TREBALL DE FI DE MÀSTER

# Màster en Matemàtica Aplicada

**Títol: Problemes algorísmics en grups lliure per lliure-abelià**


**Autor: Jordi Delgado Rodríguez**

**Director: Enric Ventura Capell**

**Departament: Departament de Matemàtica Aplicada III**


**Convocatòria: Juny 2011**




UPC

Facultat de Matemàtiques i Estadística

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Tesi de Màster
Màster en Matemàtica Aplicada

# Problemes algorísmics en grups lliure per lliure-abelià

Jordi Delgado Rodríguez

Director: Enric Ventura Capell

Departament de Matemàtica Aplicada III

*a la Màrcia*

## Agraïments

Voldria dedicar aquestes línies a persones que, des de diferents perspectives, han contribuït a la realització d'aquest treball.

En primer lloc, al meu director, l'Enric; pel seu constant estímul i les continues suggerències sense els quals el treball no hauria estat possible; però sobretot, per la seva infinita paciència.

I a la Màrcia, per demostrar que no cal entendre una cosa per entendre que val la pena.

Al Juli, per – tot i haver hagut de suportar (sense possibilitat de fugir) innumerables discursos sobre cardinals transfinits durant el seu vuitè més de gestació – proporcionar-me, un cop nascut, nits plàcides en les que poder treballar.

Al Pep, durant anys el meu únic contacte amb les matemàtiques fora del meu despatx, per proporcionar-me aquesta oportunitat, pel miler llarg de cafès compartits; i per pagar-ne aproximadament la meitat.

També voldria agrair la comprensió de tots aquells que, malgrat probablement no tinguin clara la compensació d'aquest esforç, m'han demostrat la seva estimació amb el seu suport incondicional. En particular: a la Maria Luz, la meva mare; al meu germà, el David; a la Lídia i el Lluís Maria; i als que m'han recolzat des de més lluny. Possiblement tinguin raó, però ja ho cantava el gran Silvio:

"Lo más terrible se aprende enseguida, y lo hermoso nos cuesta la vida...".

Pasmo sempre quando acabo qualquer coisa. Pasmo e desolo-me. O meu instinto de perfeição deveria inibir-me de acabar; deveria inibir-me até de dar começo.

Fernando Pessoa, [Livro do Desassossego].

# Resum

**Paraules clau:** grup lliure, grup lliure abelià, problema de decisió, automorfisme

**MSC2000:** 20E05, 20K01

En aquest treball s'estudia els grups $F_n \times \mathbb{Z}^m$ i alguns problemes de decisió algorísmica sobre ells. Aquesta família es presenta com un generalització per a la qual s'estenen de forma consistent certes nocions i característiques pròpies dels grups lliures i lliure-abelians. Així, per exemple, veiem que és tancada per subgrups i admet versions *lliure-abelianes* de conceptes com ara rang i base que concorden i estenen les nocions homònimes estàndard. Similarment, donem expressions senzilles per als endomorfismes de $F_n \times \mathbb{Z}^m$ en funció d'un endomorfisme de $F_n$, un altre de $\mathbb{Z}^m$ i un terme creuat que controla com s'entrellacen les parts lliure i lliure-abeliana. A més, caracteritzem la injectivitat i exhaustivitat dels nostres endomorfismes només en termes dels dos primers; i obtenim, per als automorfismes i la seva composició, una forma particularment simple.

A la part algorísmica, considerem certs problemes de decisió sobre $F_n \times \mathbb{Z}^m$ que usant els resultats de la primera part, reduïm als problemes homònims sobre el grup lliure juntament amb un problema abelià més o menys sofisticat. Sota aquest patró resolem a $F_n \times \mathbb{Z}^m$: el *membership problem*, l'*isomorphism problem*, el problema de l'índex finit, el problema de Howson, el problema dels punts fixos per un automorfisme, el *twisted conjugacy problem* i el primer problema de Whitehead.

# Abstract

**Keywords:** free froup, free abelian group, decision problem, automorphism

**MSC2000:** 20E05, 20K01

In this paper we study the group $F_n \times \mathbb{Z}^m$ and some decision problems on it. This family is presented as a generalization for which some notions and characteristic of free and free abelian groups consistently extend. For example, we see that it is closed by taking subgroups and supports *free by free-abelian* versions of concepts such as rank or basis. Similarly, we give expressions for the endomorphisms of $F_n \times \mathbb{Z}^m$ in terms of an endomorphism of $F_n$, another of $\mathbb{Z}^m$ and a mixed term which controls how the abelian and free abelian parts interact. We also characterize the injectivity and exhaustivity of our endos in terms only of the first two; obtaining for the automorphisms and their composition a particularly simple form.

In the algorithmic part, we consider some decision problems over $F_n \times \mathbb{Z}^m$ which, by using the results of the first part, we reduce to the homonymous problems on the free group plus a more or less sophisticated abelian one. Under this pattern we solve over $F_n \times \mathbb{Z}^m$: the membership problem, the isomorphism problem, the finite index problem, the Howson problem, the fixed points problem, the twisted conjugacy problem, and the first Whitehead problem.

# Notació

En el present treball $\mathbb{N}$ designa el conjunt dels nombres naturals (sencers no negatius) mentre que $\mathbb{Z}$ i $\mathbb{Q}$ designen respectivament els conjunts dels nombres sencers i racionals. En tots tres casos entendrem, si s'escau, que també designen l'estructura subjacent.

Sobreentendrem que el signe $\infty$ es refereix només al cardinal numerable i abreujarem $\widetilde{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$; per suposat considerarem $n < \infty$, per a tot $n \in \mathbb{N}$. Usarem el llenguatge habitual d'intervals per a representar els segments a $\widetilde{\mathbb{N}}$, per exemple $[p,q) = \{ n \in \widetilde{\mathbb{N}} \mid p \leq n < q \}$; en particular, $\mathbb{N} = [0,\infty)$ i $\widetilde{\mathbb{N}} = [0,\infty]$.

Per a tot grup $G$ i tot parell de subconjunts $A, B \subseteq G$, designarem $[A,B]$ el conjunt de commutadors d'elements de $A$ amb elements de $B$ (i *no* el subgrup generat per ells). Si $H$ és un subgrup de $G$, es designarà $H\backslash G$ i $G/H$ els conjunts de classes laterals $(Hg)$ per la dreta i $(gH)$ per l'esquerra, respectivament.

El grup lliure de rang $n$ (on $n \in \widetilde{\mathbb{N}}$) es designarà $F_n$ i els seus elements mitjançant lletres minúscules, habitualment llatines del final de l'alfabet "$u, v, w, \ldots$" si són paraules en termes dels generadors originals, i gregues amb grafies similars a les anteriors "$\nu, \omega, \ldots$", si són paraules en algun altre sistema de generadors. Quan vulguem fer explícit sobre quin conjunt de símbols s'està considerant una paraula, l'especificarem entre parèntesi a continuació del nom; per exemple amb $w(x_1, \ldots, x_n)$ indiquem que $w$ és una paraula en $\{x_1, \ldots, x_n\}^{\pm}$. Escriurem $|w|$ la longitud de $w$, i $|w|_{x_i}$ (o simplement $|w|_i$ si el conjunt de generadors és conegut) el nombre net d'aparicions del símbol $x_i$ a la paraula $w = w(x_1, \ldots, x_n)$.

Els morfismes de $F_n$ els representarem mitjançant lletres gregues minúscules "$\phi, \psi, \theta, \ldots$", i, per a les aplicacions en general, usarem el conveni de representar-les actuant per la dreta; així doncs escriurem $(w)\phi$ (o simplement $w\phi$) la imatge de $w$ per l'aplicació $\phi$.

Els elements de $\mathbb{Z}^m$ es representaran amb lletres minúscules en negreta "$\mathbf{a}, \mathbf{b}, \ldots, \mathbf{u}, \mathbf{v}, \ldots$", amb el conveni que les versions en negreta de les lletres que designin paraules lliures representen les respectives abelianitzacions; és a dir, si $u \in F_n$, aleshores $\mathbf{u} = u^{\mathrm{ab}} = (\,|u|_1, \ldots, |u|_n) \in \mathbb{Z}^n$. En el cas de tenir una família indexada de vectors, escriurem els subíndexs també en negreta, per a poder diferenciar l'$i$-èssim vector $\mathbf{u_i}$, de la $i$-èssima component del vector $\mathbf{u}$, $\mathbf{u}_i$.

Similarment, representarem les matrius mitjançant lletres llatines majúscules en negreta "$\mathbf{A}, \mathbf{P}, \mathbf{Q}, \ldots$", i donat que usem el conveni general de fer actuar les aplicacions per la dreta, entendrem per defecte els vectors $\mathbf{a} \in \mathbb{Z}^m$ com a matrius fila. Donada una matriu $\mathbf{A}$, les seves fila $i$-èssima i col.lumna

$j$-èssima les designarem respectivament $\mathbf{A}_{i\bullet}$ i $\mathbf{A}_{\bullet j}$. La matriu identitat de rang $m$ la designarem $\mathbf{I_m}$.

Per als elements del grup $G = F_n \times \mathbb{Z}^m = \langle\, X \mid \rangle \times \langle T \mid [T,T]\,\rangle$, tindrem una forma normal del tipus $t_1^{a_1} \cdots t_m^{a_m}\, u$, on $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ i $u \in F_n$. Usarem la notació $\mathbf{t^a}$ per abreujar $t_1^{a_1} \cdots t_m^{a_m}$ i donar als elements de $F_n \times \mathbb{Z}^m$ l'aspecte més compacte $\mathbf{t^a}\, u$.

Anomenarem $\pi$ i $\tau$ a les projeccions 'lliure' i 'lliure-abeliana' de $G = F_n \times \mathbb{Z}^m$, concretament

$$\begin{array}{rcl} \pi\colon G & \longrightarrow & \langle X\rangle_G \cong F_n \\ \mathbf{t^a}\, u & \longmapsto & u \end{array} \quad \text{i} \quad \begin{array}{rcl} \tau\colon G & \longrightarrow & \mathbb{Z}^m \cong \langle T\rangle_G \\ \mathbf{t^a}\, u & \longmapsto & \mathbf{a} \end{array}.$$

Notem l'abús de llenguatge en el nom de les aplicacions anteriors, similar al comès referint-nos (com farem sovint) als subgrups $\langle X\rangle_G$ i $\langle T\rangle_G$ com *la part lliure* i *la part lliure-abeliana* de $G$ respectivament – tot i que podem trobar a $G$ moltes altres 'parts' (subgrups) lliures del mateix rang que $\langle X\rangle_G$ i 'parts' (subgrups) lliure-abelians de rang fins i tot superior al de $\langle T\rangle_G$. En la mateixa línia, de vegades ens referirem informalment a $u$ com *la part lliure*, i a $\mathbf{a}$ com *la part lliure-abeliana*, de l'element $\mathbf{t^a}\, u \in F_n \times \mathbb{Z}^m$.

Pel que fa als morfismes de $F_n \times \mathbb{Z}^m$, els representarem mitjançant lletres gregues majúscules "$\Psi, \Theta, \ldots$" i els considerarem, com sempre, actuant per la dreta.

# Índex general

# Part 1

# Grups lliure per lliure-abelià

# Capítol 1
# Estructura

## 1. Generalitats

Siguin $X = \{ x_i \mid i \in I \}$ i $T = \{ t_j \mid j \in J \}$ conjunts disjunts (de símbols) amb cardinal numerable o finit i considerem el grup $G$ donat per la presentació $\langle X, T \mid [X \sqcup T, T] \rangle$, on $[A, B]$ designa el conjunt de commutadors d'elements de $A$ amb elements de $B$. Anomenant $F$ i $Z$ als subgrups generats (a $G$) per $X$ i $T$ respectivament, és clar que $F$ és lliure amb base $X$, $Z$ lliure-abelià amb base $T$, i $G$ el seu producte directe; és a dir

$$G = F \times Z = \langle X, T \mid [X \sqcup T, T] \rangle . \tag{1}$$

Definició 1.1. Direm que un grup és *lliure per lliure-abelià* si és isomorf a algun dels donats per les presentacions del tipus (1).

Observem que les relacions a (1) no fan més que establir la commutativitat dels generadors $t_j$ amb els $x_i$ i entre ells. Podem, per tant, donada una paraula en els generadors, redistribuir ordenadament les $t_j$'s a l'esquerra obtenint per a cada element de $F \times Z$ un representant de la forma $\mathbf{t}\, w$.

És clar que l'abelianitzat d'aquests grups, obtingut sense més que incorporar els commutadors $[X, X]$ a la llista de relators tindrà presentació

$$G^{\mathrm{ab}} = \langle X, T \mid [X \sqcup T, X \sqcup T] \rangle$$

i és, per tant, lliure-abelià amb base $X \sqcup T$.

En particular, si els cardinals $n = |X|$ i $m = |T|$ són finits, l'expressió (1) es pot escriure, més explícitament,

$$F_n \times \mathbb{Z}^m = \left\langle x_1, \ldots, x_n, t_1, \ldots, t_m \;\middle|\; \begin{array}{ll} t_k^{-1} x_i t_k = x_i & i \in [1, n],\ k \in [1, m] \\ t_k^{-1} t_j t_k = t_j & j, k \in [1, m] \end{array} \right\rangle , \tag{2}$$

el seu abelianitzat serà $\mathbb{Z}^{n+m}$, i tenim per als seus elements la forma normal establerta a continuació.

Lema 1.1. *El conjunt de paraules de la forma*

$$t_1^{a_1}\cdots t_m^{a_m}\,u \quad amb \quad \mathbf{a}=(a_1,\ldots,a_m)\in\mathbb{Z}^m \ \ i\ u\in F_n,$$

*que escrivint* $t_1^{a_1}\cdots t_m^{a_m} =: \mathbf{t}^{\mathbf{a}}$ *podem abreujar*

$$\mathbf{t}^{\mathbf{a}}\,u\ , \quad amb \quad \mathbf{a}\in\mathbb{Z}^m \ \ i\ u\in F_n, \tag{3}$$

*constitueixen una forma normal dels elements de* $F_n\times\mathbb{Z}^m$. □

Demostració. Com ja hem dit, la commutativitat dels $t_j$ amb els $x_i$ i entre ells permet agrupar ordenadament les $t_j$'s a l'esquerra obtenint per a qualsevol paraula en els generadors una expressió de la forma (3). La unicitat és conseqüència immediata de tractar-se d'un producte directe de paraules en $X$ per paraules en $T$, per a cadascuna de les quals usem les formes normals estàndard. □

Com és evident, $t_j = \mathbf{t}^{\boldsymbol{\delta}_j}$ amb $\boldsymbol{\delta_j} = (0,\ldots,\overset{j)}{1},\ldots,0)$. Resumim en el lema següent les propietats elementals de les formes normals amb la nova notació.

Lema 1.2. *Siguin* $u,v,u_l\in F_n$ *i* $\mathbf{a},\mathbf{b},\mathbf{a_l}\in\mathbb{Z}^m$ *amb* $l\in L$ *conjunt finit d'índexs, aleshores*

(a) $(\mathbf{t}^{\mathbf{a}}\ u)(\mathbf{t}^{\mathbf{b}}\ v)=\mathbf{t}^{\mathbf{a}+\mathbf{b}}\ uv$,
(b) $\prod_l(\mathbf{t}^{\mathbf{a_l}}\ u_l)=\mathbf{t}^{\sum_l\mathbf{a_l}}\ \prod_l u_l$,
(c) $(\mathbf{t}^{\mathbf{a}}\ u)^p=\mathbf{t}^{p\,\mathbf{a}}\ u^p$. □

Tot i que l'objecte inicial d'estudi en el que segueix són els grups lliure per lliure-abelià *finitament generats* (donats per presentacions del tipus (2)), apareixeran de forma natural grups lliure per lliure-abelià més generals (de rang lliure numerable) com a subgrups seus. Degut a això, sovint convindrà considerar també dintre del nostre àmbit els grups del tipus $F_n\times\mathbb{Z}^m$ amb $n=\infty$. Molts dels resultats inicials (no algorísmics) sobre subgrups són vàlids pràcticament sense modificacions amb aquesta extensió, que constitueix potser l'ambient més natural sobre el qual establir-los. Per exemple, tant les presentacions (2) com els lemes anteriors referents a l'existència i comportament de formes normals s'escriuen de manera gairebé idèntica en el cas $n=\infty$. Designarem $\mathcal{G}$ la família formada pels grups lliure per lliure-abelià finitament generats i $\widetilde{\mathcal{G}}$ la superfamília que inclou factors lliures de rang numerable, és a dir

$$\mathcal{G}=\{\,F_n\times\mathbb{Z}^m \mid n,m\in\mathbb{N}\,\}\ \text{i}$$
$$\widetilde{\mathcal{G}}=\{\,F_n\times\mathbb{Z}^m \mid n\in\widetilde{\mathbb{N}},m\in\mathbb{N}\,\}.$$

on hem usat $\widetilde{\mathbb{N}}$ per a designar $\mathbb{N}\cup\{\infty\}$. En ocasions, quan un enunciat sigui independent de si $n$ inclou o no el cas infinit (és a dir, de si estem a $\widetilde{\mathcal{G}}$ o a $\mathcal{G}$), per a evitar haver de duplicar-lo, les condicions que hagi de complir $n$ es donaran genèricament ($n$ es sobreentendrà dintre de l'interval corresponent en cadascun dels dos casos). Interpretant la presentació (2) i els lemes 1.1 i 1.2 amb aquest conveni obtenim les seves versions ampliades amb el cas $n = \infty$.

En la següent observació es mostra una duplicitat natural en la descripció de les famílies anteriors que comporta l'aparició d'un cas degenerat no trivial (amb $n, m \neq 0$) que precisarà de la nostra atenció.

Observació 1. Notem que per a $n = 1$ és

$$F_1 \times \mathbb{Z}^m \cong \mathbb{Z}^{m+1} \cong F_0 \times \mathbb{Z}^{m+1} \tag{4}$$

obtenint dues representacions diferents del tipus $F_n \times \mathbb{Z}^m$ per a la mateixa classe d'isomorfia i per tant certa redundància en la descripció d'aquests grups; veurem més endavant (proposició 2.6) que aquestes són les úniques redundàncies entre els grups $F_n \times \mathbb{Z}^m$. Així doncs, des d'un punt de vista estrictament algebraic el cas $n = 1$ no és essencialment diferent del cas degenerat $n = 0$ i podrem considerar-lo també com a tal, fusionant els dos casos quan sigui convenient per a simplificar la casuística. Una forma de fer-ho és excloure els casos amb $n = 1$ de les famílies $\mathcal{G}$ i $\widetilde{\mathcal{G}}$. No obstant això, subgrups amb 'aspecte' $F_1 \times \mathbb{Z}^{m'}$ emergiran de forma natural tot i l'exclusió, i obligaran a un seguiment especial en certs punts de l'anàlisi que segueix.

Lema 1.3. *$F_n \times \mathbb{Z}^m$ és abelià (i lliure-abelià) si i només si $n = 0, 1$.*

Demostració. La implicació cap a l'esquerra és evident en vista de l'observació anterior. Per a l'altra només cal recordar que $F_n$ (i per tant $F_n \times \mathbb{Z}^m$) no és abelià si $n \geq 2$. □

## 2. Subgrups

És immediat comprovar que tot producte directe de subgrups respectius dels factors d'un producte directe n'és subgrup. En el nostre cas aquest fet ens proporciona, quan $n \neq 0, 1$, subgrups de $F_n \times \mathbb{Z}^m$ de la forma $F_{n'} \times \mathbb{Z}^{m'}$ amb $n' \in [0, \infty]$ i $m' \in [0, m]$. Veurem a continuació que tots els subgrups de $F_n \times \mathbb{Z}^m$ són isomorfs a algun d'aquests i per tant la família anterior descriu (no unívocament) les classes d'isomorfia dels subgrups de $F_n \times \mathbb{Z}^m$, amb les excepcions al.ludides.

Potser convé notar, en aquest punt, que no tots els subgrups de $F_n \times \mathbb{Z}^m$ són producte directe de subgrups dels factors i per tant l'enunciat que segueix no és trivial.

