Estructures Algebraiques

Cinc Cèntims de Grups

Mario Vilar

2 de gener de 2023

Índex

1

Grups i subgrups

Definició 1.1 (Grup**).** És un conjunt G no buit dotat d'una operació interna associativa, amb element neutre i tal que tot element té simètric. Si, a més, l'operació és commutativa, diem que el grup és *abelià*:

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

Definició 1.2 (Subgrup**).** Un subgrup d'un grup G és un subconjunt no buit H de G tal que:

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

Proposició 1.3. *Siguin G un grup i $H \subset G$ un subconjunt no buit. Els tres enunciats següents són equivalents:*

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

Definició 1.4 (Grup simètric**).** Posem S_n el conjunt de les permutacions de n elements amb el producte de permutacions. És un grup que es diu *grup simètric*. A S_n tenim $n!$ permutacions.

2

Morfismes de grups

Definició 2.1 (Morfisme**).** Si G, G' són grups, una aplicació $f : G \longrightarrow G'$ és un morfisme de grups si $f(xy) = f(x)f(y)$, per a tot $x, y \in G$.

Definició 2.2 (Tipus de morfismes**).** Suposem dos grups G, G' i f una aplicació $f : G \longrightarrow G'$.

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

5. Un *automorfisme* de G és un endomorfisme de G bijectiu.

Definició 2.3 (Nucli i imatge d'un grup**).** Siguin G, G' grups. Per a un morfisme de grups $f : G \longrightarrow G'$ definim el nucli de f com $\ker(f) = \{x \in G \mid f(x) = e'\}$ (els elements del conjunt inicial que s'envien per f al neutre del conjunt d'arribada) i definim la imatge de f com $\operatorname{im}(f) = \{f(x) \mid x \in G\}$ (el conjunt d'imatges per f).

Proposició 2.4. *Si $f : G \longrightarrow G'$ és morfisme de grups,* $\ker(f)$ *és subgrup de G i* $\operatorname{im}(f)$ *és subgrup de G'.*

Proposició 2.5. *Sigui $f : G \longrightarrow G'$ un morfisme de grups:*

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

Proposició 2.6. *Sigui $f : G \longrightarrow G'$ un morfisme de grups. f és un morfisme injectiu si, i només si,* $\ker(f) = \{e\}$.

Demostració.

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

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

■

3

Lagrange

Definició 3.1 (Ordre d'un grup**).** Donat un grup G, diem que G és finit si el conjunt G és finit i, en aquest cas, diem ordre de G i indiquem per $|G|$ el cardinal del conjunt G.

Definició 3.2 (Índex de grup**).** Donats un grup G i un subgrup H de G, posem $[G : H]$ i diem índex de G en H el cardinal de G/D (que hem vist és igual al de G/E). En altres paraules, és el nombre de classes d'equivalència que existeix, tant per la dreta com per l'esquerra.

Teorema 3.3 (Teorema de Lagrange**).** *Donats un grup G i un subgrup H de G, el grup G és finit si, o només si, H i $[G : H]$ són finits. En aquest cas,*

$$|G| = |H| \cdot [G : H]. \tag{3.1}$$

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

Demostració.

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

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

■

4

Grups normals i quocients

Proposició 4.1. *Sigui G un grup, H un subgrup de G, D i E les relacions definides a partir d'H. Els enunciats següents són equivalents:*

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

Demostració.

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

$$(xh)x^{-1} = (h'x)x^{-1} = h'(xx^{-1}) = h' \in H. \tag{4.1}$$

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

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

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

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

$$\left.\begin{matrix} x' = xh \\ y' = yh' \end{matrix}\right\} \implies x'y' = x(hy)h' = x(yh'')h' = xy(h''h') \implies \left.\begin{matrix} xDx' \\ yDy' \end{matrix}\right\} \implies xyDx'y'. \tag{4.2}$$

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

$$\left.\begin{matrix} xhDx \\ x^{-1}Dx^{-1} \end{matrix}\right\} \implies xhx^{-1}Dxx^{-1} = e \implies xhx^{-1} \in H. \tag{4.3}$$

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

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

■

Definició 4.2 (Morfisme de pas al quocient**).** El definim per $\pi : G \longrightarrow G/H$ i envia cada element de G a la seva classe en G/H. És epimorfisme de grups amb nucli H.

