s. \quad (10.8)$$

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

$$m_1 x_1 + \cdots + m_n x_n = 0 \quad (10.9)$$

Veure la definició de $\ker f$ 7.2, pàg. 15. En el que que segueix es farà servir el terme **relació** per referir-se a la tupla $(m_1, \dots, m_n) \in R(S)$, 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

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

De la propietat 10.1.5 tenim

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

i de 10.1.4

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

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

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

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. 17):

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

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 $(m_1, \dots, m_n) \in R(S) = \ker f_s$ entre els generadors $S = \{x_1, \dots, x_n\}$ 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:

$$G = \langle x_1, \dots, x_n : m_1 x_1 = \cdots = m_n x_n = 0 \rangle \quad (10.12)$$

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

$$S = \{x_1, \dots, x_n\} \\ R = \{r_1, \dots, r_k\} \\ r_i = (0, \dots, m_i, \dots, 0)$$

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

$$G = \langle x_1, \dots, x_n : m_1 x_1 = \cdots = m_k x_k = 0 \rangle \quad (10.13)$$

Llavors el grup

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

on m_1, \dots, 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 [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:

$$\begin{aligned} x &= (a + 3\mathbb{Z}, b + 12\mathbb{Z}) = \\ &= a(1 + 3\mathbb{Z}, 0 + 12\mathbb{Z}) + b(0 + 3\mathbb{Z}, 1 + 12\mathbb{Z}) = \\ &= ax_1 + bx_2 \end{aligned}$$

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

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

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

$$\begin{aligned} R &= \{r_1, r_2\} \\ r_1 &= (3, 0) \\ r_2 &= (0, 12) \end{aligned}$$

Fent servir la notació (10.13):

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

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

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

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

$$y_1 = x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n \quad (10.14)$$

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 (veure [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 complet de relacions:

$$\begin{aligned} S &= \{x_1, \dots, x_n\} \\ R &= \{r_1, \dots, r_k\} \\ r_i &= (a_{i1}, \dots, a_{in}), i = 1, \dots, k. \end{aligned}$$

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

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

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

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

on m_i divideix m_{i+1} , $i = 1, \dots, (k - 1)$, aplicant els canvis de la proposició 10.2. Llavors, els generadors S' que resulten amb les relacions $r_i = (0, \dots, m_i, \dots, 0)$ generen G . Per tant, de la proposició 10.1, m_1, \dots, 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} , $j = 2, \dots, n$ en la forma:

$$a_{1j} = \lambda_j a_{11} + b_{1j}, j = 2, \dots, n, 0 \leq b_{1j} < a_{11} \quad (10.17)$$

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 $y_1 = x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n$ és un generador, per tant:

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

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} , $j = 2, \dots, k$ en la forma (notar que per simplificar la notació, denotem els elements de M després del pas anterior per a_{ij}):

$$a_{i1} = \lambda_i a_{11} + c_{i1}, i = 2, \dots, k, 0 \leq c_{i1} < a_{11} \quad (10.18)$$

És a dir, restar a 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

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

és un sistema generador minimal de $R(S)$. Ara continuem igual que el pas anterior per aconseguir que a_{i1} , $i = 2, \dots, k$ sigui un múltiple de a_{11} , és a dir $a_{i1} = \mu_i a_{11}$, $i = 2, \dots, k$. 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

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

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 $(a_{11}, b_{22}, \dots, b_{2,k})$.

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 [3, ex. 7.14.4, pàg. 353] Donat el grup amb presentació:

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

Calcular els coeficients de torsió i el nombre de Betti.

Solució Aplicant el mètode anterior tenim:

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

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 $\beta(G) = 1$.

Apèndixs

A. Definicions bàsiques

Definició 10.3 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 $d \mid a$:

$$d \mid a \Rightarrow a = qd, q \in \mathbb{N}. \quad (10.19)$$

Definició 10.4 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**:

$$\gcd(a, b) = \begin{cases} a, & a = b \\ \gcd(a - b, b), & a > b \\ \gcd(a, b - a), & b > a \end{cases} \quad (10.20)$$

Definició 10.5 Mínim comú múltiple (*Least Common Multiple*, lcm): Per a qualssevol enters a, b , amb $a, b > 0$, $\text{lcm}(a, b)$ és el menor enter positiu que és múltiple de a, b .

Definició 10.6 Nombres primers relatius: Dos nombres n, m són primers relatius si l'únic factor comú que tenen és l'1. És a dir, $\gcd(n, m) = 1$.

B. Teoremes bàsics

Teorema 10.2 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

$$D = dq + r, \quad 0 \leq r < d \quad (10.21)$$

Veure la demostració en [2, pàg. 3].