Exemple 1. Considerem a $F_2 \times \mathbb{Z} = \langle\, a, b \mid \,\rangle \times \langle\, t \mid \,\rangle$ el subgrup generat per l'element $ta$. És clar que $\langle ta \rangle = \{\, t^n a^n \mid n \in \mathbb{Z} \,\}$ té intersecció trivial amb $\langle\, a, b \mid \,\rangle$ i $\langle\, t \mid \,\rangle$ i per tant no és producte directe de subgrups respectius dels factors $F_n$ i $Z^m$.

Proposició 2.1. *La família $\widetilde{\mathcal{G}}$ és tancada per subgrups. Concretament, si $H$ és subgrup de $F_n \times \mathbb{Z}^m \in \widetilde{\mathcal{G}}$, aleshores existeixen $n' \in [0, \infty]$ i $m' \in [0, m]$ tals que $H \cong F_{n'} \times \mathbb{Z}^{m'}$.*

Demostració. Si $n = 0, 1$, aleshores $F_n \times \mathbb{Z}^m$ és lliure-abelià, tots els seus subgrups són lliure-abelians de rang no superior al de l'ambient i el resultat es segueix de forma immediata.

Per $n \geq 2$ considerem en primer lloc la següent successió exacta curta natural associada al producte directe $F_n \times \mathbb{Z}^m$

$$1 \longrightarrow \mathbb{Z}^m \xrightarrow{\iota} F_n \times \mathbb{Z}^m \xrightarrow{\pi} F_n \longrightarrow 1$$

on $\iota$ és la inclusió, $\pi$ la projecció $\mathbf{t^a}u \mapsto u$ i per tant $\ker(\pi) = \mathbb{Z}^m = \mathrm{im}(\iota)$. Sigui ara $\pi_{|H}$ la restricció de $\pi$ a $H$ subgrup de $F_n \times \mathbb{Z}^m$

$$H \xrightarrow{\pi_{|H}} H\pi.$$

És clar que $\ker(\pi_{|H}) = H \cap \ker(\pi) = H \cap \mathbb{Z}^m$, i que $H\pi \leqslant F_n$ i en conseqüència $H\pi$ és lliure de rang $n' \in [0, \infty]$. Sigui $\{y_\nu\}_\nu$ una base (que pot ser buida) de $H\pi$ i considerem $\forall \nu$, un element de $H$ (que anomenarem $\widetilde{y}_\nu$) amb part lliure igual a $y_\nu$ (és a dir triem, per a tot $\nu$, un $\widetilde{y}_\nu \in (\pi_{|H})^{-1}(y_\nu)$). Aleshores l'aplicació $y_\nu \overset{\alpha}{\longmapsto} \widetilde{y}_\nu$ és ben definida entre $\{y_\nu\}_\nu$ i $H$, i en ser $\{y_\nu\}_\nu$ base de $H\pi$, estén de forma única a un morfisme

$$H \xleftarrow{\alpha} H\pi \tag{5}$$

per al qual es comprova trivialment que $\alpha\,\pi_{|H} = \mathrm{id}_{H\pi}$ i per tant és injectiu. Obtenim així un subgrup $H\pi\alpha \leqslant H$ isomorf a $H\pi$ i per tant lliure de rang $n' \in [0, \infty]$. D'altra banda, com ja hem comentat, $\ker(\pi_{|H}) = H \cap \mathbb{Z}^m$ és subgrup de $\mathbb{Z}^m$ i per tant isomorf a $\mathbb{Z}^{m'}$ amb $m' \in [0, m]$.

En definitiva, tenim a $H$ els subgrups $H\pi\alpha$ lliure de rang $n' \in [0, \infty]$ i $\ker(\pi_{|H})$ lliure-abelià de rang $m' \in [0, m]$. Vegem a continuació que estan en producte directe. Concretament veurem que l'aplicació

$$\begin{array}{rcl} \Theta_\alpha : H & \longrightarrow & H\pi\alpha \;\times\; \ker(\pi_{|H}) \\ h & \longmapsto & (h\pi\alpha \;,\; (h\pi\alpha)^{-1}h) \end{array} \tag{6}$$

estableix un isomorfisme entre $H$ i el producte directe dels subgrups considerats. En efecte, l'aplicació està ben definida, la primera component trivialment i per la segona només cal observar que en ser $\alpha\,\pi_{|H} = \mathrm{id}_{H\pi}$, tenim $\forall h \in H$

$$((h\pi\alpha)^{-1}h)\pi = (h^{-1})\pi\alpha\pi\,(h)\pi = (h^{-1})\pi\,(h)\pi = 1.$$

També és clar que $\Theta_\alpha$ és morfisme

$$\begin{array}{rcl}(h_1h_2)\Theta_\alpha & = & ((h_1h_2)\pi\alpha, ((h_1h_2)\pi\alpha)^{-1}h_1h_2) \\ & = & (h_1\pi\alpha\ h_2\pi\alpha, (h_2\pi\alpha)^{-1}\,(h_1\pi\alpha)^{-1}h_1h_2) \\ & = & (h_1\pi\alpha\ h_2\pi\alpha, (h_1\pi\alpha)^{-1}h_1\,(h_2\pi\alpha)^{-1}h_2) \\ & = & (h_1\pi\alpha, (h_1\pi\alpha)^{-1}h_1)\,(h_2\pi\alpha, (h_2\pi\alpha)^{-1}h_2) \\ & = & (h_1)\Theta_\alpha\,(h_2)\Theta_\alpha\end{array}$$

on hem usat que tant $\pi$ com $\alpha$ són morfismes i la total commutativitat de les segones components (que recordem formaven un subgrup de $\mathbb{Z}^m$, que és al centre de $F_n \times \mathbb{Z}^m$). Comprovem per últim que l'aplicació $\Upsilon\colon (h,k) \mapsto hk$ és inversa de $\Theta_\alpha$. En efecte, és immediat de les definicions que $\Theta_\alpha \Upsilon = \mathrm{id}_H$ i, com que $\alpha\,\pi_{|H} = \mathrm{id}_{H\pi}$, tenim $\forall h \in H$, $\forall k \in \ker(\pi_{|H})$, $(h\pi\alpha\ k)\pi\alpha = h\pi\alpha$ i per tant

$$\begin{array}{rcl}(h\pi\alpha, k)\Upsilon\Theta_\alpha & = & (h\pi\alpha\cdot k)\Theta_\alpha \\ & = & ((h\pi\alpha\cdot k)\pi\alpha, ((h\pi\alpha\cdot k)\pi\alpha)^{-1}\cdot h\pi\alpha\cdot k) \\ & = & (h\pi\alpha, (h\pi\alpha)^{-1}\cdot h\pi\alpha\cdot k) \\ & = & (h\pi\alpha, k)\end{array}$$

Així doncs, també $\Upsilon\Theta_\alpha = \mathrm{id}_{H\pi\alpha\times\ker(\pi_{|H})}$ i $\Upsilon$ és inversa de $\Theta_\alpha$, que és per tant bijectiva. En definitiva, hem obtingut un isomorfisme $\Theta_\alpha$ entre $H$ i el producte directe d'un subgrup seu isomorf a $F_{n'}$ i un altre isomorf a $\mathbb{Z}^{m'}$ amb $n' \in [0,\infty]$ i $m' \in [0,m]$, tal i com volíem demostrar. □

De fet, la demostració anterior proporciona, donat un subgrup $H$, una forma concreta (i algorísmica si ho són la descripció de $H$ i l'obtenció de l'escissió $\alpha$) de descompondre $H$ com a producte directe d'un subgrup lliure i un subgrup lliure-abelià.

Corol.lari 2.2. *Si $H$ és subgrup de $F_n \times \mathbb{Z}^m \in \widetilde{\mathcal{G}}$, aleshores*

$$H = H\pi\alpha \times (H \cap \mathbb{Z}^m),$$

*on $\alpha$ és una escissió de $\pi_{|H}$ definida com a (5). Anomenarem a $H\pi\alpha$ i $H\cap\mathbb{Z}^m$ respectivament, factors lliure i lliure-abelià de $H$ segons l'escissió $\alpha$.*

Demostració. L'argument usat a la demostració anterior per als casos amb $n \geq 2$ és vàlid també per $n = 0, 1$ amb les corresponents correccions a l'interval de rangs assolibles per $H\pi$. □

És evident per construcció que, en cas de no ser trivials, el factor lliure per una escissió tindrà una base constituïda per paraules en $X \cup T$ en les que apareixeran necessàriament lletres pertanyents a $X$, mentre que el factor lliure-abelià tindrà una base formada per paraules només en $T$.

Observació 2. D'acord amb l'observació 1, si el rang de $H\pi\alpha$ és 1, aleshores $H$ és lliure-abelià de rang $m'+1$ (tot i que el factor lliure-abelià de $H$ *segons* *l'escissió* $\alpha$ té rang $m'$). En aquesta situació sovint serà convenient (ho serà per exemple en la nostra definició de base) pensar el factor lliure segons $\alpha$, $H\pi\alpha$, com a absorbit pel factor lliure-abelià $H \cap \mathbb{Z}^m$. Remarquem que aquest cas comporta, per tant, certa molesta dualitat en la interpretació dels adjectius "lliure" i "lliure-abelià" quan li són aplicats: com a grup, $H$ té 'part lliure' de rang 1 i 'part lliure-abeliana' de rang $m' + 1$ (la part lliure inclosa a la lliure-abeliana); mentre que com a subgrup de $G$ *segons qualsevol escissió*, $H$ té 'factor lliure' de rang 1 i 'factor lliure-abelià' de rang $m'$ (sempre disjunts).

COROL.LARI 2.3. *Un subgrup $H$ de $F_n \times \mathbb{Z}^m \in \widetilde{\mathcal{G}}$ és finitament generat si i només si la seva projecció $H\pi$ ho és.*

DEMOSTRACIÓ. De l'isomorfisme $H \cong H\pi\alpha \times \ker(\pi_{|H})$ a (6); donat que $\ker(\pi_{|H})$ és finitament generat (subgrup de $\mathbb{Z}^m$), $H$ ho serà si i només si ho és $H\pi\alpha$, i (com que $\alpha$ és injectiva) equivalentment $H\pi$. □

OBSERVACIÓ 3. Si $H$ (o equivalentment $H\pi$) ve donat per una família finita de generadors $\{ h_1, \ldots, h_s\}$ podem calcular (usant transformacions de Nielsen o Stallings foldings) una base $\{y_\nu\}_\nu$ de $H\pi$ (evidentment finita). Vegem que aleshores també és possible obtenir algorísmicament una escissió $\alpha$ (i per tant una base de $H\pi\alpha$):

- per *força bruta*: donat que disposem d'un conjunt finit de generadors, podem enumerar els elements de $H$ (considerant, per exemple, l'ordenació donada per la longitud de la paraula reduïda seguida d'un ordre lexicogràfic) i fer que l'algorisme recorri $H$ seguint aquest ordre buscant successivament antiimatges dels respectius $y_\nu$. L'exhaustivitat de $\pi\colon H \to H\pi$ garanteix l'existència de tals antiimatges, l'enumerabilitat de $H$ l'assoliment d'alguna d'elles (que prendrem com a imatge de $y_\nu$ per $\alpha$), i la finitud de $\{y_\nu\}_\nu$ la finalització del procés.
- de forma no tan grollera: podem aprofitar que el procés d'obtenció de la base $\{y_\nu\}_\nu$ és reversible per aconseguir (de forma no necessàriament única) una expressió $w_\nu(h_1\pi, \ldots, h_s\pi)$ de cada $y_\nu$ com a paraula en $\{ h_1\pi, \ldots, h_s\pi \}^{\pm}$. Aleshores és suficient definir $\alpha\colon y_\nu \mapsto w_\nu(h_1, \ldots, h_s)$.

Conseqüència directa de la proposició 2.1 i un fet elemental referent als subgrups d'un producte directe tenim que, fora de la ben coneguda situació lliure-abeliana (corresponent als casos $F_0 \times \mathbb{Z}^m$ i $F_1 \times \mathbb{Z}^m$), els subgrups de $F_n \times \mathbb{Z}^m$ recorren totes les formes referides a la proposició. La casuística queda resumida en el següent lema.

COROL.LARI 2.4. *(i) Els subgrups de $\mathbb{Z}^m$ són isomorfs a $\mathbb{Z}^{m'}$ amb $m' \in [0, m]$ i totes les formes són assolides.*

*(ii) Els subgrups de $F_n \times \mathbb{Z}^m$ ($n \in [2, \infty]$) són isomorfs a $F_{n'} \times \mathbb{Z}^{m'}$ amb $n' \in [0, \infty]$ i $m' \in [0, m]$ i totes les formes són assolides.*

Demostració. (i) El cas lliure-abelià és ben conegut.

(ii) Que els subgrups són de les formes donades no és més que l'enunciat de la proposició 2.1. Per veure que totes són assolides, és a dir, que per a cadascuna hi ha un subgrup isomorf a ella, només cal recordar que tot producte directe de subgrups respectius dels factors d'un producte directe n'és subgrup. Ara, com que hi ha subgrups de $F_n$ ($n \in [2,\infty]$) isomorfs a $F_{n'}$ per a tot $n' \in [0,\infty]$, i subgrups de $\mathbb{Z}^m$ isomorfs a $\mathbb{Z}^{m'}$ per a tot $m' \in [0,m]$, obtenim en cada cas (fent el seu producte directe) un subgrup de $F_n \times \mathbb{Z}^m$ isomorf a cadascun dels de l'enunciat. □

També és immediat de la proposició 2.1 el següent resultat que usarem a continuació per a caracteritzar les classes d'isomorfia dels nostres grups.

Corol.lari 2.5. *El màxim rang d'un subgrup abelià de $F_n \times \mathbb{Z}^m$ és $m$ si $n = 0$, i $m+1$ si $n \in [1,\infty]$.*

Demostració. Per a $n = 0, 1$, els grups $F_n \times \mathbb{Z}^m$ són lliure-abelians de rangs $m$ i $m+1$ respectivament i el resultat es segueix de forma immediata. En els casos en què $n \geq 2$, acabem de veure que els grups $F_{n'} \times \mathbb{Z}^{m'}$ amb $n' \in [0,\infty]$ i $m' \in [0,m]$ constitueixen una família completa de classes d'isomorfia dels subgrups de $F_n \times \mathbb{Z}^m$. Ara només cal observar que $F_1 \times \mathbb{Z}^m$ és abelià de rang $m+1$, més gran o igual que el de la resta de subgrups abelians de $F_n \times \mathbb{Z}^m$ (els $F_\epsilon \times \mathbb{Z}^{m'}$ amb $\epsilon = 0,1$ i $m' \in [0,m]$). □

Estem ja en condicions de demostrar un resultat natural que, malgrat estar latent de forma intuïtiva des de la pròpia definició, encara no havíem provat. Notem que, tot i l'aparent perogrullada, cal fer l'excepció "$n \neq 1$" (veure observació 1) per tal que l'enunciat tingui validesa.

Proposició 2.6. *Donats $n, n' \in \widetilde{\mathbb{N}} \setminus \{1\}$, i $m, m' \in \mathbb{N}$ aleshores*

$$F_n \times \mathbb{Z}^m \cong F_{n'} \times \mathbb{Z}^{m'} \;\Leftrightarrow\; n = n' \text{ i } m = m'$$

Demostració. [$\Leftarrow$] La implicació cap a l'esquerra és evident.

[$\Rightarrow$] Per a provar l'implicació cap a la dreta observem en primer lloc que si els grups donats són isomorfs, o bé ambdós són abelians i per tant $n = n' = 0$ (ja que hem exclòs els productes amb $n$ o $n'$ igual a 1), o bé ambdós són no abelians i $n, n' \geq 2$. En qualsevol dels casos, donat que els màxims rangs d'un subgrup abelià de grups isomorfs han de coincidir, del corol.lari 2.5 es dedueix que $m = m'$.

D'altra banda, com que tot grup isomorf a un de finitament generat és finitament generat, és clar que en la situació de l'enunciat, o bé $n = n' = \infty$ o bé tant $n$ com $n'$ són quantitats finites. En el primer cas ja hem acabat. En el segon, abelianitzant l'isomorfisme $F_n \times \mathbb{Z}^m \cong F_{n'} \times \mathbb{Z}^{m'}$ de partida obtenim

$\mathbb{Z}^{n+m} \cong \mathbb{Z}^{n'+m'}$, d'on $n+m = n'+m'$ i (usant que $m = m'$) podem concloure que $n = n'$. □

Recordem que l'exclusió "$n \neq 1$" no suposa cap pèrdua de generalitat ($F_1 \times \mathbb{Z}^m \cong F_0 \times \mathbb{Z}^{m+1}$) en l'abast de la proposició, que per tant inclou tots els grups que estem considerant i en proporciona una descripció no redundant. És a dir,

Corol.lari 2.7. *Els grups $F_n \times \mathbb{Z}^m$ amb $n \in \mathbb{N} \setminus \{1\}$ (resp. $n \in \widetilde{\mathbb{N}} \setminus \{1\}$) i $m \in \mathbb{N}$ constitueixen un sistema complet de representants de les classes d'isomorfia de $\mathcal{G}$ (resp. $\widetilde{\mathcal{G}}$).* □

És clar que es pot escollir altres sistemes de representants; l'anterior però, té l'avantatge d'aglutinar el centre en un únic factor i sovint l'usarem implícitament a partir d'ara. Queda, per tant justificada la utilització dels grups $F_n \times \mathbb{Z}^m$ ($n \neq 1$) com a model particular de grup lliure per lliure-abelià amb el benentès que cadascun d'ells, a més, representa una classe diferent a les representades per la resta dels membres de la família. Comentem a continuació en què es tradueix aquest fet a l'inventari de subgrups d'un grup lliure per lliure-abelià.

Havíem vist al corol.lari 2.4 que els grups $F_{n'} \times \mathbb{Z}^{m'}$ amb $n' \in [0, \infty]$ i $m' \in [0, m]$ constitueixen una família completa de classes d'isomorfia dels subgrups de $F_n \times \mathbb{Z}^m$ ($n \geq 2$). Podem usar de nou la proposició 2.6 per refinar aquest resultat extraient-ne un sistema complet de representants (sense redundàncies). Per suposat també tindrem la corresponent versió abeliana quan $n = 0, 1$.

Proposició 2.8. *(i) La família $\{\, \mathbb{Z}^{m'} \mid m' \in [0, m] \,\}$ constitueix un sistema complet de representants de les classes d'isomorfia dels subgrups de $\mathbb{Z}^m$.*

*(ii) La família $\{\, \mathbb{Z}^{m'} \mid m' \in [0, m{+}1] \,\}$ (resp. $\{\, F_{n'} \times \mathbb{Z}^{m'} \mid n' \in [2, \infty], m' \in [0, m] \,\}$) constitueix un sistema complet de representants de les classes d'isomorfia dels subgrups* abelians *(resp.* no abelians*) de $F_n \times \mathbb{Z}^m$ amb $n \geq 2$.*

Demostració. (i) El cas lliure-abelià és ben conegut (veure, per exemple, [**1**] cap. 5).

(ii) és directe del corol.lari 2.4, la proposició 2.6 i l'observació 1. □

## 3. Rang i bases

La caracterització donada a la proposició 2.6 matisa la definició de grup lliure per lliure-abelià proporcionant un sistema (no redundant) de representants de les classes d'isomorfia a $\widetilde{\mathcal{G}}$. Concretament, per a cada parell

$$(n,m) \in \widetilde{\mathbb{N}} \times \mathbb{N} \text{ amb } n \neq 1,$$

tindrem una classe a $\widetilde{\mathcal{G}}$ distingida (isomorfa a $F_n \times \mathbb{Z}^m$), i aquestes són totes. Podrem, per tant, referir-nos unívocament i amb total generalitat a les classes d'isomorfia dels nostres grups mitjançant aquest parell de nombres. Aquesta situació (que recorda molt a la que es produeix amb els grups lliures i lliure-abelians) juntament amb el lema posterior comporten la següent definició.