Definició 4.3 (Grup normal**).** Un subgrup H de G es diu normal si es compleix alguna (i, per conseqüència, totes) de les condicions de 4.1. En aquest cas, $G/D = G/E$ i l'escrivim G/H o $H \lhd G$. En particular, anomenem $x \longmapsto [x]$ com morfisme de pas al quocient.

Definició 4.4 (Grup quocient**).** Sigui H un subgrup de G. Si H és normal, G/H té estructura de grup. En efecte, $[x][y] = [xy]$ i es diu grup quocient de G en H.

Proposició 4.5. *Si $f : G \longrightarrow G'$ és un morfisme de grups,* $\ker(f)$ *és subgrup normal de G.*

Proposició 4.6. *Sigui $f : G \longrightarrow G'$ un morfisme de grups.*

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

Proposició 4.7. *Si G és abelià, aleshores cada subgrup H de G és normal. Si $[G : H] = 2$, aleshores H és normal en G.*

5

Teoremes d'isomorfia

Definició 5.1 (f factoritza a través de G/H**).** Siguin G, G' grups i sigui $f : G \longrightarrow G'$ un morfisme de grups i sigui H un subgrup normal de G. Diem que f factoritza a través de G/H si existeix un morfisme de grups $\overline{f} : G/H \longrightarrow G'$ tal que $f = \overline{f} \circ \pi$, on $\pi : G \longrightarrow G/H$ és el morfisme de pas a quocient, és a dir, si existeix un morfisme de grups $\overline{f} : G/H \longrightarrow G'$ que faci commutatiu el diagrama:

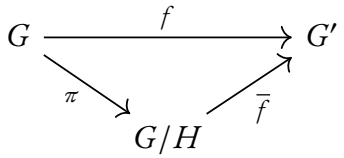


Figura 1: El diagrama commuta si, i només si, $f = \overline{f} \circ \pi$.

Proposició 5.2. *Siguin G, G' grups i sigui $f : G \longrightarrow G'$ un morfisme de grups i sigui H un subgrup normal de G. Aleshores, f factoritza a través de G/H si, i només si, $H \subset \ker(f)$.*

Demostració.

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

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

$$f(y) = f(xh) = f(x)f(h) = f(x)e' = f(x), \tag{5.1}$$

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

$$\overline{f}([x][y]) = \overline{f}([xy]) = f(xy) = f(x)f(y) = \overline{f}([x])\overline{f}([y]), \tag{5.2}$$

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

■

Teorema 5.3 (Primer teorema d'isomorfia**).** *Si G, G' són grups i $f : G \longrightarrow G'$ és un morfisme de grups, aleshores f factoritza a través de $G/\ker(f)$ i tenim $f = i \circ \tilde{f} \circ \pi$, amb $\tilde{f}$ isomorfisme de grups $G/\ker(f)$ en $\operatorname{im}(f)$, on $\pi : G \longrightarrow G/\ker(f)$ és el morfisme de pas al quocient i $i : \operatorname{im}(f) \longrightarrow G'$ la inclusió. Tenim, doncs, un diagrama commutatiu:*

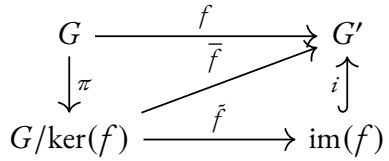


Figura 2: Primer teorema d'isomorfia.