Teorema 10.3 gcd és una combinació lineal

Per a qualssevol enters a, b , amb $a, b \neq 0$, existeixen els enters s, t tals que

$$\gcd(a, b) = as + bt. \quad (10.22)$$

Corol·lari: Si a, b són primers relatius ($\gcd(n, m) = 1$), aleshores existeixen els enters s, t tals que

$$as + bt = 1. \quad (10.23)$$

Veure la demostració en [2, pàg. 5].

Teorema 10.4 Lema d'Euclidi Per a qualssevol enters a, b , si p és un nombre primer que divideix a o b , aleshores p divideix a o divideix b . Veure la demostració en [2, pàg. 6].

Teorema 10.5 Teorema fonamental de l'aritmètica Qualsevol enter a es pot representar de forma única com a producte de potències de nombres primers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i} \quad (10.24)$$

on $p_1 < p_2 < \cdots < p_k$ són nombres primers i $\alpha_i \in \mathbb{N}$. Veure la demostració en [2, pàg. 6].

C. 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

$$a \bmod n \in \mathbb{Z}_n = \{0, 1, \dots, n-1\} \quad (10.25)$$

$$(a \bmod n) \bmod n = a \bmod n \quad (10.26)$$

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n \quad (10.27)$$

$$ab \bmod n = ((a \bmod n)(b \bmod n)) \bmod n \quad (10.28)$$

Definició 10.7 Congruència Qualsevol enters a, b són congruents respecte mod n si

$$a \bmod n = b \bmod n \quad (10.29)$$

Teorema 10.6 Si dos enters a, b són congruents respecte mod n , aleshores $a - b$ és un múltiple de n (és a dir $a - b$ divideix n).

Teorema 10.7 Si escrivim $a \sim_n b$ quan a, b són congruents mod n , aleshores, si $a_1 \sim_n b_1$ i $a_2 \sim_n b_2$, llavors

$$a_1 + a_2 \sim_n b_1 + b_2 \quad (10.30)$$

$$a_1 - a_2 \sim_n b_1 - b_2 \quad (10.31)$$

$$a_1 a_2 \sim_n b_1 b_2 \quad (10.32)$$

D. Funció ϕ d'Euler

(**Euler's totient function**) $\phi(n) \geq 1$ compta 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 qualsevol nombres n, m primers relatius ($\gcd(n, m) = 1$):

$$\phi(mn) = \phi(m)\phi(n) \quad (10.33)$$

2. Per a qualsevol nombre primer p i enter $k \geq 1$:

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right) \quad (10.34)$$

3. Donada la descomposició d'un enter en factors primers (10.24) i aplicant reiteradament (10.33) i (10.34) es té:

$$\begin{aligned} \phi(a) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \\ &= \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) = \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \\ &= a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \quad (10.35) \end{aligned}$$

E. Notació

gcd	<i>greatest common divisor.</i>
lcm	<i>least common multiple.</i>
$d \mid a$	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. 7.3, pàg. 16.
A_n	Grup altern de grau n . Veure la def. 3.3, pàg. 9.
$Biy(X)$	[3, pàg. 20] Grup format per les aplicacions bijectives del conjunt no buit $X \rightarrow X$, on l'operació és la composició de funcions. Notar que els elements de $Biy(X)$ són funcions, i la funció $h : X \rightarrow X$, $h(x) = (f \circ g)(x)$, 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. 6.
$N(S)$ o $N_G(S)$	normalitzador de S en G . Veure la def. 2.15, pàg. 6.
$o(G)$	Ordre del grup G . Veure la def. 2.7, pàg. 4.
$o(a)$	Ordre de l'element a . Veure la def. 2.8, pàg. 4.
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. 6.
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 $o(U(n)) = \phi(n)$. Veure la funció ϕ d'Euler, apèndix D. Notar que per un nombre primer p , $U(p) = \{1, 2, \dots, p-1\}$.

Conjunts/Grups

\mathbb{C}	Conjunt dels complexos.
\mathbb{N}	Conjunt dels naturals (enters positius).
\mathbb{Q}	Conjunt dels racionals.
\mathbb{Q}^+	Conjunt dels racionals positius.
\mathbb{R}	Conjunt dels reals.
\mathbb{R}^+	Conjunt dels reals positius.
\mathbb{Z}	Conjunt dels enters.
\mathbb{Z}_n	Conjunt $\{0, 1, \dots, n-1\}$ i grup amb l'addició mòdul n .
$m\mathbb{Z}$	Conjunt dels múltiples de m : $\{mx : x \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$ i grup amb l'operació d'addició. Veure el teorema 2.4, pàg. 3.
\mathbb{Z}_m^o	Grup multiplicatiu dels enters mòdul n . Veure la def. 6.1, pàg. 15.