DEFINICIÓ 3.1. Donat un grup $G \in \widetilde{\mathcal{G}}$, acabem de veure que existeixen $n \neq 1$ i $m$ únics, tals que $G \cong F_n \times \mathbb{Z}^m$; amb un abús de llenguatge que justificarem a continuació, anomenarem *rang escindit* de $G$ al parell $(n,m)$, mentre que a $n$ i $m$ els anomenarem respectivament *components lliure i lliure-abeliana* del rang (escindit) de $G$.

Vegem que la definició que acabem de donar és coherent amb la definició estàndard de rang (cardinal del mínim nombre de generadors).

LEMA 3.1. *El rang (estàndard) de $F_n \times \mathbb{Z}^m \in \widetilde{\mathcal{G}}$ és $m+n$.*

DEMOSTRACIÓ. Volem veure que el mínim dels cardinals dels conjunts que generen $F_n \times \mathbb{Z}^m$ és $m+n$. La presentació (2) (amb $n$ possiblement infinit) proporciona un sistema de $n+m$ generadors, així doncs n'hi haurà prou amb comprovar que qualsevol altre conjunt de generadors té un cardinal igual o superior. En efecte, donat $S$ un conjunt de generadors de $F_n \times \mathbb{Z}^m$, la seva imatge $S^{\text{ab}}$ a l'abelianització $(F_n \times \mathbb{Z}^m)^{\text{ab}} = \mathbb{Z}^{n+m}$ l'ha de generar, i per tant ha de ser $|S| \geq |S^{\text{ab}}| \geq n+m$. □

És a dir, podem pensar el rang escindit com un refinament del rang estàndard per als nostres grups en el que especifiquem les contribucions lliure i lliure-abeliana. En vista d'això, per simplificar el llenguatge, usarem el terme 'rang' (ometent el qualificatiu) sempre que el context o la pròpia notació evitin qualsevol possible confusió entre ambdues versions (per exemple parlarem de les components lliure i lliure-abeliana del rang i escriurem expressions com ara "$\operatorname{rang}(G) = (n,m)$" entenent en ambdós casos que es tracta del rang escindit).

Amb la nova definició i les consideracions prèvies podem rellegir la proposició 2.6 afirmant que dos grups de $\widetilde{\mathcal{G}}$ són isomorfs si i només si els seus rangs escindits coincideixen. Aquesta caracterització, evidentment també vàlida per a $\mathcal{G}$, proporciona fàcilment la decidibilitat del *isomorphism problem* en aquest darrer cas.

COROL.LARI 3.2. *L'*isomorphism problem *a $\mathcal{G}$ és decidible.*

Demostració. Siguin dos grups pertanyents a $\mathcal{G}$ donats per presentacions finites $\langle X \mid R\rangle$ i $\langle Y \mid S\rangle$. D'acord amb el corol.lari 2.7, hauran de ser respectivament isomorfs als determinats per presentacions finites (diem-ne $\mathcal{P}_{n,m}$ i $\mathcal{P}_{n',m'}$) de tipus (2) amb $n, n' \neq 1$. Aleshores, sabem que existiran seqüències finites de transformacions de Tietze simples de $\langle X \mid R\rangle$ a $\mathcal{P}_{n,m}$ i de $\langle Y \mid S\rangle$ a $\mathcal{P}_{n',m'}$. Ara, podem engegar dos procediments diagonals que recorrin respectivament totes les transformacions de Tietze simples aplicables successivament a cadascuna de les presentacions inicials. En vista del que acabem de comentar ambdós procediments necessàriament arribaran en temps finit a les presentacions $\mathcal{P}_{n,m}$ i $\mathcal{P}_{n',m'}$ respectivament. Un cop aquí, només caldrà aplicar la proposició 2.6 per concloure que $\langle X \mid R\rangle$ i $\langle Y \mid S\rangle$ presenten grups isomorfs si i només si $n = n'$ i $m = m'$. □

Revestint convenientment la idea darrera la nostra definició de rang, donem també, a continuació, una versió adaptada del concepte de base.

Definició 3.2. Un parell $(A, B)$ de subconjunts d'un grup $G \in \widetilde{\mathcal{G}}$ s'anomenarà *base de* $G$ si es compleixen les tres condicions següents:

(a) $A$ és buit o base d'un subgrup lliure no abelià de $G$ (remarquem que això exclou els casos amb $|A| = 1$),
(b) $B$ és base (abeliana) del centre de $G$, i
(c) $\langle A \cup B\rangle = G$.

En tal cas, direm també que $A$ i $B$ són respectivament les *components lliure i lliure-abeliana de la base* $(A, B)$. Observem que de les condicions (a), (b) i (c) es dedueixen immediatament

(d) $\langle A\rangle \cap \langle B\rangle = \{1\}$, i
(e) $A \cap B = \varnothing$

ja que $\langle A\rangle \cap \langle B\rangle$ està continguda al centre de $G$ i cap element no trivial de $\langle A\rangle$ hi pertany; i el neutre no pot formar part de cap base.

Observació 4. Sigui $G \in \widetilde{\mathcal{G}}$ un grup donat per la presentació (1), tenim dues possibilitats:

- si $|X| \neq 1$, aleshores $(X, T)$ és base de $G$, i
- si $|X| = 1$, aleshores $(\varnothing, X \sqcup T)$ és base de $G$.

Sovint, quan no sigui necessari fer explícit quina és la component lliure i quina la lliure-abeliana (o vulguem evitar complicacions derivades de la dualitat comentada a les observacions 1 i 2), abusarem del llenguatge dient que $A \sqcup B$ és base de $G$. És a dir, Definició 3.3. Sempre que anomenem un subconjunt $E \subseteq G$ base de $G$ lliure per lliure-abelià, estarem sobreentenent que $E = A \sqcup B$ amb $(A, B)$ base de $G$ en el sentit de la definició 3.2.

Remarquem que amb l'ús d'aquest conveni no estem perdent informació ja sempre podem recuperar $A$ i $B$ identificant a $E$ quines paraules utilitzen lletres en $X$: si són dues o més, $A$ estarà constituït per aquestes i $B$ per les que s'escriuen exclusivament en $T$; en cas contrari $A = \varnothing$ i $B = E$.

Aquest conveni simplifica considerablement alguns enunciats (per exemple a la darrera observació es pot fusionar els dos casos afirmant senzillament que $X \sqcup T$ és base de $\langle X, T \mid [X \sqcup T, T] \rangle$) i fa palès que la definició 3.2 no és més que una extensió dels conceptes estàndard de base lliure i lliure-abeliana. En efecte, en els casos degenerats (per als que el concepte de base ja existeix) la definició estàndard coincideix amb la nova definició de base, amb el conveni anterior.

Lema 3.3. *Si $G \in \widetilde{\mathcal{G}}$ és lliure no abelià (resp lliure-abelià), aleshores $E$ és base – en el sentit de 3.3 – de $G$ si i només si és base lliure (resp. lliure-abeliana) de $G$.* □

Donem a continuació una caracterització (potser més intuïtiva) de base d'un grup $G$ lliure per lliure-abelià.

Proposició 3.4. *Un parell $(A, B)$ de subconjunts de $G = F_n \times \mathbb{Z}^m$ $(n \neq 1)$ és base si i només si $G = \langle A \rangle \times \langle B \rangle$, amb $A$ base de $\langle A \rangle \cong F_n$ i $B$ base de $\langle B \rangle \cong \mathbb{Z}^m$. En particular, $|A| = n$ i $|B| = m$.*

Demostració. [$\Rightarrow$] Vegem en primer lloc que $G = \langle A \rangle \times \langle B \rangle$. Comencem observant que en ser el centre de $G$, $\langle B \rangle$ és subgrup normal de $G$. Per tant $\langle A \rangle$ i $\langle B \rangle$ commuten, $\langle A \rangle \langle B \rangle$ és subgrup de $G$ i, per (c), $G = \langle A \cup B \rangle = \langle A \rangle \langle B \rangle$. D'aquí obtenim fàcilment la normalitat de $\langle A \rangle$ en $G$. En efecte, en vista de l'anterior tindrem que per a tot $\tilde{a} \in \langle A \rangle$ i tot $g \in G$, existiran $a \in \langle A \rangle$ i $b \in \langle B \rangle$ tals que $g = ab$ i, per tant,

$$g^{-1} \tilde{a}\, g = (ab)^{-1} \tilde{a}\, ab = a^{-1} \tilde{a}\, a \in \langle A \rangle$$

on hem usat que $b \in \langle B \rangle = Z(G)$. Així doncs tant $\langle A \rangle$ com $\langle B \rangle$ són normals en $G = \langle A \cup B \rangle$. D'altra banda, de (d) la intersecció $\langle A \rangle \cap \langle B \rangle$ ha de ser trivial i per tant $G$ és producte directe de $\langle A \rangle$ i $\langle B \rangle$.

Ara, com que és $G = \langle A \rangle \times \langle B \rangle \cong F_n \times \mathbb{Z}^m$, els respectius centres han de ser isomorfs. Així doncs, $B$ és (per (b)) base lliure-abeliana de

$$\langle B \rangle = Z(G) \cong Z(F_n \times \mathbb{Z}^m) = \mathbb{Z}^m$$

i per tant de rang $m$; i $A$ (per (a)) base lliure de

$$\langle A \rangle \cong (\langle A \rangle \times \langle B \rangle) / \langle B \rangle \cong (F_n \times \mathbb{Z}^m) / \mathbb{Z}^m \cong F_n$$

i per tant de rang $n$, com volíem veure.

[$\Leftarrow$] La implicació cap a l'esquerra, i en conseqüència l'afirmació final sobre els cardinals, són immediates. $\square$

Reinterpretar la darrera proposició en el llenguatge de les presentacions aporta certa llum sobre tot l'esquema.

COROL.LARI 3.5. *Un parell $(A, B)$ de subconjunts d'un grup $G \in \widetilde{\mathcal{G}}$ és base de $G$ si i només si $|A| \neq 1$ i $G = \langle A, B \mid [A \sqcup B, B] \rangle$*

DEMOSTRACIÓ. [$\Rightarrow$] És directe de la definició que $|A| \neq 1$; i de la proposició 3.4, si $(A, B)$ és base de $G$, aleshores $\langle A \rangle = \langle A \mid \rangle$, $\langle B \rangle = \langle B \mid [B, B] \rangle$ i

$$G = \langle A \mid \rangle \times \langle B \mid [B, B] \rangle = \langle A, B \mid [A, B], [B, B] \rangle = \langle A, B \mid [A \sqcup B, B] \rangle$$

[$\Leftarrow$] Com hem comentat a l'observació 4, $(A, B)$ és trivialment base de $\langle A, B \mid [A \sqcup B, B] \rangle$, si $|A| \neq 1$. $\square$

Aquest corol.lari, més enllà d'un canvi de llenguatge, il.lustra la nostra definició de base com a entitat que fa canònica la definició inicial de grup lliure per lliure-abelià en termes de presentacions. I, en aquest sentit, suggereix la possibilitat d'una caracterització categòrica per als grups lliure per lliure-abelià i les seves bases, que assagem a continuació.

PROPOSICIÓ 3.6. *Siguin $G$ un grup i $A, B$ subconjunts disjunts de $G$ tals que els elements de $B$ commuten amb els de $A \sqcup B$, aleshores:*

*$G$ és lliure per lliure-abelià amb base $(A, B)$ si i només si $|A| \neq 1$ i per a tot grup $H$, tota aplicació $\varphi \colon A \sqcup B \to H$ tal que els elements de $B\varphi$ commutin amb els de $(A \sqcup B)\varphi$, estén de forma única a un morfisme $\widetilde{\varphi} \colon G \to H$.*

DEMOSTRACIÓ. [$\Rightarrow$] Si $G$ és lliure per lliure-abelià amb base $(A, B)$ evidentment $|A| \neq 1$ i podem prendre $\langle A, B \mid [A \sqcup B, B] \rangle$ com a presentació de $G$ (corol.lari 3.5). En conseqüència, les aplicacions $\varphi$ de l'enunciat respecten, per hipòtesi, les relacions a $G$ i aleshores $\varphi$ estén a un morfisme de $G$ a $H$, que ha de ser únic en ser $(A, B)$ base i per tant $A \sqcup B$ generadors de $G$.

[$\Leftarrow$] Sigui $K = \langle A, B \mid [A \sqcup B, B] \rangle$ amb $|A| \neq 1$ que, tal i com acabem de veure, compleix la propietat universal. Considerem ara les inclusions $\theta \colon A \sqcup B \hookrightarrow K$ i $\zeta \colon A \sqcup B \hookrightarrow G$; ambdues satisfan les condicions que es demana a les $\varphi$ de l'enunciat ($\theta$ per que així ho estableix la presentació de $K$, i $\zeta$ per hipòtesi sobre $G$). Si ara apliquem la condició categòrica prenent $\varphi$ igual a $\theta$ i $\zeta$ respectivament obtenim l'existència de morfismes $\widetilde{\theta}$ i $\widetilde{\zeta}$ únics que fan commutatius els següents diagrames (que escrivim superposats)

$$\begin{tikzcd} A \sqcup B \arrow[r, hook, "\zeta"] \arrow[d, hook, "\theta"'] & G \arrow[dl, dotted, shift left, "\exists!\,\widetilde{\theta}"] \\ K \arrow[ur, dotted, shift left, "\exists!\,\widetilde{\zeta}"] & \end{tikzcd} .$$

Només falta veure que $\widetilde{\theta}$ i $\widetilde{\zeta}$ són inversos l'un de l'altre. En efecte, considerem el diagrama

$$\begin{tikzcd} A \sqcup B \arrow[r, hook, "\zeta"] \arrow[d, hook, "\theta"'] & G \arrow[dl, dotted, "\exists!\text{ extensió}"] \\ G & \end{tikzcd} ,$$

donat que tant $\widetilde{\theta}\widetilde{\zeta}$ com $\mathrm{id}_G$ estenen, la unicitat implica que $\widetilde{\theta}\widetilde{\zeta} = \mathrm{id}_G$. De forma completament anàloga es dedueix que $\widetilde{\zeta}\widetilde{\theta} = \mathrm{id}_K$. Així doncs $\widetilde{\theta}$ i $\widetilde{\zeta}$ són inverses l'una de l'altra i per tant $G$ i $K$ són isomorfs, la qual cosa conclou la demostració. □

OBSERVACIÓ 5. En la caracterització anterior no hem donat en cap moment condicions sobre els cardinals de $A$ i $B$. Així, la proposició 3.6 es podria prendre, de fet, com a definició categòrica general dels grups lliure per lliure-abelià sobre una certa base (sense restriccions) mentre que el cas finitament generat correspondria exactament a quan $A$ i $B$ tenen cardinals finits.

Feta aquesta precisió insistim en que el present treball es centrarà en l'estudi del cas finitament generat que donarem per suposat sobre el grup de partida sempre que no s'indiqui el contrari. Cal no oblidar, no obstant, que en aquest estudi apareixen de forma natural (com a subgrups) grups lliure per lliure-abelià de la forma $F_\infty \times \mathbb{Z}^{m'}$. Així doncs, el conveni no serà aplicable quan ens referim a subgrups generals i caldrà, en aquest cas, aclarir si estem considerant els de rang infinit o no.

Només per coherència notacional i terminològica agrupem part dels resultats anteriors en un nou enunciat.

COROL.LARI 3.7. *Sigui $(A,B)$ base de $G \in \widetilde{\mathcal{G}}$, aleshores*

$$\mathrm{rang}(G) = (\,|A|\,,|B|\,)$$

*És a dir, el cardinals de les components lliure i lliure-abeliana de tota base són respectivament les components lliure i lliure-abeliana del rang de $G$. En particular, si $(A,B)$ i $(A',B')$ són bases de $G$, tindrem $|A| = |A'|$ i $|B| = |B'|$.* □

També conseqüència directa de la proposició 3.4 obtenim la següent propietat desitjable en una entitat anomenada *base* de $G$.

COROL.LARI 3.8. *Si $(A, B)$ és base de $G$ lliure per lliure-abelià, aleshores tot element de $G$ s'escriu de forma 'única' en termes dels elements de $(A, B)$ (evidentment, entenent que la 'unicitat' de la part abeliana és mòdul reordenacions dels elements de $B$).*

DEMOSTRACIÓ. Si $(A, B)$ és base de $G$ ja hem vist a 3.4 que $G = \langle A\rangle \times \langle B\rangle$. És a dir tot element de $G$ s'escriu de forma única en termes d'un de $\langle A\rangle$ i un de $\langle B\rangle$ i (de nou per 3.4) els elements d'aquests dos subgrups de forma única en termes dels elements de les bases respectives $A$ i $B$ llevat reordenació dels últims. $\square$

OBSERVACIÓ 6. Hem presentat fins ara propietats de les noves bases (són conjunts minimals de generadors amb cardinal determinat tals que tot element del grup s'escriu de forma única en termes dels seus) que es corresponen bé amb les anàlogues per les bases lliures o lliure-abelianes estàndard. Malgrat els evidents paralel.lismes cal ser curós a l'hora de traslladar a les noves bases comportaments típics d'aquelles. La polarització (intrínseca) de la nostra definició fa que certes propietats estàndard no siguin extensibles. Per exemple, en el nostre cas *no* és cert que "tota família de $n+m$ generadors de $G \cong F_n \times \mathbb{Z}^m$ (de rang $n+m$) constitueixi una base de $G$", enunciat que *sí* és vàlid tant per als grups lliures com per als lliure-abelians amb els rangs corresponents.

EXEMPLE 2. Serveixi de contraexemple considerar a $F_2 \times \mathbb{Z} = \langle\, a, b \mid\, \rangle \times \langle\, t \mid\, \rangle$ els elements $x_1 = ta^2$, $x_2 = ab$ i $x_3 = ta^3b^2$. Òbviament no és possible formar una base amb $x_1, x_2, x_3$ ja que cap d'ells pertany al centre de $F_2 \times \mathbb{Z}$, en canvi $x_2x_3^{-1}x_1x_2 = a$, $x_2^{-1}x_1^{-1}x_3 = b$ i $x_1a^{-2} = t$, i per tant generen $G$.

## 4. Bases de subgrups

Acabem la secció amb una sèrie de resultats de caire eminentment algorísmic essencials per atacar alguns dels problemes de decisió que ens plantejarem a la segona part.

Sabem que tot subgrup $H$ de $G \in \widetilde{\mathcal{G}}$ és producte directe d'un grup lliure per un grup lliure-abelià; aleshores la proposició 3.4 indica que per a aconseguir una base de $H$ serà suficient obtenir-ne una de cadascun dels factors segons una escissió del tipus (5). Vegem que, en realitat, qualsevol base de $G$ respon a aquest patró.

PROPOSICIÓ 4.1. *Sigui $H$ un subgrup de $G = \langle X \mid \rangle \times \langle T \mid [T,T] \rangle \in \widetilde{\mathcal{G}}$, aleshores un subconjunt $E \subseteq H$ és base de $G$ si i només si*

$$E = E_X \sqcup E_T$$

*amb $E_T$ base (lliure-abeliana) de $H \cap \mathbb{Z}^m$ i $E_X$ base (lliure) de $H\pi\alpha$, per a una certa escissió $\alpha$ del tipus* (5).

DEMOSTRACIÓ. [$\Rightarrow$] Sigui $E = A \sqcup B$ amb $(A,B)$ base de $H$ i considerem els següents dos subconjunts de $E$: $E_X$ format per les paraules de $E$ que en forma normal tenen lletres en $X$ i $E_T$ format per les que no (i.e. les que només tenen lletres en T). Aleshores és clar que $E = E_X \sqcup E_T$, i la projecció $\pi\colon H \to H\pi$ envia $E_X$ a una base $(E_X)\pi$ de $H\pi$ i $E_T$ a l'element trivial. Ara, com que $E$ és base per hipòtesi, $E_T$ ha de ser base del $\ker(\pi_{|H}) = H \cap \mathbb{Z}^m$ i la restricció de $\pi$ a $E_X$ és bijectiva; prenent $\alpha$ la seva inversa obtenim el resultat.