Demostració. Per 5.2, existeix un morfisme $\overline{f} : G/\ker(f) \longrightarrow G'$, que envia $[x] \longmapsto f(x)$, tal que $f = \overline{f} \circ \pi$. Clarament, $\overline{f}$ és injectiu i $\overline{f} = i \circ \tilde{f}$, amb $\tilde{f}$ isomorfisme de $G/\ker(f)$ en $\mathrm{im}(\overline{f})$. Com $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$, per la definició de $\overline{f}$ obtenim el resultat desitjat.

$$\overline{f} = i \circ \tilde{f}, \quad \tilde{f} : \begin{array}{ccc} G/\ker(f) & \longrightarrow & \mathrm{im}(\overline{f}) \\ [x] & \longmapsto & f(x) \end{array} \quad f = i \circ \tilde{f} \circ \pi, \ \tilde{f} \text{ és injectiva.} \tag{5.3}$$

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

Teorema 5.4 (Segon teorema d'isomorfia**).** *Sigui $\varphi : G \longrightarrow G'$ un epimorfisme de grups. Sigui H' un subgrup normal de G' i $H = \varphi^{-1}(H')$. Aleshores, φ indueix un isomorfisme de G/H en $G'H'$.*

Corol·lari 5.5. *Si G és un grup i F i H són subgrups normals de G amb $F \subset H$, aleshores H/F és subgrup normal de G/F i el morfisme de pas al quocient $G \longrightarrow G/F$ indueix un isomorfisme de G/H en $(G/F)/(H/F)$.*

Teorema 5.6 (Tercer teorema d'isomorfia**).** *Sigui G un grup, H i F subgrups de G, amb H normal en G. Posem $HF := \{hf \mid h \in H, f \in F\}$. Aleshores, HF és un subgrup de G, $F \cap H$ és un subgrup normal de F i H és un subgrup normal d'HF. A més, la inclusió d'F en HF indueix un isomorfisme de $F/(F \cap H)$ en HF/H.*

6

Grups cíclics

Definició 6.1 (Ordre d'un element**).** El subgrup $\langle x \rangle$ és el conjunt dels elements de G que són iguals a x^n per a algun $n \in \mathbb{Z}$. En particular, $\ker(f_x) = m\mathbb{Z}$ és subgrup de $\mathbb{Z}$. Tenim $\langle x \rangle \cong \mathbb{Z}/m\mathbb{Z}$. Si $m > 0$, diem que m és l'ordre de x i posem $\mathrm{ord}(x)$. En cas que $m = 0$, diem que x té ordre infinit. L'ordre de l'element és l'ordre del subgrup que genera. En particular, l'ordre de x divideix l'ordre de G, $|G|$.

Definició 6.2 (Grup cíclic**).** Un grup G es diu cíclic si existeix $x \in G$ tal que $G = \langle x \rangle$ (és a dir, que està generat per un únic element). Diem que G està generat per x. Denotem per C_n el grup cíclic d'ordre n i aquest és isomorf a $\mathbb{Z}/n\mathbb{Z}$.

Proposició 6.3. *Tot grup cíclic és isomorf a $\mathbb{Z}$ o bé a $\mathbb{Z}/m\mathbb{Z}$, per a un enter $m > 0$. Per tant, dos grups cíclics del mateix ordre són isomorfs entre ells.*

Lema 6.4. *Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n per a tot enter $k > 0$, es compleix:*

$$\mathrm{ord}(x^k) = \frac{n}{\mathrm{mcd}(n, k)}. \tag{6.1}$$

Corol·lari 6.5. *Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n. Aleshores, x^k genera G si, i només si,* $\mathrm{mcd}(n, k) = 1$.

Proposició 6.6. *Tot subgrup d'un grup cíclic és cíclic.*

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

$$x^\ell = (x^m)^q \in \langle x^m \rangle. \tag{6.2}$$

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

Proposició 6.7. *Si G és un grup cíclic d'ordre n, per a cada divisor d de n existeix un únic subgrup de G d'ordre d.*