Referències

[1] Benjamin Baumslag i Bruce Chandler. *Schaum's outline of theory and problems of group theory*. McGraw-Hill, 1968.

[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.

¹Notar 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.

Índex alfabètic

- Índex d'un subgrup, 11
- algorisme d'Euclidi, 24
- Bijecció, 2
- Centralitzador d'un element a , 6
- Centralitzador d'un subgrup H , 6
- Centre, 5
- Classe generada per una relació d'equivalència, 2
- classes d'equivalència, 11
- coeficients de torsió, 20
- Composició de funcions, 2
- Congruència, 24
- Conjugat, 6
- Conjugat d'un subconjunt S per un element a , 6
- Conjunts quocients, 3
- Cor, 14
- coset, 10

- De la divisió entera, 24
- Divisor, 23

- epimorfisme, 16
- Euler's totient function, 24

- Fórmula de transitivitat de l'índex, 12
- Funció ϕ d'Euler, 24
- Funció (o aplicació, *mapping*), 1
- Funció bijectiva (*bijective*), 2
- Funció injectiva (*one-to-one*), 2
- Funció restringida a un subconjunt, 2
- Funció surjectiva (*sobrejectiva*, *onto*), 2

- generador minimal, 4
- Grup, 3
- Grup abelià, 4
- Grup additiu dels enters, 3
- Grup additiu dels enters múltiples de m , 3
- Grup additiu dels enters mòdul n , 3, 16
- Grup additiu dels racionals, 3
- Grup altern de grau n , A_n , 9
- Grup cíclic, 5
- grup especial lineal, 13
- Grup finitament generat, 4
- Grup isomòrfic, 16
- Grup multiplicatiu dels enters mòdul n , 15, 16
- Grup multiplicatiu dels racionals diferents de zero, 3
- Grup permutatiu:, 7
- Grup quaternió, 3
- Grup quocient (*factor group*), 14

- Grup simètric de grau n , S_n , 8
- Grup simple, 14
- grupoide, 3
- grupoide abelià, 3
- grupoide associatiu o semigrup, 3
- Grups homomòrfics, 15
- grups isomorfs, 17

- homomorfisme natural, 16

- imatge de f , 17
- Inversió, 9
- isomorfisme, 16

- Kernel, 15

- Lema d'Euclidi, 24

- Mínim comú múltiple, 24
- Màxim comú divisor, 24
- matriu de G respecte la presentació (S,R) , 22
- monomorfisme, 16
- multiplicació de cicles, 8

- Natural homomorphism, 16
- nombre de Betti, 21
- Nombres primers relatius, 24
- Normalitzador, 6
- Notació per cicles (*cycle notation*), 8
- nucli (*kernel*), 15

- One-to-one, 2
- Onto, 2
- Operació binària, 2
- Ordre d'un element a d'un grup G , 4
- Ordre d'un grup, 4

- p-grup, 18
- p-grup maximal, 18
- p-subgrup de Sylow, 18
- Partició, 2
- permutació (*permutation*), 2
- Permutació parella, 9
- Permutació senar, 9
- permutacions, 7
- Petit teorema de Fermat, 12
- presentació de G mitjançant generadors i relacions, 21
- Primer teorema d'isomorfia, 17
- Primer teorema de Sylow, 18
- Producte de subgrups, 6

- Producte directe de grups, 7
- projecció, 16
- propietat de simetria, 1
- propietat reflexiva, 1
- propietat transitiva, 1

- Quart teorema d'isomorfia, 18

- Relació d'equivalència, 1

- Segon teorema d'isomorfia, 18
- Segon teorema de Sylow, 19
- sistema complet de relacions de G respecte S , 21
- Sistema generador, 4
- sistema generador, 21
- Sobreyectiva, 2
- Subconjunt conjugat, 6
- subconjunt propi, 4
- Subgrup, 3
- Subgrup conjugat, 5
- subgrup de les relacions de G respecte d' S , 21

- Subgrup de torsió, 20
- Subgrup generat, 4
- Subgrup Normal, 12
- subgrup propi, 3, 4
- subgrups conjugats, 14

- taula de Cayley, 7
- taula de multiplicació, 7
- Teorema d'estructura de grups abelians finitament generats, 20
- Teorema d'estructura de grups abelians finits, 19
- Teorema de Cayley, 17
- Teorema de Lagrange, 11
- Teorema de Poincaré, 14
- Teorema fonamental de l'aritmètica, 24
- Teorema fonamental dels grups cíclics, 5
- Tercer teorema d'isomorfia, 18
- Tercer teorema de Sylow, 19
- Test de normalitat, 13
- torsió, 4