[$\Leftarrow$] La implicació cap a l'esquerra és conseqüència directa de la proposició 3.4. □

DEFINICIÓ 4.1. En la situació de l'enunciat anterior, diem que $E$ és una base de $H$ *donada per l'escissió* $\alpha$ (o que és una $\alpha$-*base* de $H$).

Òbviament, el concepte de $\alpha$-base és només una forma còmoda d'al.ludir a l'escissió subjacent i no suposa cap restricció ni caracteritza la base referida.

OBSERVACIÓ 7. Tenim, per tant dues formes naturals de pensar una base $E$ d'un grup $G \in \widetilde{\mathcal{G}}$ com a unió disjunta d'un parell de conjunts: el punt de vista (*algebraic*) de la definició 3.2, en què els constituents són bases, $B$ del centre de $G$, i $A$ d'un complementari lliure no abelià; i el punt de vista (*constructiu* o *combinatori*) de la proposició 4.1, en què els constituents són respectivament el conjunt $E_T$ format per les paraules de $E$ escrites només en $T$, i el conjunt $E_X$ format per les que contenen alguna lletra de $X$. És a dir, per a tota base $E$ de $G$, tenim

$$E = A \sqcup B = E_X \sqcup E_T \text{ , i}$$
$$G = \langle A \rangle \times \langle B \rangle = \langle E_X \rangle \times \langle E_T \rangle$$

amb la següent casuística:

- si $|E_X| \neq 1$ , aleshores $A = E_X$ i $B = E_T$, i
- si $|E_X| = 1$ , aleshores $A = \varnothing$ i $B = E_X \sqcup E_T$

Si $H$ està donat per un conjunt finit de generadors l'obtenció de bases de cadascun dels factors segons $\alpha$ (i per tant l'obtenció d'una base de $H$) és un procés algorísmic; i tal i com succeeix amb els casos degenerats, un cop es disposa d'una base finita, és pura mecànica obtenir l'expressió d'un element qualsevol (escrit en termes del conjunt inicial de generadors) en aquesta base.

PROPOSICIÓ 4.2. *Siguin $G \in \widetilde{\mathcal{G}}$ i $H \leqslant G$ un subgrup donat per una família finita de generadors, aleshores existeix un procediment algorísmic per trobar una base de $H$ i reescriure els generadors originals en aquesta base.*

DEMOSTRACIÓ. Sigui $H = \langle h_1, \ldots, h_s \rangle \leqslant G$, volem construir algorísmicament una base de $H$.

Resseguint la primera part de la demostració de 2.1 podem calcular una base (lliure) $E_X = \{\widetilde{y}_1, \ldots, \widetilde{y}_{n'}\}$ de $H\pi\alpha$ (factor lliure de $G$ segons $\alpha$). Detallem el procés:

(1) Calculem la imatge per $\pi$ dels generadors de $H$: $\{h_1\pi, \ldots, h_s\pi\}$.
(2) Donat que $\pi$ és epimorfisme, $\{h_1\pi, \ldots, h_s\pi\}$ constituirà un conjunt de generadors de $H\pi \leqslant F_n$, del que mitjançant una seqüència finita de transformacions de Nielsen (o *Stallings foldings*) podem obtenir una base $\{y_1, \ldots, y_{n'}\}$ de $H\pi$. És clar que aquest procés és algorísmic.
(3) Calculem la imatge $\{\widetilde{y}_1, \ldots, \widetilde{y}_{n'}\}$ de $\{y_1, \ldots, y_{n'}\}$ per una escissió $\alpha$ algorísmica (que tenim garantida d'acord amb l'observació 3).

Com que $\{y_1, \ldots, y_{n'}\}$ és base lliure de $H\pi$ i $\alpha$ és injectiva, acabem de calcular una base (lliure) $E_X = \{\widetilde{y}_1, \ldots, \widetilde{y}_{n'}\}$ de $H\pi\alpha$.

Pel que fa a la part abeliana, l'isomorfisme $\Theta_\alpha$ (que tenim explícitament en termes de $\alpha$) seguit de la projecció sobre la segona coordenada constitueix un morfisme (òbviament exhaustiu) de $H$ sobre $\ker(\pi_{|H})$. Aplicat a $\{h_1, \ldots, h_s\}$ proporciona un conjunt de generadors de $\ker(\pi_{|H}) \cong \mathbb{Z}^{m'}$ que podrem reduir de la forma habitual a una base lliure-abeliana $E_T$ de $\ker(\pi_{|H})$.

Hem obtingut algorísmicament bases respectives de $H\pi\alpha$ i $\ker(\pi_{|H})$; ara la proposició 4.1 conclou la primera part de l'enunciat.

Per a la segona serà suficient comprovar que podem calcular l'expressió de cada generador en base $E_X \sqcup E_T$.

Observem que resseguint en sentit contrari la seqüència de la Nielsen-reducció $(h_1\pi, \ldots, h_s\pi) \rightsquigarrow \cdots \rightsquigarrow (y_1, \ldots, y_{n'})$ i acumulant els canvis realitzats en cada pas, obtenim l'expressió $h_l\pi = w_l(y_1, \ldots, y_{n'})$ de $h_l\pi$ en termes de la base $\{y_1, \ldots, y_{n'}\}$ de $H\pi$. Ara, la descomposició $h_l = h_l\pi\alpha \cdot (h_l\pi\alpha)^{-1}h_l$ donada per l'isomorfisme $\Theta_\alpha$ fa la resta. El primer factor serà

$$(h_l\pi)\alpha = w_l(y_1\alpha, \ldots, y_{n'}\alpha) = w_l(\widetilde{y}_1, \ldots, \widetilde{y}_{n'}) \ ,$$

i l'obtenim, per tant, escrit en termes de la base lliure $E_X$, mentre que el segon, en pertànyer al $\ker(\pi_{|H})$, el podem escriure (usant àlgebra lineal elemental) en termes de $E_T$ que és base de $\ker(\pi_{|H})$. □

Observació 8. En vista del corol.lari 3.5, la proposició anterior ens diu que donada una família finita $\{ h_1, \dots, h_s \}$, sempre podrem obtenir algorísmicament una presentació de $\langle h_1, \dots, h_s \rangle$.

En vista del que hem exposat fins ara, quan vulguem representar explícitament una base $E$ d'un subgrup finitament generat $H$ de $G \in \mathcal{G}$, escriurem

$$E = \{ \mathbf{t}^{\mathbf{a_1}} u_1, \dots, \mathbf{t}^{\mathbf{a_{n'}}} u_{n'}, \mathbf{t}^{\mathbf{b_1}}, \dots, \mathbf{t}^{\mathbf{b_{m'}}} \} \tag{7}$$

amb $n', m' \in \mathbb{N}$, i

- $\mathbf{a_1}, \dots, \mathbf{a_{n'}} \in \mathbb{Z}^m$,
- $\{u_1, \dots, u_{n'}\}$ base lliure de $H\pi \leqslant F_n$, i
- $\{\mathbf{b_1}, \dots, \mathbf{b_{m'}}\}$ base lliure-abeliana de $H \cap \mathbb{Z}^m \leqslant \mathbb{Z}^m$.

Amb les notacions introduïdes serà

$$\begin{aligned} E_X &= \{ \mathbf{t}^{\mathbf{a_1}} u_1, \dots, \mathbf{t}^{\mathbf{a_{n'}}} u_{n'} \} \quad \text{i} \\ E_T &= \{ \mathbf{t}^{\mathbf{b_1}}, \dots, \mathbf{t}^{\mathbf{b_{m'}}} \}. \end{aligned}$$

Per brevetat, designarem

$$L = \langle \mathbf{b_1}, \dots, \mathbf{b_{m'}} \rangle, \text{ subgrup de rang } m' \text{ de } \mathbb{Z}^m,$$

i també

$$\mathbf{A} = \begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_{n'}} \end{pmatrix} \in \mathcal{M}_{n' \times m}(\mathbb{Z})$$

la matriu sencera $n' \times m$ que té per files els $\mathbf{a_i} \in \mathbb{Z}$, $i \in [1, n']$.

Lema 4.3. *Amb les notacions anteriors, tenim*

$$H = \{ \mathbf{t}^{\mathbf{a}} \, \omega(u_1, \dots, u_{n'}) \mid \omega \in F_{n'} \ , \ \mathbf{a} \in \boldsymbol{\omega} \mathbf{A} + L \} \ ,$$

*on $\omega$ designa un element del grup lliure abstracte en $n'$ símbols $\{s_1, \dots, s_{n'}\}$ i $\omega(u_1, \dots, u_{n'})$ l'element de $G$ obtingut substituint cada símbol $s_i$ a $\omega$ per la respectiva paraula $u_i \in H\pi$. Com sempre, representem en negreta, $\boldsymbol{\omega}$, l'abelianitzat de la paraula $\omega$.*

*Dit d'una altra forma, si $\mu$ és el morfisme de $F_{n'} = \langle s_1, \dots, s_{n'} \mid \rangle$ en $F_n = \langle x_1, \dots, x_n \mid \rangle$ donat per $s_i \mapsto u_i(x_1, \dots, x_n)$, $i \in [1, n']$, aleshores*

$$H = \{ \mathbf{t}^{\mathbf{a}} \, \omega\mu \mid \omega \in F_{n'} \ , \ \mathbf{a} \in \boldsymbol{\omega} \mathbf{A} + L \} \ .$$

Demostració. Donat que $H = \langle E_X \rangle \times \langle E_T \rangle$, el subgrup està descrit pels parells $(w, \mathbf{t}^{\mathbf{b}})$ al producte directe anterior; on $\mathbf{b} \in L$ i $w$ un element de $\langle E_X \rangle \leqslant G$. Més formalment, $w = \omega(\mathbf{t}^{\mathbf{a_1}} u_1, \dots, \mathbf{t}^{\mathbf{a_{n'}}} u_{n'})$ amb $\omega$ una paraula lliure arbitrària en $n'$ símbols[1]. Ara, de la commutativitat de les $t$'s, podem

[1]Remarquem que, tot i que $w \neq \omega$ (de fet, són paraules en grups aliens) s'utilitza grafies similars per subratllar que descriuen el mateix element en bases diferents.

reordenar i reescriure $w$ en forma normal

$$\begin{aligned} w &= \omega(\mathbf{t}^{\mathbf{a_1}} u_1, \ldots, \mathbf{t}^{\mathbf{a_{n'}}} u_{n'}) \\ &= \mathbf{t}^{|\omega|_1 \mathbf{a_1} + \cdots + |\omega|_{n'} \mathbf{a_{n'}}}\, \omega(u_1, \ldots, u_{n'}) \\ &= \mathbf{t}^{\boldsymbol{\omega}\mathbf{A}}\, \omega(u_1, \ldots, u_{n'})\ . \end{aligned}$$

Finalment, agrupant les $t$'s de $w$ i $\mathbf{t}^{\mathbf{b}}$ obtenim la descripció proposada per als elements de $H$. □

És a dir, per construir el subgrup $H$ a partir de la base $E$ és suficient considerar totes les paraules lliures en $u_i$, $i = 1, \ldots, n'$ i completar-les amb totes les parts abelianes que satisfacin la relació lineal esmentada.

Definició 4.2. Donats un subgrup $H$ de $G = \langle\, X, T \mid [X \sqcup T, T]\,\rangle$ i una paraula lliure $w \in G\pi = \langle X \rangle_G$, direm que el conjunt

$$\mathfrak{c}_{w,H} = \{\, \mathbf{a} \in \mathbb{Z}^m \mid t^{\mathbf{a}} w \in H \,\} \subseteq \mathbb{Z}^m$$

és la *compleció abeliana* de $w$ a $H$; i de qualsevol element $\mathbf{a} \in \mathfrak{c}_{w,H}$, que *completa (abelianament)* $w$ a $H$.

Corol.lari 4.4. *De la definició anterior i el lema 4.3 es dedueix immediatament que*

(i) *si* $w \notin H\pi$, *aleshores* $\mathfrak{c}_{w,H} = \varnothing$, *i*
(ii) *si* $w \in H\pi$, *aleshores* $\mathfrak{c}_{w,H} = \boldsymbol{\omega}\mathbf{A} + L$

*on* $\boldsymbol{\omega}$ *és l'abelianització de la paraula* $\omega$ *que expressa* $w$ *en termes de la base* $\{u_1, \ldots, u_{n_1}\}$, *és a dir*[1] $w = \omega(u_1, \ldots, u_{n_1})$. □

# Capítol 2
# Morfismes

En aquest capítol pretenem estudiar els endomorfismes dels grups lliure per lliure-abelià. Donat que, com veurem aviat, els casos amb $n = \infty$ desembocarien en l'aparició de matrius de dimensió infinita, i el cas lliure-abelià de rang infinit l'hem exclòs de partida, ens restringirem al cas finitament generat. És a dir, en tot el capítol considerarem *només* els endomorfismes de grups $F_n \times \mathbb{Z}^m \in \mathcal{G}$. Concretament volem caracteritzar l'expressió dels endo, mono, epi i isomorfismes de

$$G = F_n \times \mathbb{Z}^m = \langle\, X \mid \,\rangle \times \langle\, T \mid [T,T]\,\rangle = \langle X, T \mid [X \sqcup T, T]\,\rangle$$

en termes de les imatges dels generadors $X = \{\, x_1, \dots, x_n \,\}$ i $T = \{\, t_1, \dots, t_m \,\}$ amb $n, m \in \mathbb{N}$ (com ja hem vist, sense pèrdua de generalitat podem prendre $n \neq 1$).

És clar que associats a les parts lliure i lliure-abeliana, emergiran com a constituents de cada $\Psi \in \operatorname{End}(F_n \times \mathbb{Z}^m)$, endomorfismes respectius, $\phi$ de $F_n$ i $\mathbf{Q}$ de $\mathbb{Z}^m$. Veurem que excepte en un cas degenerat (que no inclou ni epis ni monos), els endomorfismes de $F_n \times \mathbb{Z}^m$ es poden descriure en termes de $\phi$, $\mathbf{Q}$ i una matriu $\mathbf{P}$ que controla l'aparició de lletres $t_j^{\text{'s}}$ a partir de lletres $x_i$ sota $\Psi$. A més, les caracteritzacions d'injectivitat i exhaustivitat només involucren $\phi$ i $\mathbf{Q}$, i tenen expressions senzilles i molt naturals en termes d'aquests.

Comencem considerant una assignació genèrica dels generadors $X \sqcup T$ en $F_n \times \mathbb{Z}^m$,

$$\Psi : \begin{cases} x_i & \mapsto & t_1^{p_{i1}} \cdots t_m^{p_{im}}\, w_i \\ t_j & \mapsto & t_1^{q_{j1}} \cdots t_m^{q_{jm}}\, z_j \end{cases},$$

amb $p_{ik}, q_{jk} \in \mathbb{Z}$ i $w_i, z_j \in F_n$ $(i \in [1,n],\ j,k \in [1,m])$. Anomenant $\phi$ a l'endomorfisme $x_i \mapsto w_i$ de $F_n$, i, $\mathbf{P}$ i $\mathbf{Q}$ a les matrius

$$\mathbf{P} = \begin{pmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nm} \end{pmatrix} = \begin{pmatrix} \mathbf{p_1} \\ \vdots \\ \mathbf{p_n} \end{pmatrix} = \begin{pmatrix} \mathbf{p_{\bullet 1}} \cdots \mathbf{p_{\bullet m}} \end{pmatrix} \in \mathcal{M}_{n\times m}(\mathbb{Z}), \text{ i}$$

$$\mathbf{Q} = \begin{pmatrix} q_{11} & \cdots & q_{1m} \\ \vdots & \ddots & \vdots \\ q_{m1} & \cdots & q_{mm} \end{pmatrix} = \begin{pmatrix} \mathbf{q_1} \\ \vdots \\ \mathbf{q_m} \end{pmatrix} = \begin{pmatrix} \mathbf{q_{\bullet 1}} \cdots \mathbf{q_{\bullet m}} \end{pmatrix} \in \mathcal{M}_m(\mathbb{Z}) \ ,$$

podem, usant la notació abreujada, escriure $\Psi$ de la forma més compacta

$$\Psi : \left\{ \begin{array}{lcl} x_i & \mapsto & \mathbf{t}^{\mathbf{p_i}} \ x_i\phi \\ t_j & \mapsto & \mathbf{t}^{\mathbf{q_j}} \ z_j \ , \end{array} \right. \tag{8}$$

amb $\phi$ endomorfisme de $F_n$, $\mathbf{p_i}, \mathbf{q_j} \in \mathbb{Z}^m$ i $z_j \in F_n$ $(i \in [1,n],\ j \in [1,m])$.

Evidentment no totes les assignacions anteriors estendran a morfisme de $F_n \times \mathbb{Z}^m$ però per a les que ho facin és un càlcul rutinari obtenir la imatge d'un element genèric $\mathbf{t^a}u$ en forma normal.

Proposició 0.5. *Si una assignació $\Psi$ de la forma anterior estén a endomorfisme de $F_n \times \mathbb{Z}^m$, aleshores $\forall \mathbf{a} \in \mathbb{Z}^m$, $\forall u \in F_n$*

$$\begin{array}{lcl} u & \overset{\Psi}{\longmapsto} & \mathbf{t}^{\mathbf{uP}} \ u\phi \\ \mathbf{t^a} & \overset{\Psi}{\longmapsto} & \mathbf{t}^{\mathbf{aQ}} \ z_1^{a_1} \cdots z_m^{a_m} \ , \end{array}$$

*on hem designat $\mathbf{u}$ – en negreta – el vector de $\mathbb{Z}^n$ abelianitzat de $u \in F_n$. Per suposat, tindrem*

$$\mathbf{t^a}u \overset{\Psi}{\longmapsto} \mathbf{t}^{\mathbf{aQ+uP}} \ z_1^{a_1} \cdots z_m^{a_m} \ u\phi \ .$$

Demostració. Es tracta només d'usar la condició de morfisme juntament amb les relacions de $F_n \times \mathbb{Z}^m$, en efecte

$$\begin{array}{rcl} \mathbf{t^a}\Psi & = & (t_1^{a_1} \cdots t_m^{a_m})\Psi = (t_1\Psi)^{a_1} \cdots (t_m\Psi)^{a_m} \\ & = & (\mathbf{t}^{\mathbf{q_1}} \ z_1)^{a_1} \cdots (\mathbf{t}^{\mathbf{q_m}} \ z_m)^{a_m} \\ & = & \mathbf{t}^{a_1\mathbf{q_1} + \cdots + a_m\mathbf{q_m}} \ z_1^{a_1} \cdots z_m^{a_m}, \\ & = & \mathbf{t}^{\mathbf{aQ}} \ z_1^{a_1} \cdots z_m^{a_m}, \end{array}$$

i també

$$\begin{array}{rcl} u\Psi & = & u(x_i)\Psi = u(x_i\Psi) = u(t_1^{p_{i1}} \cdots t_m^{p_{im}} \ x_i\phi) \\ & = & t_1^{|u|_1 p_{11} + \cdots + |u|_n p_{n1}} \cdots t_m^{|u|_1 p_{1m} + \cdots + |u|_n p_{nm}} \ u(x_i\phi) \\ & = & t_1^{\mathbf{up_{\bullet 1}}} \cdots t_m^{\mathbf{up_{\bullet m}}} \ u\phi \\ & = & \mathbf{t}^{\mathbf{uP}} \ u\phi \ . \end{array}$$

Per tant,

$$(\mathbf{t^a}u)\Psi = \mathbf{t^a}\Psi \ u\Psi = \mathbf{t}^{\mathbf{aQ}} \ z_1^{a_1} \cdots z_m^{a_m} \ \mathbf{t}^{\mathbf{uP}} \ u\phi = \mathbf{t}^{\mathbf{aQ+uP}} \ z_1^{a_1} \cdots z_m^{a_m} \ u\phi \ . \qquad \square$$

# 1. Endomorfismes

Caracteritzem a continuació quan una de les assignacions anteriors estén a endomorfisme de $F_n \times \mathbb{Z}^m$ i en donem una classificació en termes dels paràmetres que la defineixen.