Demostració. Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n ($|G| = n$) i d un divisor de n. Un subgrup d'un grup cíclic G és cíclic, 6.6, i és d'ordre d si està generat per un element d'ordre d. Per 6.4, $x^{\frac{n}{d}}$ té ordre d i $\langle x^{\frac{n}{d}} \rangle$ és subgrup de G d'ordre d. De nou per 6.4, els elements de G que tenen ordre d són els x^k amb $\frac{n}{\mathrm{mcd}(n,k)} = d$, és a dir, són els x^k amb k múltiple d'$\frac{n}{d}$ ($k = \ell \frac{n}{d}$ per algun ℓ). Per tant,

$$x^k = (x^{\frac{n}{k}})^\ell \in \langle x^{\frac{n}{d}} \rangle. \tag{6.3}$$

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

7 Subgrup generat per un conjunt

Definició 7.1 (Subgrup generat per S**).** Sigui G un grup, S un subconjunt de G. Definim el subgrup de G generat per S, que indicarem per $\langle S \rangle$, com la intersecció de tots els subgrups de G que contenen S. Si H és subgrup de G i $H = \langle S \rangle$, direm que S és un conjunt (o sistema) de generadors de H. Clarament $\langle \emptyset \rangle = \{e\}$.

Proposició 7.2. *El subgrup de G generat per un subconjunt no buit S de G és el conjunt de tots els elements de la forma*

$$x_1^{n_1} \dots x_r^{n_r}, \tag{7.1}$$

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

8

Producte directe de grups

Definició 8.1 (Producte directe de $G_1 \times \cdots \times G_r$**).** Generalitzant, si $G_1, \ldots, G_r$ grups en el producte cartesià $G_1 \times \cdots \times G_r$ definim la operació binària interna per $(x_1, \ldots, x_r)(y_1, \ldots, y_r) = (x_1 y_1, \ldots, x_r y_r)$. $G_1 \times \cdots \times G_r$ és grup:

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

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

Proposició 8.2. *Siguin G_1 i G_2 grups cíclics d'ordres n_1 i n_2, respectivament. El producte directe $G_1 \times G_2$ és cíclic si i només si n_1 i n_2 són primers entre ells. En aquest cas, si x_1 és un generador de G_1 i x_2 és un generador de G_2, $\langle (x_1, x_2) \rangle$ és un generador de $G_1 \times G_2$.*

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

$$\operatorname{ord}(x_1, x_2) = \operatorname{mcm}(\operatorname{ord} x_1, \operatorname{ord} x_2), \tag{8.1}$$

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

$$(x_1, x_2)^{\operatorname{mcm}(\operatorname{ord}(x_1), \operatorname{ord}(x_2))} = (e_1, e_2). \tag{8.2}$$

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

Definició 8.3 (Producte directe intern**).** Si f està definida com

$$\begin{array}{rccc} f: & H_1 \times H_2 & \longrightarrow & G \\ & (h_1, h_2) & \longmapsto & h_1 h_2 \end{array} \tag{8.3}$$

i és isomorfisme, diem que G és producte directe intern de $H_1 \cap H_2$. Equivalentment, si es compleixen les tres condicions següents:

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

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

$$\begin{array}{l} H_1 \cong \{(h_1, e_2) \mid h_1 \in H_1\} \text{ subgrup normal d'} H_1 \times H_2, \\ H_2 \cong \{(e_1, h_2) \mid h_2 \in H_2\} \text{ subgrup normal d'} H_1 \times H_2; \end{array} \tag{8.4}$$

9

Grups definits per generadors i relacions

Definició 9.1 (Relació entre elements**).** Sigui G un grup generat per un conjunt finit $S = \{x_1, \ldots, x_n\}$, és a dir, $G = \langle x_1, \ldots, x_n \rangle$. Una relació entre els elements de S és una igualtat del tipus

$$x_1^{k_1} \ldots x_n^{k_n} = e, \text{ on } k_1, \ldots, k_n \in \mathbb{Z}. \tag{9.1}$$

Definició 9.2 (Grup definit pels generadors**).** Si G és un grup finit definit pel conjunt de generadors S i el conjunt de relacions R a partir de R i S podem escriure els elements de G i la taula del producte de G.

10

Grups resolubles

Definició 10.1 (Grup resoluble**).** Un grup G és resoluble si existeix una cadena finita de subgrups de G de la següent forma: comença amb el trivial i cadascun està inclòs en el següent i cadascun d'ells compleix que cadascun és normal amb el següent i els quocients són abelians:

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,\ i = 0 \div n - 1. \tag{10.1}$$

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

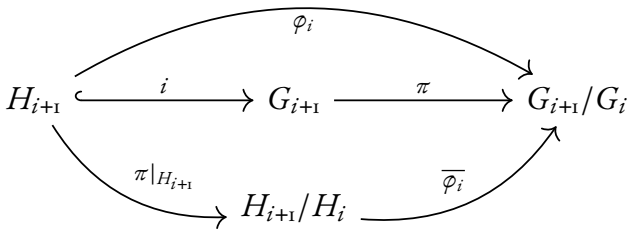
Una successió de grups es diu que és una *torre normal* si compleix la primera propietat i és una *torre abeliana* si compleix la segona propietat. És *resoluble* si és una torre abeliana l'últim subgrup de la qual és el neutre (és a dir, que $G_0 = \{e\}$, el subgrup trivial de G).

Proposició 10.2.

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

Demostració.

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



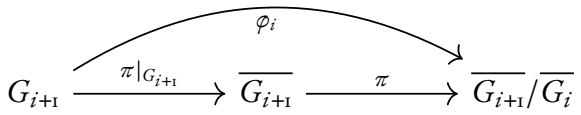
$$\ker(\varphi_i) = H_{i+1} \cap G_i = (H \cap G_{i+1}) \cap G_i = H \cap G_i = H_i \implies H_i \lhd H_{i+1}$$
$$\varphi_i \text{ factoritza a través de } H_{i+1}/H_i \text{ i } \overline{\varphi_2} : H_{i+1}/H_i \longrightarrow G_i/G_{i+1}. \tag{10.2}$$

- Per 4.5, $\ker(\varphi_i) \lhd H_{i+1}$; així doncs, $H_i \lhd H_{i+1}$.
- $\overline{\varphi_i}$ és injectiu pel teorema d'isomorfia: sigui $[x] \in H_{i+1}/H_i$ tal que, en concret, $[x] \in \ker(\overline{\varphi_i})$. Aleshores, $\overline{\varphi_i}([x]) = \varphi_i(x) = \overline{e}$, on $\overline{e}$ és el neutre en G_{i+1}/G_i. Prenent $x \in \ker(\varphi_i) = H_i$, $[x]$ és la classe del neutre en H_{i+1}/H_i: $\overline{\varphi_i}([x]) = \varphi_i(x) = \overline{e}$.
- Així, H_{i+1}/H_i és isomorf a $\operatorname{im}(\overline{\varphi_i}) \subset G_{i+1}/G_i$ abelià (ja que G és resoluble per hipòtesi), de manera que H_{i+1}/H_i és també abelià.

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

$$\overline{G_i} \lhd \overline{G_{i+1}} \;\Big|\; \forall x \in G_i, \forall y \in G_{i+1}, G_i \lhd G_{i+1},\, yxy^{-1} \in G_i \implies \overline{y}\,\overline{x}\,\overline{y}^{-1} \in \overline{G_i} \tag{10.3}$$

Per tant, considerem el següent diagrama un altre cop:



Per tant, $G_i \subset \ker(\varphi_i)$; en particular, $G_{i+1}/\ker(\varphi_i)$ és isomorf a $\overline{G_{i+1}}/\overline{G_i}$. Així doncs, $G_i \subset \ker(\varphi_i) \subset G_{i+1}$ implica, per 5.5:

$$\begin{aligned} G_{i+1}/\ker(\varphi_i) \cong \frac{G_{i+1}/G_i}{\ker(\varphi_i)/G_i} &\text{ és abelià } (G_{i+1}/G_i \text{ abelià, } G \text{ és resoluble}) \\ &\implies G_{i+1}/\ker(\varphi_i) \text{ abelià} \implies \overline{G_{i+1}}/\overline{G_i} \text{ abelià.} \end{aligned} \tag{10.4}$$