PROPOSICIÓ 1.1. *Una assignació $\Psi$ de la forma (8) estén a endomorfisme si i només si és d'un dels següents dos tipus (disjunts):*

$$\mathbf{I)} \quad \left\{ \begin{array}{lll} x_i & \mapsto & \mathbf{t}^{\mathbf{p_i}}\ x_i\phi \\ t_j & \mapsto & \mathbf{t}^{\mathbf{q_j}} \end{array} \right. \quad \textit{amb } \phi \in \mathrm{End}(F_n) \ \textit{ i } \mathbf{p_i}, \mathbf{q_j} \in \mathbb{Z}^m,$$

$$\mathbf{II)} \quad \left\{ \begin{array}{lll} x_i & \mapsto & \mathbf{t}^{\mathbf{p_i}}\ w^{h_i} \\ t_j & \mapsto & \mathbf{t}^{\mathbf{q_j}}\ w^{l_j} \end{array} \right. \quad \textit{amb} \quad \begin{array}{l} 1 \neq w \in F_n \ \textit{no potència pròpia}, \\ \mathbf{h} \in \mathbb{Z}^n \ \textit{ i } \mathbf{p_i}, \mathbf{q_j}, \mathbf{l} \in \mathbb{Z}^m, \mathbf{l} \neq \mathbf{0} \end{array} \quad ,$$

*(en els dos casos amb $i \in [1,n]$ i $j \in [1,m]$).*

DEMOSTRACIÓ. Una assignació $\Psi$ estén a morfisme si i només si respecta les relacions de $F_n \times \mathbb{Z}^m$. En el nostre cas, les commutativitats donades per les relacions es traduiran en commutativitats entre les respectives parts lliures de les imatges. Concretament haurà de ser, per a tot $i \in [1,n]$ i tot $k \in [1,m]$

$$\begin{aligned} 1 = (x_i^{-1} t_k^{-1} x_i t_k)\Psi &= (x_i\Psi)^{-1}\ (t_k\Psi)^{-1}\ x_i\Psi\ t_k\Psi \\ &= (\mathbf{t}^{\mathbf{p_i}} w_i)^{-1}\ (\mathbf{t}^{\mathbf{q_k}} z_k)^{-1}\ \mathbf{t}^{\mathbf{p_i}} w_i\ \mathbf{t}^{\mathbf{q_k}} z_k \\ &= \mathbf{t}^{-\mathbf{p_i} - \mathbf{q_k} + \mathbf{p_i} + \mathbf{q_k}}\ w_i^{-1} z_k^{-1} w_i z_k \\ &= w_i^{-1} z_k^{-1} w_i z_k \ , \end{aligned}$$

és a dir, $w_i$ commuta amb $z_k$. Anàlogament, per a tot $j, k \in [1,m]$, obtenim que $z_j$ commuta amb $z_k$. En resum

(9) $$\Psi \text{ estén a endomorfisme} \quad \Leftrightarrow \quad \forall i,j,k \quad w_i, z_j \in C(z_k)$$

on $C(z_k)$ és el centralitzador de $z_k$ a $F_n$. Observem que l'extensibilitat de $\Psi$ no depèn dels valors dels $p_{ij}$ i $q_{jk}$. Distingim ara dos casos:

*I*) ($z_k = 1 \quad \forall k \in [1,m]$) Aleshores la condició de commutativitat (9) es compleix trivialment $\forall w_1, \ldots, w_n \in F_n$ (i.e $\forall \phi$ endomorfisme de $F_n$) i l'extensió pren automàticament la forma del tipus I.

*II*) ($\exists k \in [1,m]$ tal que $z_k \neq 1$) Donat que el centralitzador de $z_k \neq 1$ és cíclic infinit, tenim que $C(z_k) = \langle w \rangle$ amb $w$ no potència pròpia. En efecte, les possibles arrels de $w$ commutarien amb $w$ i per tant també amb $z_k$, és a dir serien, en definitiva, potències de $w$. D'altra banda, és evident que els elements de $\langle w \rangle$ commuten entre si. Així, en aquest segon cas $\Psi$ estén a endomorfisme si i només si existeix un $w \in F_n \setminus \{1\}$ no potència pròpia tal que per a tot $i$ i tot $j$, $w_i, z_j \in \langle w \rangle$. Aleshores és clar que

$$\begin{array}{lr} w_i = w^{h_i} \text{ amb } h_i \in \mathbb{Z} & \forall i \ , \\ z_j = w^{l_j} \text{ amb } l_j \in \mathbb{Z} & \forall j \ , \text{ i} \\ z_k = w^{l_k} \text{ amb } l_k \in \mathbb{Z} \setminus \{0\}, & \end{array}$$

obtenint l'expressió donada per als morfismes de tipus II. □

Evidentment, donat que tot endomorfisme és extensió única de la seva restricció a un conjunt de generadors, l'anterior és en realitat una classificació dels endomorfismes de $F_n \times \mathbb{Z}^m$. Podem ara particularitzar la proposició 0.5 a cadascun dels casos, obtenint les respectives expressions generals dels endomorfismes de tipus I i II en forma normal.

Corol.lari 1.2. *$\Psi$ és endomorfisme de $F_n \times \mathbb{Z}^m$ si i només si és d'un dels següents dos tipus mútuament excloents*

**(I)** $\Psi_{\phi,\mathbf{Q},\mathbf{P}} := \mathbf{t^a} u \mapsto \mathbf{t^{aQ+uP}} \ u\phi$,
*amb* $\phi \in \mathrm{End}(F_n)$, $\mathbf{Q} \in \mathcal{M}_m(\mathbb{Z})$ *i* $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$.

**(II)** $\Psi_{w,\mathbf{l},\mathbf{h},\mathbf{Q},\mathbf{P}} := \mathbf{t^a} u \mapsto \mathbf{t^{aQ+uP}} \ w^{\mathbf{a}\,\mathbf{l}^T + \mathbf{u}\,\mathbf{h}^T}$,
*amb* $1 \neq w \in F_n$ *no potència pròpia,* $\mathbf{Q} \in \mathcal{M}_m(\mathbb{Z})$, $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$, $\mathbf{0} \neq \mathbf{l} \in \mathbb{Z}^m$ *i* $\mathbf{h} \in \mathbb{Z}^n$.

Ens referirem a ells com endomorfismes de tipus I i II i els designarem $\mathrm{End_I}(F_n \times \mathbb{Z}^m)$ i $\mathrm{End_{II}}(F_n \times \mathbb{Z}^m)$ respectivament. Tenim, per tant, una partició

$$\mathrm{End}(F_n \times \mathbb{Z}^m) = \mathrm{End_I}(F_n \times \mathbb{Z}^m) \sqcup \mathrm{End_{II}}(F_n \times \mathbb{Z}^m).$$

Calculem a continuació com es composen els endomorfismes de $F_n \times \mathbb{Z}^m$ en termes d'aquesta classificació.

Proposició 1.3. *El comportament algebraic dels tipus anteriors ve donat pels següents quatre casos:*

(a) (tipus I) *seguit de* (tipus I)*:* $\Psi_{\phi_1,\mathbf{Q_1},\mathbf{P_1}} \Psi_{\phi_2,\mathbf{Q_2},\mathbf{P_2}} =$

$$\Psi_{\phi_1\phi_2\,,\,\mathbf{Q_1Q_2}\,,\,\mathbf{P_1Q_2+A_1P_2}}, \tag{10}$$

(b) (tipus I) *seguit de* (tipus II)*:* $\Psi_{\phi_1,\mathbf{Q_1},\mathbf{P_1}} \Psi_{w_2,\mathbf{l_2},\mathbf{h_2},\mathbf{Q_2},\mathbf{P_2}} =$

$$\Psi_{w_2\,,\,\mathbf{l_2Q_1^T}\,,\,\mathbf{l_2P_1^T+h_2A_1^T}\,,\,\mathbf{Q_1Q_2}\,,\,\mathbf{P_1Q_2+A_1P_2}}, \tag{11}$$

(c) (tipus II) *seguit de* (tipus I)*:* $\Psi_{w_1,\mathbf{l_1},\mathbf{h_1},\mathbf{Q_1},\mathbf{P_1}} \Psi_{\phi_2,\mathbf{Q_2},\mathbf{P_2}} =$

$$\Psi_{w_1\phi_2\,,\,\mathbf{l_1}\,,\,\mathbf{h_1}\,,\,\mathbf{Q_1Q_2+l_1^T w_1P_2}\,,\,\mathbf{P_1Q_2+h_1^T w_1P_2}}, \tag{12}$$

(d) (tipus II) *seguit de* (tipus II)*:* $\Psi_{w_1,\mathbf{l_1},\mathbf{h_1},\mathbf{Q_1},\mathbf{P_1}} \Psi_{w_2,\mathbf{l_2},\mathbf{h_2},\mathbf{Q_2},\mathbf{P_2}} =$

$$\Psi_{w_2\,,\,\mathbf{l_2Q_1^T+h_2w_1^T l_1}\,,\,\mathbf{l_2P_1^T+h_2w_1^T h_1}\,,\,\mathbf{Q_1Q_2+l_1^T w_1P_2}\,,\,\mathbf{P_1Q_2+h_1^T w_1P_2}}, \tag{13}$$

*on hem usat el conveni (que mantindrem d'ara endavant) de designar* $\mathbf{A_1}$ *– en negreta – la matriu* $n \times n$ *abelianització de* $\phi_1 \in \mathrm{End}(F_n)$.

Demostració. N'hi ha prou amb aplicar successivament les expressions per als endomorfismes de cada tipus donades al corol.lari 1.2. Així, anomenant $\Psi_1$ i $\Psi_2$ als endomorfismes que actuen en primer i segon lloc, tenim:

(a) Si ambdós són de tipus I,

$$\begin{aligned} (\mathbf{t}^{\mathbf{a}}\,u)\Psi_1\Psi_2 &= (\mathbf{t}^{\mathbf{aQ_1+uP_1}}\;u\phi_1)\Psi_2 \\ &= \mathbf{t}^{\mathbf{(aQ_1+uP_1)Q_2+uA_1P_2}}\;u\phi_1\phi_2 \\ &= \mathbf{t}^{\mathbf{aQ_1Q_2+u(P_1Q_2+A_1P_2)}}\;u\phi_1\phi_2 \\ &= (\mathbf{t}^{\mathbf{a}}\,u)\Psi_{\phi_1\phi_2\,,\,\mathbf{Q_1Q_2}\,,\,\mathbf{P_1Q_2+A_1P_2}}. \end{aligned}$$

(b) Quan composem un endomorfisme de tipus I seguit d'un de tipus II,

$$\begin{aligned} (\mathbf{t}^{\mathbf{a}}\,u)\Psi_1\Psi_2 &= (\mathbf{t}^{\mathbf{aQ_1+uP_1}}\;u\phi_1)\Psi_2 \\ &= \mathbf{t}^{\mathbf{(aQ_1+uP_1)Q_2+uA_1P_2}}\;w_2^{\mathbf{(aQ_1+uP_1)l_2^{\mathit{T}}+uA_1h_2^{\mathit{T}}}} \\ &= \mathbf{t}^{\mathbf{aQ_1Q_2+u(P_1Q_2+A_1P_2)}}\;w_2^{\mathbf{aQ_1l_2^{\mathit{T}}+u(P_1l_2^{\mathit{T}}+A_1h_2^{\mathit{T}})}} \\ &= (\mathbf{t}^{\mathbf{a}}\,u)\Psi_{w_2\,,\,\mathbf{l_2Q_1^{\mathit{T}}}\,,\,\mathbf{l_2P_1^{\mathit{T}}+h_2A_1^{\mathit{T}}}\,,\,\mathbf{Q_1Q_2}\,,\,\mathbf{P_1Q_2+A_1P_2}}. \end{aligned}$$

(c) Si es tracta d'un endomorfisme de tipus II seguit d'un de tipus I,

$$\begin{aligned} (\mathbf{t}^{\mathbf{a}}\,u)\Psi_1\Psi_2 &= (\mathbf{t}^{\mathbf{aQ_1+uP_1}}\;w_1^{\mathbf{al_1^{\mathit{T}}+uh_1^{\mathit{T}}}})\Psi_2 \\ &= \mathbf{t}^{\mathbf{(aQ_1+uP_1)Q_2+(al_1^{\mathit{T}}+uh_1^{\mathit{T}})w_1P_2}}\;(w_1^{\mathbf{al_1^{\mathit{T}}+uh_1^{\mathit{T}}}})\phi_2 \\ &= \mathbf{t}^{\mathbf{a(Q_1Q_2+l_1^{\mathit{T}}w_1P_2)+u(P_1Q_2+h_1^{\mathit{T}}w_1P_2)}}\;(w_1\phi_2)^{\mathbf{al_1^{\mathit{T}}+uh_1^{\mathit{T}}}} \\ &= (\mathbf{t}^{\mathbf{a}}\,u)\Psi_{w_1\phi_2\,,\,\mathbf{l_1}\,,\,\mathbf{h_1}\,,\,\mathbf{Q_1Q_2+l_1^{\mathit{T}}w_1P_2}\,,\,\mathbf{P_1Q_2+h_1^{\mathit{T}}w_1P_2}}. \end{aligned}$$

(d) I, per últim, si ambdós són de tipus II, $(\mathbf{t}^{\mathbf{a}}\,u)\Psi_1\Psi_2 =$

$$\begin{aligned} &= (\mathbf{t}^{\mathbf{aQ_1+uP_1}}\;w_1^{\mathbf{al_1^{\mathit{T}}+uh_1^{\mathit{T}}}})\Psi_2 \\ &= \mathbf{t}^{\mathbf{(aQ_1+uP_1)Q_2+(al_1^{\mathit{T}}+uh_1^{\mathit{T}})w_1P_2}}\;w_2^{\mathbf{(aQ_1+uP_1)l_2^{\mathit{T}}+(al_1^{\mathit{T}}+uh_1^{\mathit{T}})w_1h_2^{\mathit{T}}}} \\ &= \mathbf{t}^{\mathbf{a(Q_1Q_2+l_1^{\mathit{T}}w_1P_2)+u(P_1Q_2+h_1^{\mathit{T}}w_1P_2)}}\;w_2^{\mathbf{a(Q_1l_2^{\mathit{T}}+l_1^{\mathit{T}}w_1h_2^{\mathit{T}})+u(P_1l_2^{\mathit{T}}+h_1^{\mathit{T}}w_1h_2^{\mathit{T}})}} \\ &= (\mathbf{t}^{\mathbf{a}}\,u)\Psi_{w_2\,,\,\mathbf{l_2Q_1^{\mathit{T}}+h_2w_1^{\mathit{T}}l_1}\,,\,\mathbf{l_2P_1^{\mathit{T}}+h_2w_1^{\mathit{T}}h_1}\,,\,\mathbf{Q_1Q_2+l_1^{\mathit{T}}w_1P_2}\,,\,\mathbf{P_1Q_2+h_1^{\mathit{T}}w_1P_2}} \end{aligned}$$

obtenint les quatre expressions de l'enunciat. □

Veiem que la composició és tancada per als endomorfismes d'ambdós tipus mentre que el tipus II absorbeix els productes creuats. En particular, donat que la identitat pertany trivialment als endomorfismes de tipus I, tenim que aquests constitueixen un submonoide de $\mathrm{End}(F_n)$. És més, obtenim una identificació natural entre endomorfismes de tipus I i ternes $(\phi, \mathbf{Q}, \mathbf{P})$. Concretament

Corol.lari 1.4. *L'aplicació* $\Psi_{\phi,\mathbf{Q},\mathbf{P}} \mapsto (\phi, \mathbf{Q}, \mathbf{P})$ *estableix un isomorfisme (de monoides) entre* $\mathrm{End}_{\mathrm{I}}(F_n \times \mathbb{Z}^m)$ *i el conjunt* $\mathrm{End}(F_n) \times \mathcal{M}_m(\mathbb{Z}) \times \mathcal{M}_{n\times m}(\mathbb{Z})$ *amb l'operació induïda*

$$(\phi, \mathbf{Q}, \mathbf{P})\,(\phi', \mathbf{Q}', \mathbf{P}') = (\phi\phi', \mathbf{Q}\mathbf{Q}', \mathbf{P}\mathbf{Q}' + \mathbf{A}\mathbf{P}') \tag{14}$$

*(on* $\mathbf{A}$ *designa l'abelianització de* $\phi \in \mathrm{End}(F_n)$*) i neutre* $(\mathrm{id}_{F_n}, \mathbf{I}_m, \mathbf{0})$.

DEMOSTRACIÓ. És clar a partir del corol.lari 1.2.I que tot endomorfisme de tipus I té imatge a $\mathrm{End}(F_n) \times \mathcal{M}_m(\mathbb{Z}) \times \mathcal{M}_{n\times m}(\mathbb{Z})$, per concloure que l'aplicació és ben definida només cal, per tant, veure que l'imatge és única, en efecte si $\Psi := \Psi_{\phi,\mathbf{Q},\mathbf{P}} = \Psi_{\phi',\mathbf{Q}',\mathbf{P}'} =: \Psi'$, tenim per a tot $\mathbf{a} \in \mathbb{Z}^m$ que $(\mathbf{t}^{\mathbf{a}})\Psi = (\mathbf{t}^{\mathbf{a}})\Psi'$ i en conseqüència que $\mathbf{aQ} = \mathbf{aQ}'$; i per a tot $u \in F_n$ que $(u)\Psi = (u)\Psi'$ i per tant $\mathbf{uP} = \mathbf{uP}'$ i $u\phi = u\phi'$. És clar, doncs, que ha de ser $\phi = \phi'$, $\mathbf{Q} = \mathbf{Q}'$ i $\mathbf{P} = \mathbf{P}'$ i l'aplicació està ben definida.

L'exhaustivitat és, de nou, conseqüència directa del corol.lari 1.2.I, la injectivitat és immediata ja que els paràmetres $\phi, \mathbf{Q}, \mathbf{P}$ caracteritzen $\Psi_{\phi,\mathbf{Q},\mathbf{P}}$ i la condició de morfisme amb l'operació donada no és més que el resultat establert a (10). Per últim, l'afirmació sobre el neutre és de comprovació directa a partir de (14). □

Els endomorfismes de tipus I representen un paper especialment important en el que segueix ja que, com veurem en breu, inclouen tots els automorfismes de $F_n \times \mathbb{Z}^m$ que centraran part de l'estudi posterior. De manera que sovint serà còmode pensar-los com a ternes

$$(\phi, \mathbf{Q}, \mathbf{P}) \in \mathrm{End}(F_n) \times \mathcal{M}_m(\mathbb{Z}) \times \mathcal{M}_{n\times m}(\mathbb{Z})$$

amb l'operació (14), per exemple podem calcular fàcilment les potències d'un endomorfisme de tipus I qualsevol.

LEMA 1.5. *Sigui* $(\phi, \mathbf{Q}, \mathbf{P})$ *un endomorfisme de tipus I, aleshores per a tot* $k \geq 1$,

$$(\phi, \mathbf{Q}, \mathbf{P})^k = (\phi^k, \mathbf{Q}^k, \sum_{i=1}^{k} \mathbf{A}^{i-1}\,\mathbf{P}\,\mathbf{Q}^{k-i}) \tag{15}$$

*on* $\mathbf{A}$ *és l'abelianització de* $\phi$.