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

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = H \tag{10.5}$$

una torre abeliana de H i

$$\{\overline{e}\} = \overline{G}_0 \subset \overline{G}_1 \subset \cdots \subset \overline{G}_n = \overline{G} \tag{10.6}$$

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

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = H = \pi^{-1}\left(\overline{G}_0\right) \subset \pi^{-1}\left(\overline{G}_1\right) \subset \cdots \subset \pi^{-1}\left(\overline{G}_n\right) = G. \tag{10.7}$$

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

$$\pi^{-1}(\overline{G_{i+1}}) \xrightarrow{\pi|_{\pi^{-1}(\overline{G_{i+1}})}} \overline{G_{i+1}} \longrightarrow \overline{G_{i+1}}/\overline{G_i}, \qquad \ker=\pi^{-1}(\overline{G_i})$$

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

■

11

Grups simples

Definició 11.1 (Grup simple**).** Un grup G es diu simple si no té subgrups normals propis no trivials, és a dir, diferents de $\{e\}$ i G. Els grups S_3, A_4, S_4, D_{2n} no són simples.

Proposició 11.2. *Un grup no trivial és simple i resoluble si, i només si, és cíclic d'ordre primer.*

12

Grups diedrals

Definició 12.1 (Grup diedral D_{2n}**).** D_{2n} és el grup generat per ρ i σ amb relacions $\rho^n = Id$, $\sigma^2 = Id$ i $\sigma\rho\sigma = \rho^{-1}$. Posem

$$D_{2n} = \left\langle \rho, \sigma \mid \rho^n = Id, \sigma^2 = Id, \sigma\rho\sigma = \rho^{-1} \right\rangle. \tag{12.1}$$

13

Accions i òrbites

Definició 13.1 (Acció per l'esquerra d'un grup**).** Sigui S un conjunt i G un grup. Una acció de G sobre S és una aplicació:

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, s) & \longmapsto & g \cdot s \end{array} \tag{13.1}$$

Complint:

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

Definició 13.2 (Òrbita d'una acció**).** Si $G \times S \longrightarrow S$ és una acció, $s \in S$, diem òrbita de S el conjunt $\{gs \mid g \in G\} = O_s$. L'estabilitzador de s és $E(s) = \{g \in G \mid gs = s\}$.

Definició 13.3 (Fix per l'acció**).** Diem que $s \in S$ és fix per l'acció de G si $gs = s$, per a tot $g \in G$. Equivalentment, $O(s) = \{s\}$ o $E(s) = G$.

Proposició 13.4. *Donada una acció p de G sobre S, amb $s \in S$, l'aplicació:*

$$\begin{array}{ccc} G & \longrightarrow & S \\ g & \longmapsto & gs \end{array} \tag{13.2}$$

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

Definició 13.5 (Acció per conjugació**).** L'acció per conjugació d'un grup sobre ell mateix és:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, h) & \longmapsto & ghg^{-1} \end{array} \tag{13.3}$$

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

$$\begin{array}{c} E(h) = \{g \in G \mid ghg^{-1} = h\} = Z_G(h), \text{ centralitzada d'} h \text{ en } G. \\ O(h) = \{ghg^{-1} \mid g \in G\}, \text{ és la classe de conjugació d'} h. \end{array} \tag{13.4}$$

Definició 13.6 (Acció per conjugació d'un grup sobre el conjunt dels seus subgrups**).** Sigui H subgrup de G. Sigui $g \in G$. El conjugat d'H per g és un subgrup de G tal que $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. L'acció per conjugació d'un grup sobre el conjunt dels seus subgrups és

$$\begin{array}{c} (gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1}. \\ (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}. \end{array} \tag{13.5}$$

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

$$\begin{array}{ccc} G \times \mathscr{H} & \longrightarrow & \mathscr{H} \\ (g, H) & \longmapsto & gHg^{-1} \end{array} \tag{13.6}$$

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

Definició 13.7 (Acció per translació**).** Si H és un subgrup d'un grup G, podem considerar l'acció de H en G per translació a l'esquerra

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg. \end{array} \tag{13.7}$$

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

$$\rho : \begin{array}{ccc} H \times G/D_F & \longrightarrow & G/D_F \\ (h, gF) & \longmapsto & (hg)F. \end{array} \tag{13.8}$$

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

$$H \cap \left(\bigcap_{g \in G} gFg^{-1} \right). \tag{13.9}$$

I $E(gF) = H \cap gFg^{-1}$.

Proposició 13.8 (Equació de les classes**).** *Si G és un grup finit, es compleix*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : Z_G(x_i)] \tag{13.10}$$

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

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

$$|S| = |S_0| + \sum_{i=1}^{r} [G : E(x_i)], \tag{13.11}$$

dona la fórmula de l'enunciat. ∎

Definició 13.9 (p-grup**).** Si p és un nombre primer, un grup finit G s'anomena p-grup si $|G| = p^r$, per a algun r enter natural > 0.

Proposició 13.10 (Congruència dels punts fixos**).** *Si G és un p-grup que opera sobre un conjunt finit S, aleshores*

$$|S| \equiv |S_0| \pmod{p} \tag{13.12}$$

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

Corol·lari 13.11. *Si G és un p-grup, el seu centre $Z(G)$ és no trivial.*

Corol·lari 13.12 (Congruència del normalitzador**).** *Sigui H un p-subgrup d'un grup finit G. Aleshores*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}. \tag{13.13}$$

14

Cauchy i Sylow

Teorema 14.1 (Teorema de Cauchy**).** *Sigui G un grup finit d'ordre n i p un nombre primer que divideix n. Aleshores G té un element (i per tant un subgrup) d'ordre p.*

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

$$(k, (g_1, \cdots, g_p)) \longmapsto \left(g_{k+1}, \dots, g_{k+p}\right), \tag{14.1}$$

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

$$|S_0| \equiv |S| \pmod{p} \implies p \mid |S_0|. \tag{14.2}$$

El conjunt en qüestió és el següent:

$$S_0 = \left\{(x, \dots, x) \mid x \in G, x^p = e\right\}. \tag{14.3}$$

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

Definició 14.2 (p-subgrup de Sylow**).** Els p-subgrups de G amb ordre la màxima potència de p dividint $|G|$ es diuen p-subgrups de Sylow de G. En particular, si G és grup d'ordre n i p primer amb $p \mid n$, diem p-subgrup de Sylow de G un subgrup de G d'ordre p^r amb $p^r \mid n$ i $p^{r+1} \nmid n$.

Teorema 14.3 (Primer teorema de Sylow**).** *Sigui G un grup finit, p un nombre primer i $r > 0$ un nombre enter tals que p^r divideix $|G|$. Aleshores existeixen subgrups $H_1, \cdots, H_r$ de G tals que $|H_i| = p^i$, $1 \leq i \leq r$, i $H_i \lhd H_{i+1}$, $1 \leq i \leq r-1$. En particular, H_r és subgrup de Sylow.*

Demostració. Raonem per inducció. Si $r = 1$, és conseqüència directa del teorema de Cauchy 14.1. Seguim la inducció sobre r. Suposem que $r \geq 2$ i que existeixen subgrups $H_1, \dots, H_{r-1}$ de G tals que $|H_i| = p^i$ i $H_i \lhd H_{i+1}$. Com $p \mid [G : H_{r-1}]$, per la congruència del normalitzador 13.12, tenim $p \mid [N_G(H_{r-1}) : H_{r-1}]$.