DEMOSTRACIÓ. Per inducció sobre $k$. El resultat és trivial per a $k = 1$ i suposat cert per a $k$, tenim que per a $(k+1)$ és

$$\begin{array}{rcl} (\phi, \mathbf{Q}, \mathbf{P})^{k+1} & = & (\phi, \mathbf{Q}, \mathbf{P})(\phi, \mathbf{Q}, \mathbf{P})^k \\ & = & (\phi, \mathbf{Q}, \mathbf{P})(\phi^k, \mathbf{Q}^k, \sum_{i=1}^{k} \mathbf{A}^{i-1}\,\mathbf{P}\,\mathbf{Q}^{k-i}) \\ & = & (\phi^{k+1}, \mathbf{Q}^{k+1}, \mathbf{P}\mathbf{Q}^k + \mathbf{A}(\sum_{i=1}^{k} \mathbf{A}^{i-1}\,\mathbf{P}\,\mathbf{Q}^{k-i}) \\ & = & (\phi^{k+1}, \mathbf{Q}^{k+1}, \mathbf{P}\mathbf{Q}^k + \sum_{i=1}^{k} \mathbf{A}^{i}\,\mathbf{P}\,\mathbf{Q}^{k-i}) \\ & = & (\phi^{k+1}, \mathbf{Q}^{k+1}, \sum_{i=1}^{k+1} \mathbf{A}^{i-1}\,\mathbf{P}\,\mathbf{Q}^{k+1-i})\ , \end{array}$$

la qual cosa completa la demostració. □

Seguidament, refinem les condicions d'endomorfisme per tal de caracteritzar quins d'ells són injectius o exhaustius. Comencem observant una conseqüència immediata del corol.lari 1.2.

LEMA 1.6. *Si* $\Psi$ *és un endomorfisme de tipus II,* $\mathrm{im}(\Psi)$ *és abelià.*

DEMOSTRACIÓ. És directa de 1.2.II. $\square$

## 2. Monomorfismes

Veurem a continuació que els endomorfismes injectius de $F_n \times \mathbb{Z}^m$ són precisament els endomorfismes de tipus I tals que tant la seva 'part lliure' com la seva 'part lineal' són injectives.

PROPOSICIÓ 2.1. *$\Psi$ és monomorfisme de $F_n \times \mathbb{Z}^m$ $(n \neq 1)$ si i només si és de tipus I amb $\phi$ monomorfisme de $F_n$ i $\det(\mathbf{Q}) \neq 0$.*

DEMOSTRACIÓ. [$\Rightarrow$] Evidentment $\Psi$ no pot ser de tipus II, ja que si ho fos tindríem que necessariament $n \neq 0$ (no hi ha cap $w$ no trivial a $F_0$) i com que $\mathrm{im}(\Psi)$ seria abelià, els commutadors (no trivials a $F_n$ ja que $n \neq 0$ com acabem de veure i $n \neq 1$ per conveni) estarien al nucli. Tampoc pot ser $\det(\mathbf{Q}) = 0$, ja que existiria un $\mathbf{a} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ tal que $\mathbf{aQ} = \mathbf{0}$ i aleshores $1 \neq \mathbf{t}^{\mathbf{a}} \mapsto \mathbf{t}^{\mathbf{aQ}} = \mathbf{t}^{\mathbf{0}} = 1$.

Veiem finalment que $\phi$ és injectiu. En cas contrari existirà un $u \in F_n \setminus \{1\}$ tal que $u\phi = 1$. Ara, com $\Psi$ ha de ser de tipus I, tenim

$$\begin{array}{rcll} 1 \neq u^b & \mapsto & (\mathbf{t}^{\mathbf{uP}})^b = \mathbf{t}^{b\mathbf{uP}} & \forall b \in \mathbb{Z} \\ \mathbf{t}^{\mathbf{a}} & \mapsto & \mathbf{t}^{\mathbf{aQ}} & \forall \mathbf{a} \in \mathbb{Z}^m \end{array}$$

i serà suficient veure que podem trobar un $\mathbf{a} \in \mathbb{Z}^m$ i un $b \in \mathbb{Z}$ tals que $\mathbf{aQ} = b\mathbf{uP}$ (en tal cas $\Psi$ no seria injectiu contradient la hipòtesi). Ara bé, com $\det(\mathbf{Q}) \neq 0$ l'endomorfisme de $\mathbb{Q}^m$ donat per $\mathbf{Q}$ és invertible i, en particular $\exists \boldsymbol{\alpha} \in \mathbb{Q}^m$ tal que $\boldsymbol{\alpha}\mathbf{Q} = \mathbf{uP}$, aleshores escribint $\boldsymbol{\alpha} = \frac{1}{b}\mathbf{a}$ amb $\mathbf{a} \in \mathbb{Z}^m$ i $b \in \mathbb{Z}$, obtenim els $\mathbf{a}$ i $b$ desitjats.

[$\Leftarrow$] Sigui $\Psi$ de tipus $I$, amb $\phi$ monomorfisme de $F_n$ i $\det(\mathbf{Q}) \neq \mathbf{0}$, aleshores

$$(\mathbf{t}^{\mathbf{a}}u)\Psi = 1 \;\Leftrightarrow\; \left\{ \begin{array}{l} u\phi = 1 \\ \mathbf{aQ} + \mathbf{uP} = \mathbf{0} \end{array} \right. \;\Rightarrow\; \left\{ \begin{array}{l} u = 1 \\ \mathbf{a} = \mathbf{0} \end{array} \right. .$$

En efecte, per ser $\phi$ monomorfisme, $u\phi = 1$ implica $u = 1$, per tant $\mathbf{u} = \mathbf{0}$ i la segona equació queda $\mathbf{aQ} = \mathbf{0}$. Ara, la hipòtesi $\det(\mathbf{Q}) \neq \mathbf{0}$ permet concloure que també $\mathbf{a} = \mathbf{0}$ i per tant $\Psi$ és injectiu. $\square$

## 3. Epimorfismes

Per als epimorfismes obtenim una caracterització paral.lela a la que acabem de donar per als monos.

PROPOSICIÓ 3.1. *$\Psi$ és epimorfisme de $F_n \times \mathbb{Z}^m$ $(n \neq 1)$ si i només si és de tipus I amb $\phi$ automorfisme de $F_n$ i $\det(\mathbf{Q}) = \pm 1$.*

DEMOSTRACIÓ. [$\Rightarrow$] Si anomenem $\pi$ a la projecció $F_n \times \mathbb{Z}^m \to F_n$ donada per $\mathbf{t^a}u \mapsto u$ i $\Psi$ és un endomorfisme de tipus II, tenim que $\mathrm{im}(\Psi\pi) \subseteq \langle w \rangle \neq F_n$, ja que $n \neq 1$. Per tant $\Psi$ no és exhaustiva (si ho fos també ho seria $\Psi\pi$). Així doncs, els epimorfismes han de ser de tipus I. Ara, de l'exhaustivitat $\Psi$ tenim la de $\Psi\pi$; i la imatge per $\Psi\pi$ dels generadors, $\{x_i\phi\}_i$, genera (i, per tant és base de) $F_n$. És a dir, $\phi$ és automorfisme.

Vegem a continuació que $\det(\mathbf{Q}) = \pm 1$. De nou, de l'exhaustivitat de $\Psi$ tenim que per a tot $j$ hi ha antiimatges dels $t_j \in F_n \times \mathbb{Z}^m$. Sabem doncs que, per a tot $j \in [1, m]$, existeixen $\mathbf{b}_j \in \mathbb{Z}^m$ i $u_j \in F_n$ tals que

$$(\mathbf{t}^{\mathbf{b}_j} u_j)\Psi = t_j = \mathbf{t}^{\boldsymbol{\delta}_j}.$$

Aleshores, usant l'expressió per als endomorfismes de tipus I, als que sabem que ha de pertànyer $\Psi$, i separant les parts lliure i abeliana, queda

$$\begin{cases} u_j\phi = 1 \\ \mathbf{b}_j\mathbf{Q} + \mathbf{u}_j\mathbf{P} = \boldsymbol{\delta}_j \end{cases}.$$

Ara, com que $\phi$ és automorfisme, $u_j = 1$, $\mathbf{u} = \mathbf{0}$ i la segona equació queda $\mathbf{b}_j\mathbf{Q} = \boldsymbol{\delta}_j$. Hem vist, per tant, que existeix un $\mathbf{b}_j \in \mathbb{Z}^m$ tal que

$$\mathbf{b}_j\mathbf{Q} = \boldsymbol{\delta}_j, \quad \forall j \in [1, m] .$$

Anomenant $\mathbf{B}$ la matriu que té per files els $\mathbf{b_j}$ obtenim $\mathbf{BQ} = \mathbf{I_n}$ amb $\mathbf{B} \in \mathcal{M}_m(\mathbb{Z})$, d'on $\mathbf{Q}$ és invertible a $\mathcal{M}_m(\mathbb{Z})$, i.e. $\det(\mathbf{Q}) = \pm 1$.

[$\Leftarrow$] Volem veure que per a tot $\mathbf{t^a}u$ existeix un $\mathbf{t^b}v$ tal que $(\mathbf{t^b}v)\Psi = \mathbf{t^a}u$, és a dir que per a tot $\mathbf{a} \in \mathbb{Z}^m$ i per a tot $u \in F_n$, existeixen $\mathbf{b} \in \mathbb{Z}^m$ i $v \in F_n$ tals que $\mathbf{t}^{\mathbf{bQ+vP}}v\phi = \mathbf{t^a}u$. Separant les parts lliure i abeliana queda

$$\begin{cases} v\phi = u \\ \mathbf{bQ} + \mathbf{vP} = \mathbf{a} \end{cases}.$$

Aleshores, donat que $\phi$ és automorfisme de $F_n$, tenim que $v = u\phi^{-1}$ i per tant $\mathbf{v} = \mathbf{uA}^{-1}$ amb $\mathbf{A}$ l'abelianització de $\phi$. Ara usant que $\det(\mathbf{Q}) = \pm 1$ podem aïllar $\mathbf{b}$ de la segona equació

$$\mathbf{b} = (\mathbf{a} - \mathbf{vP})\mathbf{Q}^{-1} = (\mathbf{a} - \mathbf{uA^{-1}P})\mathbf{Q}^{-1},$$

obtenint les $v$ i $\mathbf{b}$ desitjades, i per tant, l'exhaustivitat de $\Psi$. □

OBSERVACIÓ 9. El desenvolupament anterior proporciona les antiimatges per $\Psi$ epimorfisme, que resulten ser úniques. Així doncs queda determinada la seva *inversa* i $\Psi$ és automàticament monomorfisme (i per tant *automorfisme*) la qual cosa és, per suposat, també conseqüència directa de les caracteritzacions donades.

COROL.LARI 3.2. *$F_n \times \mathbb{Z}^m$ és hopfià i no cohopfià.*

DEMOSTRACIÓ. Usant les caracteritzacions establertes a les proposicions 2.1 i 3.1, tenim

$$\Psi \text{ epi } \Leftrightarrow \left\{ \begin{array}{l} \Psi \text{ de } \textit{tipus I} \\ \phi \text{ auto de } F_n \\ \det(\mathbf{Q}) = \pm 1 \end{array} \right\} \begin{array}{c} \Rightarrow \\ \not\Leftarrow \end{array} \left\{ \begin{array}{l} \Psi \text{ de } \textit{tipus I} \\ \phi \text{ mono de } F_n \\ \det(\mathbf{Q}) \neq 0 \end{array} \right\} \Leftrightarrow \Psi \text{ mono.}$$

□

Malgrat que la hopfianitat de $F_n \times \mathbb{Z}^m$ no és directament deduïble de ser producte directe de grups hopfians finitament generats (a [**13**], Tyrer, partint d'un grup simple S adequat, obté un subgrup de $S^{\mathbb{N}}$ finitament generat no hopfià que és producte directe de dos grups hopfians), sí que era coneguda per ser $F_n \times \mathbb{Z}^m$ un *PC-group*. La hopfianitat dels *PC-groups* és conseqüència del seu caràcter residualment finit, establert per Green a la seva tesi doctoral [**7**] i també deduïble del fet de ser grups lineals tal i com demostra Humphries a [**9**]. És ben sabut (es pot trobar una demostració a [**11**], p.195-196) que tot grup finitament presentat residualment finit és hopfià, per tant ho són els *PC-groups* i en particular $F_n \times \mathbb{Z}^m$ tal i com s'ha comprovat aquí directament a partir de la forma dels seus monomorfismes i epimorfimes.

## 4. Automorfismes

En vista de la hopfianitat de $F_n \times \mathbb{Z}^m$, la caracterització donada a la proposició 3.1 per als epimorfismes, també ho és per als isomorfismes. Resumim el que això suposa seguidament.

TEOREMA 4.1. *$\Psi$ és automorfisme de $F_n \times \mathbb{Z}^m$ si i només si és de la forma*

$$\Psi_{\phi,\mathbf{Q},\mathbf{P}} : \mathbf{t}^{\mathbf{a}} u \longmapsto \mathbf{t}^{\mathbf{aQ}+u\mathbf{P}}\, u\phi \ , \tag{16}$$

*amb $\phi$ automorfisme de $F_n$, $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$. És més, tenim que l'aplicació*

$$\Psi_{\phi,\mathbf{Q},\mathbf{P}} \longmapsto (\phi, \mathbf{Q}, \mathbf{P})$$

*estableix un isomorfisme entre* $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$ *i el conjunt* $\mathrm{Aut}(F_n) \times \mathrm{GL}_m(\mathbb{Z}) \times \mathcal{M}_{n\times m}(\mathbb{Z})$ *amb l'operació induïda*

$$(\phi, \mathbf{Q}, \mathbf{P})\,(\phi', \mathbf{Q}', \mathbf{P}') = (\phi\phi', \mathbf{QQ}', \mathbf{PQ}' + \mathbf{AP}') \ , \tag{14'}$$

*neutre* $(\mathrm{id}_{F_n}, \mathbf{I}_m, \mathbf{0})$ *i invers* $(\phi, \mathbf{Q}, \mathbf{P})^{-1} = (\phi^{-1}, \mathbf{Q}^{-1}, -\mathbf{A}^{-1}\mathbf{P}\mathbf{Q}^{-1})$. *Com sempre,* $\mathbf{A}$ *designa l'abelianitzat de $\phi$.*

DEMOSTRACIÓ. La primera part no és més que l'enunciat de la proposició 3.1 donada la hopfianitat, i la segona surt de considerar la restricció de l'isomorfisme de monoides establert al corol.lari 1.4 a $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$ d'acord amb la caracterització obtinguda per als automorfismes. □

Tal i com fèiem amb els endomorfismes de tipus I, podrem pensar els automorfismes de $F_n \times \mathbb{Z}^m$ com a ternes $(\phi, \mathbf{Q}, \mathbf{P})$, ara de

$$\mathrm{Aut}(F_n) \times \mathrm{GL}_m(\mathbb{Z}) \times \mathcal{M}_{n\times m}(\mathbb{Z})$$

amb l'operació (14') i, evidentment, l'expressió (15) obtinguda per a les potencies és valida en el cas particular dels automorfismes.

També serà convenient disposar de la forma general, en termes de la nova notació, dels automorfismes interns de $F_n \times \mathbb{Z}^m$. No és d'estranyar, donada la commutativitat de les $t^{\text{'s}}$, que només es conservi la conjugació de la part lliure.

Lema 4.2. *Sigui* $\mathbf{t}^{\mathbf{a}}u \in F_n \times \mathbb{Z}^m$*, aleshores l'automorfisme intern resultat de conjugar per* $\mathbf{t}^{\mathbf{a}}u$ *és*

$$\Gamma_{\mathbf{t}^{\mathbf{a}}u} = (\gamma_u, \mathbf{I_m}, \mathbf{0})\ .$$

Demostració. En efecte, per a tot $\mathbf{t}^{\mathbf{b}}v \in F_n \times \mathbb{Z}^m$, tenim

$$(\mathbf{t}^{\mathbf{b}}v)\Gamma_{\mathbf{t}^{\mathbf{a}}u} = (\mathbf{t}^{\mathbf{a}}u)^{-1}\,(\mathbf{t}^{\mathbf{b}}v)\,(\mathbf{t}^{\mathbf{a}}u) = \mathbf{t}^{-\mathbf{a}+\mathbf{b}+\mathbf{a}}\ u^{-1}vu = \mathbf{t}^{\mathbf{b}}\ (v)\gamma_u\ .$$

És a dir, $\phi = \gamma_u$, $\mathbf{Q} = \mathbf{I_m}$ i $\mathbf{P} = \mathbf{0}$, com volíem demostrar. □

Establim a continuació una descomposició particularment simple i convenient dels automorfismes de $F_n \times \mathbb{Z}^m$ que ens permetrà obtenir com a conseqüència gairebé immediata el caràcter finitament generat de $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$.

Lema 4.3. *Sigui* $(\phi, \mathbf{Q}, \mathbf{P})$ *un automorfisme genèric de* $F_n \times \mathbb{Z}^m$*, aleshores es té*

$$(\phi, \mathbf{Q}, \mathbf{P}) = (\phi, \mathbf{I_m}, \mathbf{0})\,(\mathrm{id}_{F_n}, \mathbf{Q}, \mathbf{0})\,(\mathrm{id}_{F_n}, \mathbf{I_m}, \mathbf{A}^{-1}\mathbf{P})\ . \tag{17}$$

Demostració. És una comprovació rutinària que el producte (14) dels tres elements de la dreta és igual a l'element de l'esquerra,

$$(\phi, \mathbf{I_m}, \mathbf{0})\,(\mathrm{id}_{F_n}, \mathbf{Q}, \mathbf{0})\,(\mathrm{id}_{F_n}, \mathbf{I_m}, \mathbf{A}^{-1}\mathbf{P}) = (\phi, \mathbf{Q}, \mathbf{0})\,(\mathrm{id}_{F_n}, \mathbf{I_m}, \mathbf{A}^{-1}\mathbf{P}) = (\phi, \mathbf{Q}, \mathbf{P}).$$

□

El lema anterior ens diu que podem pensar tot automorfisme de $F_n \times \mathbb{Z}^m$ com a 'producte' d'un automorfisme de $F_n$, un element de $\mathrm{GL}_m(\mathbb{Z})$ i una matriu de $\mathcal{M}_{n\times m}(\mathbb{Z})$. Serà suficient aleshores donar un sistema de generadors finit de cadascun dels constituents per obtenir-ne un de $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$.

Proposició 4.4. *El grup* $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$ *és finitament generat.*

Demostració. Observem, en primer lloc, que es tenen els tres monomorfismes naturals següents:

$$\begin{array}{ccc} \mathrm{Aut}(F_n) & \to & \mathrm{Aut}(F_n \times \mathbb{Z}^m) \\ \phi & \mapsto & (\phi, \mathbf{I_m}, \mathbf{0}) \end{array}\ ,$$

$$\begin{array}{rcl} \mathrm{GL}_m(\mathbb{Z}) & \to & \mathrm{Aut}(F_n \times \mathbb{Z}^m) \\ \mathbf{Q} & \mapsto & (\mathrm{id}_{F_n}, \mathbf{Q}, \mathbf{0}) \end{array}, \text{ i}$$

$$\begin{array}{rcl} \mathcal{M}_{n\times m}(\mathbb{Z}) & \to & \mathrm{Aut}(F_n \times \mathbb{Z}^m) \\ \mathbf{P} & \mapsto & (\mathrm{id}_{F_n}, \mathbf{I_m}, \mathbf{P}) \end{array};$$

on les operacions als grups de l'esquerra són respectivament: la composició d'automorfismes a $\mathrm{Aut}(F_n)$, el producte de matrius a $\mathrm{GL}_m(\mathbb{Z})$, i la suma de matrius a $\mathcal{M}_{n\times m}(\mathbb{Z})$. És rutinari a partir de (14') que les anteriors aplicacions (evidentment injectives) són morfismes.

Ara, en vista de la descomposició (17), serà suficient donar sistemes de generadors finits per als tres grups origen i considerar les seves respectives immersions (mitjançant els monomorfismes anteriors) en $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$.

Així doncs, podem prendre els següents sistemes de generadors:

- les transformacions elementals de Nielsen, $\{\eta_k\}_k$, per $\mathrm{Aut}(F_n)$;
- les matrius elementals, $\{\mathbf{E_l}\}_l$, per $\mathrm{GL}_m(\mathbb{Z})$; i
- les $n \times m$ matrius canòniques

$$\mathbf{M_{ij}} = \begin{array}{cc} & j \\ i & \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix} \end{array},$$

  per $(\mathcal{M}_{n\times m}(\mathbb{Z}), +)$.