Pel teorema de Lagrange, el grup quocient $N_G(H_{r-1})/H_{r-1}$ (on $H_{r-1} \triangleleft N_G(H_{r-1})$) té un subgrup divisible per p i, per 14.1 un altre cop, aquest és precisament p. La seva antiimatge per la projecció

$$\pi : N_G(H_{r-1}) \longrightarrow N_G(H_{r-1})/H_{r-1} \tag{14.4}$$

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

Corol·lari 14.4. *Si G es un grup finit i p un nombre primer dividint $|G|$, aleshores existeixen p-subgrups de Sylow de G. Tot p-grup és resoluble.*

Teorema 14.5 (Segon teorema de Sylow**).** *Siguin G un grup finit, H un p-subgrup de G i S un p-subgrup de Sylow de G, amb p primer. Aleshores existeix $x \in G$ tal que $H \subset xSx^{-1}$. En particular dos p-subgrups de Sylow de G són conjugats.*

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

$$\begin{array}{ccc} H \times G/D_S & \longrightarrow & G/D_S \\ (h, gS) & \longrightarrow & hgS \end{array} \tag{14.5}$$

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

$$\begin{aligned} gS \text{ punt fix} \iff hgS = gS \iff g^{-1}hgS = S \iff g^{-1}hg \in S \\ \iff h \in gSg^{-1} \iff H \subset gSg^{-1}, \forall h \in H. \end{aligned} \tag{14.6}$$

Per tant, el conjunt de punts fixos és $X_0 = \{xS \in G/D_S \mid H \subset xSx^{-1}\}$. Com que H és p-grup i $|G/D_S| = [G : S]$, la congruència de punts fixos 13.10 dona $|X_0| \equiv [G : S] \pmod{p}$. Com $p \nmid [G : S]$ (G/S és p-subgrup de Sylow), tenim $p \nmid |X_0|$ i, per tant, $|X_0|$ no és buit. ■

Corol·lari 14.6. *El grup G té un únic p-subgrup de Sylow S si, i només si, G té un p-subgrup de Sylow que és un subgrup normal.*

Teorema 14.7 (Tercer teorema de Sylow**).** *Sigui G un grup finit i n_p el nombre de p-subgrups de Sylow de G. Aleshores es compleix*

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

Demostració.

1. Pel segon teorema de Sylow 14.5, n_p és el cardinal de l'òrbita d'un p-subgrup de Sylow S_p per l'acció de G per conjugació sobre el conjunt dels subgrups de G. L'estabilitzador de S_p per a aquesta acció és $N_G\left(S_p\right)$, de manera que $n_p = [G : N_G(S_p)]$.
2. Ara $\left[G : S_p\right] = \left[G : N_G\left(S_p\right)\right]\left[N_G\left(S_p\right) : S_p\right]$, per tant, n_p divideix $\left[G : S_p\right]$, ja que $S_p \subset N_G \subset G$.

$$\left[G : S_p\right] = \left[G : N_G\left(S_p\right)\right]\left[N_G\left(S_p\right) : S_p\right] \iff \frac{|G|}{|S_p|} = \frac{|G|}{|N_G(S_p)|} \cdot \frac{|N_G(S_p)|}{|S_p|}. \tag{14.7}$$

   D'aquesta manera, $n_p \mid [G : S_p]$.
3. Sigui ara X el conjunt de p-subgrups de Sylow de G. Considerem l'acció de S_p en X per conjugació. Aleshores el conjunt de punts fixos és $X_0 = \left\{T \in X \mid xTx^{-1} = T, \forall x \in S_p\right\} = \left\{T \in X \mid S_p \subset N_G(T)\right\}$. Volem veure $X_0 = \left\{S_p\right\}$. En efecte, si $T \in X_0$, aleshores S_p i T són p-subgrups de Sylow de $N_G(T)$ i T és normal en $N_G(T)$. Com que $T \lhd N_G(T)$ implica que $N_G(T)$ té exactament un p-subgrup de Sylow, apliquem 14.6 i ens queda $T = S_p$ i $X_0 = \{S_p\}$. Com $|X| = n_p$ i $|X_0| = 1$, per la congruència dels punts fixos, 13.10, tenim $n_p \equiv 1 \pmod{p}$.

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