Obtenint el següent sistema de generadors finit per $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$,

$$\{(\eta_k, \mathbf{I_m}, \mathbf{0})\}_k \cup \{(\mathrm{id}_{F_n}, \mathbf{E_l}, \mathbf{0})\}_l \cup \{(\mathrm{id}_{F_n}, \mathbf{I_m}, \mathbf{M_{ij}})\}_{i,j}\ . \tag{18}$$

□

Aquest és un resultat ja conegut en un àmbit molt més general. A [**10**], Laurence dóna un sistema de generadors finit per al grup d'automorfismes del *PC-group* de tot graf finit. Donat que $F_n \times \mathbb{Z}^m$ és el *PC-group* definit pel *join graph* del graf nul de $n$ vèrtexs (que identificarem amb els generadors $\{x_i\}_i$ de $F_n$) i el graf complet de $m$ vèrtexs (que identificarem amb els generadors $\{t_j\}_j$ de $\mathbb{Z}^m$), podem traduir al nostre cas els automorfismes generadors donats per Laurence resultant essencialment (amb certes redundàncies) els mateixos que hem obtingut aquí. Concretament,

- els *graph automorphisms* (automorfismes que permuten vèrtexs) només poden permutar entre si vèrtexs del mateix subgraf constituent. Obtenim per tant automorfismes de la forma $(\sigma, \mathbf{I_m}, \mathbf{0})$ amb $\sigma$ automorfisme de $F_n$ que permuta el conjunt $\{x_i\}_i$ (de vegades considerat elemental de Nielsen) i $(\mathrm{id}_{F_n}, \mathbf{Q_p}, \mathbf{0})$ amb $\mathbf{Q_p}$ matriu de permutació i per tant elemental.

- Les *inversions* (automorfismes que inverteixen un vèrtex i fixen la resta) prenen, en el nostre cas, les formes $(\mathrm{id}_{F_n}, \mathbf{I_m} - 2\mathbf{M_{jj}}, \mathbf{0})$ on és clar que $\mathbf{I_m} - 2\mathbf{M_{jj}}$ és una matriu elemental de $\mathrm{GL}_m(\mathbb{Z})$ i $(\alpha_{x_i}, \mathbf{I_m}, \mathbf{0})$ amb $\alpha_{x_i}$ l'automorfisme (elemental de Nielsen) de $F_n$ que envia $x_i \mapsto x_i^{-1}$ i fixa la resta ($j \in [1, m],\ i \in [1, n]$).
- les *transvections* (automorfismes amb l´únic vèrtex no fix $x$ transformat d'acord amb $x \mapsto xy^{\pm 1}$ o $x \mapsto y^{\pm 1}x$, on $y \neq x$ és un vèrtex que té les mateixes adjacències que $x$, excepte les que suposarien llaços) donen sobre $F_n \times \mathbb{Z}^m$ la següent casuística:
  Si $x = x_i$ i $y = x_j$ amb $j \neq i$ (les adjacències d'ambdós són amb els $\{t_j\}_j$) obtenim els automorfismes $(\beta, \mathbf{I_m}, \mathbf{0})$ amb $\beta$ (elemental de Nielsen) que envia $x_i$ a $x_i x_j^{\pm 1}$ o $x_j^{\pm 1} x_i$ i fixa la resta.
  Si $x = x_i$ i $y = t_j$ (els $t_j$ són adjacents entre ells, i per tant, als veïns de $x_i$) tenim l'automorfisme que envia $x_i \mapsto t_j^{\pm 1} x_i = x_i t_j^{\pm 1}$ i fixa la resta. En la nostra notació són $(\mathrm{id}_{F_n}, \mathbf{I_m}, \pm\mathbf{M_{ij}})$ ($j \in [1, m],\ i \in [1, n]$).
  Si $x = t_j$ i $y = t_k$ amb $j \neq k$ ($t_k$ té les adjacències de $t_j$ excepte el llaç a $t_k$) queda l'automorfisme que envia $t_j \mapsto t_j t_k^{\pm 1} = t_k^{\pm 1} t_j$. Així doncs, d'aquest tercer cas obtenim la família $(\mathrm{id}_{F_n}, \mathbf{I_m} \pm \mathbf{M_{jk}}, \mathbf{0})$ ($j, k \in [1, m]$ tals que $j \neq k$), on, de nou, és clar que les $\mathbf{I_m} \pm \mathbf{M_{jk}}$ són matrius elementals.

Observem que amb els *graph automorphisms*, les *inversions*, i les *transvections* obtenim ja tots els generadors de (18). Descriurem, no obstant, per completesa, l'aspecte que tenen en el nostre cas el quart i últim tipus d'automorfismes donats per Laurence,

- els *locally inner automorphisms* s'obtenen mitjançant el següent procediment. Donat un vèrtex $x$, sigui $\Delta$ el subgraf resultant d'eliminar del graf original el vèrtex $x$, els vèrtexs adjacents a $x$ i les arestes incidents als vèrtexs eliminats. Aleshores per a cada subgraf $\Xi$ unió de components connexes de $\Delta$ considerem l'automorfisme (*locally inner*) que a tot vèrtex $y$ de $\Xi$ el transforma conjugant-lo per x i deixa fixes la resta.
  En el nostre cas, si partim d'un dels $x_i$, el subgraf $\Delta$ associat és el graf nul que té per vèrtexs els $\{x_j\}_{j \neq i}$ restants; aleshores, els possibles $\Xi$ no són més que els subconjunts de $\{x_j\}_{j \neq i}$. D'aquesta manera obtenim per cada $x_i$ i cada $S \subseteq \{x_j\}_{j \neq i}$, l'automorfisme $(\gamma_{x_i, S}, \mathbf{I_m}, \mathbf{0})$ de $F_n \times \mathbb{Z}^m$, on $\gamma_{x_i, S}$ és l'automorfisme de $F_n$ que envia tot $x_k \in S$ a $x_i x_k x_i^{-1}$ i deixa fixes els vèrtexs de $\{x_i\}_i \setminus S$.
  Observem per últim que si partim de qualsevol dels $t_j$, el corresponent subgraf $\Delta$ és buit i en conseqüència també ho és l'únic $\Xi$ a considerar. Per tant tots els *locally inner automorphisms* provinents de les $t_j^{\text{'s}}$ prenen la forma $(\mathrm{id}_{F_n}, \mathbf{I_m}, \mathbf{0})$, és a dir la forma de l'automorfisme identitat de $F_n \times \mathbb{Z}^m$, que evidentment no cal incloure en cap sistema de generadors.

# Part 2

# Problemes algorísmics

# Capítol 3
# Problemes resolts

"Begin at the beginning and go
on till you come to the end:
then stop."

The King

Un problema de decisió és un enunciat que, en funció d'unes certes dades d'entrada, assoleix un entre dos valors possibles (típicament `veritable` i `fals`). Una solució algorísmica d'un problema de decisió és un procediment computacional (expressable, per exemple, en termes d'una màquina de Turing) que a partir de les dades d'entrada, retorni `SI` en cas que l'expressió prengui el valor `veritable`, i retorni `NO` en cas contrari. Quan disposem d'un tal algorisme direm que el problema de decisió és *algorísmicament decidible*. Sovint, sobreentenent el caràcter algorísmic del plantejament direm simplement que el problema és *decidible* o *resoluble*.

Des d'un punt de vista algorísmic l'enunciat "sigui $G$ un grup" no és suficientment precís. El comportament algorísmic d'un grup pot dependre de la forma com ens ha estat donat. Així doncs, pel que fa als problemes de decisió algorísmica per a grups, suposarem sempre que els ingredients del problema ens han estat donats de forma *algorísmica*: els elements han d'estar representats per objectes finits, els processos de multiplicació i inversió han de poder realitzar-se de forma algorísmica i els morfismes entre grups han d'estar representats per una quantitat finita d'informació de manera que hom pugui computar algorísmicament les imatges.

Un cop establerta la connexió entre l'univers lliure per lliure-abelià i els seus factors, es fa palès que certs problemes de decisió algorísmica a $G = F_n \times \mathbb{Z}^m$ es traduiran en les respectives versions del problema sobre la part lliure (on ja es disposa de molts resultats) i la part lliure-abeliana (sobre la que alguns dels problemes de decisió prenen una forma trivial o resoluble fàcilment amb àlgebra lineal), juntament amb una certa complicació derivada de com estan entrellaçades a $G$ les parts lliures i lliure-abelianes del problema. Succeeix que aquest entrellaçament és, en molt casos, de tipus lineal i per tant atacable amb eines clàssiques. Així, tractarem de reduir els problemes de decisió que considerarem sobre els nostres grups, als problemes homònims sobre el grup lliure, juntament amb un problema abelià més o menys sofisticat.

En tota la part algorísmica suposarem, si no s'indica el contrari, que el grup lliure per lliure abelià sobre el que es plantegen els problemes és finitament generat i donat per una presentació finita, concretament

$$G = F_n \times \mathbb{Z}^m = \langle\, X \mid \,\rangle \times \langle\, T \mid [T,T]\,\rangle = \langle X, T \mid [X \sqcup T, T]\,\rangle \tag{19}$$

on $n, m \in \mathbb{N}$, $X = \{x_1, \ldots, x_n\}$ i $T = \{t_1, \ldots, t_m\}$ són conjunts disjunts, i $[X \sqcup T, T]$ és el conjunt de commutadors de $X \sqcup T$ amb $T$. Suposarem també que els elements, subgrups, morfismes i altres objectes associats al grup $G$ que apareguin en els problemes de decisió venen, per defecte, donats algorísmicament en termes de la presentació anterior.

Comentem, a mode introductori, l'aparença que prenen en el nostre cas els tres problemes clàssics de Dehn i la seva decidibilitat.

- el *word problem*, $\mathrm{WP}(F_n \times \mathbb{Z}^m)$, consistent en decidir, donada una paraula en els generadors (que estem suposant són els $X, T$ donats per la presentació), si aquesta paraula representa l'element neutre a $G$.
  De forma semblant al que succeïa en els casos lliure i lliure-abelià, l'existència d'una forma normal per als elements de $G$ converteix el problema en trivial. Així, d'acord amb el lema 1.1, donada una paraula $g = g(X, T)$ en els generadors, només cal posar-la en forma normal $\mathbf{t}^{\mathbf{a}}\, u$ (procés evidentment algorísmic). Aleshores $g =_G 1$ si i només si $\mathbf{a} = \mathbf{0}$ i $u = 1$. Per tant, el *word problem* per als grups $F_n \times \mathbb{Z}^m$ és decidible.
- el *conjugacy problem*, $\mathrm{CP}(F_n \times \mathbb{Z}^m)$, consistent en decidir, donades dues paraules qualssevol en els generadors, si aquestes representen elements conjugats a $G$.
  Un cop escrites les dues paraules en forma normal, $\mathbf{t}^{\mathbf{a}} u$ i $\mathbf{t}^{\mathbf{b}} v$, el problema consisteix en decidir sobre l'existència d'un cert $\mathbf{t}^{\mathbf{c}} w \in G$ tal que $(\mathbf{t}^{\mathbf{c}} w)^{-1}\, \mathbf{t}^{\mathbf{a}} u\, \mathbf{t}^{\mathbf{c}} w = \mathbf{t}^{\mathbf{b}} v$. Després de les manipulacions òbvies derivades de la commutativitat de les $\mathbf{t}'^{\mathrm{s}}$, tot queda reduït a comprovar si $\mathbf{a} = \mathbf{b}$ i decidir si $u$ i $v$ són conjugats a $F_n$, és a dir al *conjucacy problem* de $F_n$ (decidible mitjançant un procés de reducció cíclica i cancel.lació). Així doncs, el *conjucacy problem* per als grups $F_n \times \mathbb{Z}^m$ és decidible.
- l'*isomorphism problem*, $\mathrm{IP}(F_n \times \mathbb{Z}^m)$, consistent en decidir, donades dues presentacions finites de grups lliure per lliure-abelià, si presenten grups isomorfs. (Evidentment, ara no estem pressuposant que les presentacions siguin de la forma (19)).
  Tal i com hem demostrat al corol.lari 3.2, un argument diagonal juntament amb la caracterització 2.6 proporcionen fàcilment la decidibilitat de l'isomorphism problem per als grups $F_n \times \mathbb{Z}^m$.

Estudiem a continuació, una primera generalització natural, bastant immediata en el nostre cas, del *word problem* de Dehn.

# 1. Membership problem

Si $H$ és un subgrup finitament generat de $G$, el *membership problem per $H$ a $G$*, $\mathrm{MP}(H,G)$, és el problema consistent en decidir, donat un element $g \in G$ qualsevol, si $g \in H$. El *(generalized) membership problem* per $G$, $\mathrm{MP}(G)$, és el problema consistent en decidir, donats un subgrup finitament generat $H \leqslant G$ arbitrari i un element $g \in G$ qualsevol, si $g \in H$.

En ambdós casos estem suposant, com sempre, que $H$ ve donat per un nombre finit $\{h_1,\dots,h_s\}$ de generadors, i tant aquests com $g$, com a paraules en els generadors originals de $G$.

En els casos de $F_n$ i $\mathbb{Z}^m$ el *membership problem* és fàcilment decidible. Per a $F_n$, es tracta només de si es pot o no llegir la paraula corresponent a $g$ sobre el *folded graph* de Stallings de $H$, i el cas lliure-abelià és de comprovació immediata.

Proposició 1.1. *El* membership problem *del grup $G = F_n \times \mathbb{Z}^m$ és decidible, i en cas afirmatiu (i.e. quan $g \in H$) podem calcular l'expressió de $g$ en termes dels generadors de $H$.*

Demostració. Siguin $g, h_1, \dots, h_s$ paraules en els generadors $X, T$ de G. Volem decidir algorísmicament si, pensades com a elements de $G$, es compleix $g \in \langle h_1, \dots, h_s\rangle = H$.

És clar, en primer lloc, que a efectes del que ens interessa podem suposar les paraules anteriors escrites en forma normal, ja que si no ho estan d'entrada, el procediment de conversió a forma normal es pot fer, certament, de manera algorísmica.

Siguin doncs, $g = \mathbf{t}^{\mathbf{a}}\, u$ un element qualsevol de $G$, i $E = E_X \sqcup E_T$ una $\alpha$-base de $H$ (que podem calcular a partir de $\{h_1,\dots,h_s\}$ d'acord amb la proposició 4.2). Ara, el següent procediment decideix el *membership problem* de $G$:

(1) Decidim si $u \in \langle (E_X)\pi \rangle$.
Això no és més que el *membership problem* a $F_n$, que podem decidir ja que disposem de $(E_X)\pi$ conjunt de generadors (de fet base lliure) de $\langle (E_X)\pi \rangle$.
En cas de resposta negativa (la part lliure de $g$ no està continguda a la projecció lliure de $H$ i per tant $g \notin H$) també ho serà la del *membership problem* de $G$. Si la resposta és afirmativa passem al punt següent.

(2) Decidim si $(u\alpha)^{-1}g \in \langle E_T \rangle$.
És clar per construcció que $(u\alpha)^{-1}g \in \mathbb{Z}^m$, aleshores només es tracta de determinar l'existència de solucions d'un sistema diofàntic lineal, i el problema és, per tant, decidible.

En segon lloc, hem vist també a la proposició 4.2 que donats un element $g$ i una base $E$ de $H$, podíem obtenir algorísmicament l'expressió de $g$ en base $E$. I com el procés d'obtenció de la base $E$ a partir dels generadors originals és reversible, podrem també calcular l'expressió de $g$ en termes d'aquests. $\square$

## 2. Subgrups d'índex finit

En aquest apartat l'objectiu és decidir, per un subgrup $H \leqslant G$ generat per una família finita d'elements de $G$, si és o no d'índex finit, i, si la resposta és afirmativa buscar una col.lecció de representants de les corresponents classes laterals.

Comencem recordant amb un lema un parell propietats elementals que necessitarem sobre el comportament de l'índex sota epimorfismes.

LEMA 2.1. *Siguin $G$ i $G'$ grups qualssevol i $\rho : G \twoheadrightarrow G'$ un epimorfisme entre ells, aleshores:*

(a) $H \leqslant G \;\Rightarrow\; [G' : H\rho] \leq [G : H]$ ,
*en particular,* $H \leqslant_{f.i.} G \;\Rightarrow\; H\rho \leqslant_{f.i.} G'$.
(b) $H' \leqslant G' \;\Rightarrow\; [G' : H'] = [G : H'\rho^{-1}]$ ,
*en particular,* $H' \leqslant_{f.i.} G' \;\Leftrightarrow\; H'\rho^{-1} \leqslant_{f.i.} G$.

DEMOSTRACIÓ. (a) És suficient veure que l'aplicació $Hx \mapsto (Hx)\rho$ del conjunt de classes laterals per la dreta de $G$ mòdul $H$ en el conjunt classes laterals per la dreta de $G'$ mòdul $H\rho$ està ben definida i és exhaustiva.

Està ben definida donat que la imatge de qualsevol subconjunt és única i $(Hx)\rho = (H\rho)\,x\rho$ és una classe lateral per la dreta de $G'$ mòdul $H\rho$. L'exhaustivitat és conseqüència immediata de la de $\rho$, en efecte, per a tota $(H\rho)\,x'$ classe lateral per la dreta de $G'$ mòdul $H\rho$, $x' \in G'$, i en ser $\rho$ exhaustiva existeix un $x \in G$ tal que $x\rho = x'$. Per tant $(Hx)\rho = (H\rho)\,x\rho = (H\rho)\,x'$ i tota classe lateral per la dreta de $G'$ mòdul $H\rho$ és imatge per l'aplicació donada d'una classe lateral per la dreta de $G$ mòdul $H$, tal i com volíem veure.

(b) Considerem ara l'aplicació $H'x' \mapsto (H'x')\rho^{-1}$ del conjunt de classes laterals per la dreta de $G'$ mòdul $H'$ en el conjunt de classes laterals per la dreta de $G$ mòdul $H'\rho^{-1}$. Volem veure que està ben definida i és bijectiva.

Evidentment la preimatge completa d'un conjunt per una aplicació és única. D'altra banda $y \in (H'x')\rho^{-1}$ si i només si $y\rho(x')^{-1} \in H'$, i de l'exhaustivitat de $\rho$, si i només si $y\rho(x\rho)^{-1} \in H'$, amb $x \in G$ tal que $x\rho = x'$. En ser $\rho$ morfisme, l'anterior és equivalent a $(yx^{-1})\rho \in H'$, és a dir a $y \in (H'\rho^{-1})\,x$. Així doncs $(H'x')\rho^{-1} = (H'\rho^{-1})\,x$ amb $x$ preimatge de $x'$ per $\rho$, i l'aplicació està ben definida.

L'exhaustivitat es dedueix directament del que acabem de veure, en efecte donada $(H'\rho^{-1})\,x$ una classe lateral per la dreta de $G$ mòdul $H'\rho^{-1}$, tenim que $(H'\rho^{-1})\,x = (H'\,x\rho)\rho^{-1}$. La injectivitat és immediata de l'exhaustivitat de $\rho$. ◻

Observem que si $H$ és un subgrup d'índex finit de $G = F_n \times \mathbb{Z}^m$, el primer apartat del lema 2.1 aplicat a les projeccions lliure, $\pi : \mathbf{t^a}u \mapsto u$, i abeliana, $\tau : \mathbf{t^a}u \mapsto \mathbf{t^a}$, estableix la finitud dels índexs $[F_n : H\pi]$ i $[\mathbb{Z}^m : H\tau]$, és a dir

$$H \leqslant_{f.i.} F_n \times \mathbb{Z}^m \;\Rightarrow\; \begin{cases} H\pi \leqslant_{f.i.} F_n \\ H\tau \leqslant_{f.i.} \mathbb{Z}^m \end{cases}. \tag{20}$$

Per tant la finitud dels índexs $[F_n : H\pi]$ i $[\mathbb{Z}^m : H\tau]$ és una condició necessària per a la de l'índex $[G : H]$ de tot subgrup $H$ de $G$. Ara, si $H$ està donat mitjançant una família finita de generadors, també ho estaran $H\pi$ i $H\tau$ i, en aquestes condicions, sabem decidir (algorísmicament) si els respectius índexs, $[F_n : H\pi]$ i $[\mathbb{Z}^m : H\tau]$, són finits. En el cas lliure, l'índex és finit si i només si tots els vèrtexs del *folded graph de Stallings* corresponent al subgrup $H$ són complets (i, en tal cas l'índex coincideix amb el nombre de vèrtexs); mentre que, com és ben sabut, un subgrup de $\mathbb{Z}^m$ té índex finit si i només si té rang $m$. És clar que tant el procés d'obtenció del *folded graph*, com la determinació del rang d'un subgrup d'un grup abelià són processos algorísmics.

Així doncs, si algun dels dos índexs $[F_n : H\pi]$ i $[\mathbb{Z}^m : H\tau]$ no és finit tampoc ho serà $[G : H]$ i haurem acabat. Notem que la situació contraria (quan ambdós índexs són finits) també conclouria si la implicació recíproca de (20) fos certa, però aquest no és el cas, com prova el següent senzill contraexemple.

Exemple 3. Considerem a $G = F_2 \times \mathbb{Z}^2 = \langle a, b \mid \rangle \times \langle s, t \mid [s,t] \rangle$ el subgrup $H = \langle sa, tb \rangle$. És clar que $H\pi = F_2$ i $H\tau = \mathbb{Z}^2$ i per tant els índexs $[F_2 : H\pi]$ i $[\mathbb{Z}^2 : H\tau]$ són finits (iguals a 1), mentre que l'índex $[F_n \times \mathbb{Z}^m : H]$ no pot ser finit ja que cap potència de $a$ pertany a $H$.

Sembla raonable, per tant, intentar reforçar les condicions necessàries de (20) (mantenint tant la seva necessarietat com el caràcter algorísmic de la seva decisió) per fer-les també suficients i així poder deduir la finitud de

$[G : H]$ del seu compliment. Una temptativa natural en aquesta direcció és substituir a (20), $H\pi$ i $H\tau$ per subgrups seus adients. Veurem en el que resta de secció que l'estratègia proposada és reeixida considerant els subgrups $H \cap F_n \leqslant H\pi$ i $H \cap \mathbb{Z}^m \leqslant H\tau$.

LEMA 2.2. *Siguin $G$ un grup qualsevol i $H, K$ subgrups de $G$, aleshores*

$$[K : H \cap K] \leq [G : H] ,$$

*en particular, $H \leqslant_{f.i.} G \;\Rightarrow\; H \cap K \leqslant_{f.i.} K$.*

DEMOSTRACIÓ. Vegem que l'aplicació $(H \cap K)k \mapsto Hk$ entre el conjunt de classes laterals per la dreta de $K$ mòdul $H \cap K$ i el conjunt de classes laterals per la dreta de $G$ mòdul $H$ està ben definida i és injectiva. En efecte, tenim per a tot $k, k' \in K$,

$$(H \cap K)\, k = (H \cap K)\, k' \;\Leftrightarrow\; k'k^{-1} \in H \cap K \;\Leftrightarrow\; k'k^{-1} \in H \;\Leftrightarrow\; Hk = Hk'.$$

La relació de l'enunciat no és més que l'efecte sobre els cardinals dels conjunts de classes (índexs) de l'existència d'una injecció entre ells. □

LEMA 2.3. *Siguin $G_1$ i $G_2$ grups qualssevol, $G = G_1 \times G_2$ el seu producte directe i $H$ un subgrup de $G$, aleshores*

$$[G_1 \times G_2 : H] \leqslant [G_1 : H \cap G_1] \cdot [G_2 : H \cap G_2] ,$$

*en particular, $H \leqslant_{f.i.} G$ si i només si $H \cap G_1 \leqslant_{f.i.} G_1$ i $H \cap G_2 \leqslant_{f.i.} G_2$.*

DEMOSTRACIÓ. Vegem que l'aplicació

$$\begin{array}{rcl} (H \cap G_1)\backslash G_1 \;\times\; (H \cap G_2)\backslash G_2 & \longrightarrow & H \backslash (G_1 \times G_2) \\ \big(\, (H \cap G_1)\, g_1 \;,\; (H \cap G_2)\, g_2 \,\big) & \longmapsto & H\, g_1 g_2 \end{array} \tag{21}$$

està ben definida i és exhaustiva. En efecte, siguin $(H \cap G_1)\, g_1 = (H \cap G_1)\, g_1'$ i $(H \cap G_2)\, g_2 = (H \cap G_2)\, g_2'$, és a dir $g_1'\, g_1^{-1} \in H \cap G_1$ i $g_2'\, g_2^{-1} \in H \cap G_2$, aleshores ambdós pertanyen a $H$ i per tant també $g_1'\, g_1^{-1} g_2'\, g_2^{-1} \in H$. Ara, en estar $G_1$ i $G_2$ en producte directe, els seus elements commuten entre sí, llavors

$$g_2'\, g_1'\, (g_1\, g_2)^{-1} = g_2'\, g_1'\, g_2^{-1} g_1^{-1} = g_1'\, g_1^{-1} g_2'\, g_2^{-1} \in H ,$$

i, per tant, $H\, g_2'\, g_1' = H\, g_1 g_2$, i l'aplicació està ben definida. L'exhaustivitat és òbvia.

Així doncs, queda demostrada la desigualtat de l'enunciat. Aleshores és evident que si els dos índexs $[G_1 : H \cap G_1]$ i $[G_2 : H \cap G_2]$ són finits, també ho serà $[G_1 \times G_2 : H]$. El recíproc és conseqüència directa del lema 2.2. □

Aquest lema juntament amb el 2.2 aplicats al nostre cas ($G = F_n \times \mathbb{Z}^m$) proporcionen ja la caracterització que buscàvem.

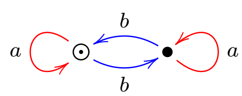
COROL.LARI 2.4. *Siguin* $G = F_n \times \mathbb{Z}^m$ *i* $H \leqslant G$*, aleshores*

$$[F_n \times \mathbb{Z}^m : H] \leq [F_n : H \cap F_n] \cdot [\mathbb{Z}^m : H \cap \mathbb{Z}^m] \ , \tag{22}$$

*en particular,* $H \leqslant_{f.i.} G$ *si i només si* $H \cap F_n \leqslant_{f.i.} F_n$ *i* $H \cap \mathbb{Z}^m \leqslant_{f.i.} \mathbb{Z}^m$*.* □

Pel que fa al càlcul de l'índex de $H$, la desigualtat (22), que tant pot ser estricta com assolir la igualtat, només ens en proporciona una fita. Veiem-ho amb un exemple.

EXEMPLE 4. Sigui $G = F_2 \times \mathbb{Z}^2 = \langle a, b \mid \rangle \times \langle s, t \mid [s,t] \rangle$ i considerem els subgrups $K = \langle a, b^2, bab \rangle$ i $K' = \langle s, t^2 \rangle$. $K$ és un subgrup del grup lliure $\langle a, b \mid \rangle$ que té folded graph de Stallings




amb tots dos vèrtexs complets, i per tant índex 2 a $F_2$. Més concretament, el graf anterior proporciona els representants $\{1, b\}$ de les classes laterals per la dreta mòdul $K$. D'altra banda, és evident que $\mathbb{Z}^2 = \langle s, t \rangle = K' \sqcup tK'$ i per tant $[F_2 : K] = [\mathbb{Z}^2 : K'] = 2$.

Ara és fàcil veure que el nou subgrup $H = \langle a, b^2, bab, s, t^2 \rangle$, amb interseccions $H \cap F_2 = K$ i $H \cap \mathbb{Z}^2 = K'$, té índex 4 a $G$ (el conjunt $\{1, b, t, tb\}$ constitueix un sistema complet de representants de les classes laterals per la dreta mòdul $H$) i hem construït un cas en el que l'expressió (22) assoleix la igualtat

$$[F_2 \times \mathbb{Z}^2 : H] = 4 = 2 \cdot 2 = [F_2 : H \cap F_2] \cdot [\mathbb{Z}^2 : H \cap \mathbb{Z}^2] \ .$$

Considerem finalment el subgrup $H'$ obtingut afegint un nou generador $tb$ als generadors de $H$, és a dir $H' = \langle a, b^2, bab, s, t^2, tb \rangle$. És clar, que mòdul $H'$, podem identificar les classes laterals per la dreta amb representants 1 i $tb$, i les classes amb representants $b$ i $t$, i que aquestes són totes les identificacions possibles. Així doncs, el conjunt $\{1, b\}$ és un sistema complet de representats de les classes laterals per la dreta de $H'$ que és, per tant, un subgrup d'índex 2 de $G$. Per altra banda és evident que les interseccions de $H'$ amb $F_n$ i $\mathbb{Z}^m$ coincideixen amb les respectives de $H$ i per tant tenen el mateix índex (2) en els ambients corresponents. En definitiva, per al subgrup $H'$ es té

$$[F_2 \times \mathbb{Z}^2 : H'] = 2 < 2 \cdot 2 = [F_2 : H' \cap F_2] \cdot [\mathbb{Z}^2 : H' \cap \mathbb{Z}^2] \ ,$$

constituint aquest un cas en el que la desigualtat a (22) és estricta.

Com a conseqüència immediata del lema 2.4, si $H$ ens ha estat donat mitjançant un conjunt finit de generadors, podrem decidir algorísmicament sobre la finitud del seu índex a $G$ quan puguem fer-ho sobre la del de $H \cap F_n$ a $F_n$ (és clar que sempre podrem validar algorísmicament la finitud de l'índex d'un subgrup de $\mathbb{Z}^m$ sense més que comprovar si el seu rang és màxim). Estudiem doncs aquest cas; sigui $H$ un subgrup de $F_n \times \mathbb{Z}^m$ que podem suposar (proposició 4.2) donat per una base

$$E = \{\, \mathbf{t}^{\mathbf{a_1}} u_1, \ldots, \mathbf{t}^{\mathbf{a_{n'}}} u_{n'}, \mathbf{t}^{\mathbf{b_1}}, \ldots, \mathbf{t}^{\mathbf{b_{m'}}} \,\}$$

amb $n', m' \in \mathbb{N}$, $\mathbf{a_1}, \ldots, \mathbf{a_{n'}} \in \mathbb{Z}^m$, $\{u_1, \ldots, u_{n'}\}$ base lliure de $H\pi \leqslant F_n$, i $\{\mathbf{b_1}, \ldots, \mathbf{b_{m'}}\}$ base lliure-abeliana de $H \cap \mathbb{Z}^m \leqslant \mathbb{Z}^m$. Com ja hem fet anteriorment, escriurem $L = \langle \mathbf{b_1}, \ldots, \mathbf{b_{m'}} \rangle$ i $\mathbf{A}$ la matriu sencera $n' \times m$ que té per files els $\mathbf{a_i} \in \mathbb{Z}$, $i \in [1, n']$.

Lema 2.5. *Amb aquestes notacions, tenim*

$$H \cap F_n = \{\, w \in F_n \mid \mathbf{0} \in \mathfrak{c}_{w,H} \,\} = \{\, w \in F_n \mid \boldsymbol{\omega}\mathbf{A} \in L \,\} \leqslant H\pi$$

*on $\boldsymbol{\omega}$ és l'abelianització de la paraula $\omega$ que expressa $w$ en termes de la base $\{u_1, \ldots, u_{n_1}\}$ de $H\pi$.*

Demostració. La primera igualtat és conseqüència immediata de la definició de la compleció abeliana, $\mathfrak{c}_{w,H}$, de $w$ en $H$; mentre que la segona ho és del corol.lari 4.4, en efecte $\mathbf{0} \in \boldsymbol{\omega}\mathbf{A} + L$ si i només si $\boldsymbol{\omega}\mathbf{A} \in L$. □

És a dir, si anomenem $\rho$ l'abelianització de $F_{n'}$, i $\mathbf{A}\colon \mathbb{Z}^{n'} \to \mathbb{Z}^m$ el morfisme $\mathbf{v} \mapsto \mathbf{v}\mathbf{A}$ corresponent a multiplicar per l'esquerra de la matriu $\mathbf{A}$, tenim

$$\begin{array}{ccccccc} F_n \geqslant H\pi & \cong & F_{n'} & \overset{\rho}{\twoheadrightarrow} & \mathbb{Z}^{n'} & \xrightarrow{\mathbf{A}} & \mathbb{Z}^m \\ \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} \\ H \cap F_n & \cong & (L)\mathbf{A}^{-1}\rho^{-1} & \longleftarrow\!\shortmid & (L)\mathbf{A}^{-1} & \longleftarrow\!\shortmid & L \end{array} , \tag{23}$$

on hem designat $\mathbf{A}^{-1}$ i $\rho^{-1}$ les preimatges per les corresponents aplicacions.

Així doncs, hem expressat $H \cap F_n$ com a preimatge completa per un epimorfisme d'un subgrup que sabem calcular, i sobre el que és rutinari decidir si és d'índex finit. Ara el lema 2.1.(b) ens permet traslladar el resultat a $H \cap F_n$ i, usant el corol.lari 2.4, concloure.

Proposició 2.6. *Si $H$ és un subgrup de $G = F_n \times \mathbb{Z}^m$ donat per una família finita de generadors, aleshores podem decidir algorísmicament si $H$ té índex finit a $G$ i, en cas afirmatiu, calcular l'índex i un sistema de representants de les classes laterals de $G$ mòdul $H$.*

Demostració. Del corol.lari 2.4 sabem que $H$ té índex finit a $G$ si i només si són finits els índexs $[F_n : H \cap F_n]$ i $[\mathbb{Z}^m : L]$, on $L = H \cap \mathbb{Z}^m$. Ara bé, d'acord amb el que hem vist, tenim

$$(L)\mathbf{A}^{-1}\rho^{-1} \cong H \cap F_n \leqslant H\pi \leqslant F_n \,.$$

És ben conegut que en aquestes circumstàncies

$$[F_n : H \cap F_n] = [F_n : H\pi] \cdot [H\pi : H \cap F_n] \,,$$

per tant, $H \cap F_n$ té índex finit a $F_n$ si i només si els dos índexs de la dreta són finits. La finitud del primer d'ells és decidible sense més que comprovar si el *folded graph* de Stallings obtingut a partir de les imatges per $\pi$ dels generadors de $H$ és complet. Per decidir sobre la finitud de $[H\pi : H \cap F_n]$ observem que, en ser $H \cap F_n \cong (L)\mathbf{A}^{-1}\rho^{-1}$ amb $\rho$ epimorfisme, del lema 2.1.(b) es dedueix que aquesta és equivalent a la de $[\mathbb{Z}^{n'} : (L)\mathbf{A}^{-1}]$.

En definitiva, la finitud de l'índex de $H$ a $G$ ha quedat reduïda a la finitud de l'índex $[F_n : H\pi]$ (decidible a partir del *folded graph* de Stallings) juntament a la dels índexs de dos subgrups calculables ($[\mathbb{Z}^m : L]$ i $[\mathbb{Z}^{n'} : (L)\mathbf{A}^{-1}]$) de respectius grups lliure-abelians. Evidentment els dos darrers índexs seran finits si i només si els corresponents subgrups són de rang màxim i aquesta condició és òbviament decidible.

Vegem ara que, en el cas de ser $H$ d'índex finit a $G$, podem calcular una família de representants de les classes laterals i, per tant, l'índex. Observem en primer lloc que els plantejaments usats anteriorment per establir la finitud dels índexs $[F_n : H\pi]$, $[\mathbb{Z}^{n'} : (L)\mathbf{A}^{-1}]$ i $[\mathbb{Z}^m : L]$ proporcionen també formes algorísmiques de determinar famílies de representants de les respectives classes laterals. En el primer cas, sabem que les classes laterals per la dreta es corresponen biunívocament amb els vèrtexs (que seran complets) del *folded graph* de Stallings de $H\pi$, evidentment calculable. Les classes laterals mòdul subgrups de grups lliure-abelians finitament generats, són fàcilment calculables a partir de bases respectives (per una descripció detallada del procediment, veure la demostració de la proposició 3.7).

Ara, si $H\pi \backslash F_n = \{(H\pi)\, u_i\}_i$ i $(H \cap F_n)\backslash H\pi = \{(H \cap F_n)\, v_j\}_j$, aleshores $(H \cap F_n)\backslash F_n = \{(H \cap F_n)\, v_j\, u_i\}_{i,j}$ és una família de representants de les classes laterals per la dreta de $F_n$ mòdul $H \cap F_n$. Amb aquesta i la que tenim per $\mathbb{Z}^m/L$, només hem d'usar l'aplicació (21) i, usant el *membership problem* a $H$, descartar repeticions per obtenir una família de representants de les classes laterals de $G$ mòdul $H$. Evidentment el seu cardinal serà l'índex de $H$ a $G$. $\square$

Observació 10. Per a $H \leqslant_{f.i.} G = F_n \times \mathbb{Z}^m$ cal descartar qualsevol igualtat tipus *fórmula de Schreier* que expressi l'índex en funció dels rangs escindits de $H$ i $G$. És suficient considerar a $G = F_2 \times \mathbb{Z} = \langle a, b \mid \rangle \times \langle t \mid \rangle$ els subgrups $H = \langle a, b, t^2 \rangle$ i $K = \langle a, b^2, bab, t \rangle$, ambdós d'índex 2 a $G$, però amb $\operatorname{rang}(H) = (2,1) \neq (3,1) = \operatorname{rang}(K)$.

## 3. Interseccions i la propietat de Howson

Diem que un grup té la *propietat de Howson* quan la intersecció de tot parell de subgrups finitament generats és, de nou, finitament generada.

La propietat de Howson és trivial per a $\mathbb{Z}^m$, on tots els subgrups són lliures abelians de rang menor o igual que $m$ i per tant finitament generats. Per a $F_n$, va ser establerta inicialment pel propi Howson [**8**] el 1954 i pot deduir-se també, directament de la finitud de l'ordre del graf del *pull-back* de dos subgrups finitament generats qualssevol.

Baumslag, a [**2**], va establir el 1966 com a generalització del resultat de Howson la conservació de la susdita propietat sota productes lliures. L'existència de subgrups finitament generats de $F_n \times \mathbb{Z}^m$ entrellaçats per una part lliure que abelianitza a zero ens permet construir un contraexemple per a la conservació sota productes directes (i en particular, els que estem considerant) de la propietat de Howson.

Proposició 3.1. *$F_n \times \mathbb{Z}^m$ $(n \geq 2, m \geq 1)$ no compleix la propietat de Howson.*

Demostració. Donem a continuació un contraexemple.

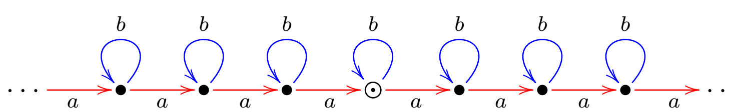
Exemple 5. Considerem a $F_2 \times \mathbb{Z} = \langle a, b \mid \, \rangle \times \langle t \mid \, \rangle$ els subgrups

$$H = \langle ta, b \rangle = \{t^r w \mid w \in F_2 \text{ i } r = |w|_a\}, \text{ i}$$
$$K = \langle t^{-1}a, b \rangle = \{t^r w \mid w \in F_2 \text{ i } r = -|w|_a\}.$$

Tenim que

$$\begin{aligned} H \cap K &= \{t^r w \mid w \in F_2 \text{ i } r = |w|_a = -|w|_a\} \\ &= \{t^0 w \mid w \in F_2 \text{ i } |w|_a = 0\} \\ &= \langle \{a^{-k} b a^k \mid k \in \mathbb{Z}\} \rangle \,. \end{aligned}$$

És fàcil veure usant *Stallings foldings* que el darrer conjunt de generadors (infinit) constitueix una base i és, per tant, mínim. En efecte, el *folded graph* de Stallings de $H \cap K$ és




i l'arbre maximal format per les arestes etiquetades amb $a$ determina la base infinita $\{a^{-k} b a^k \mid k \in \mathbb{N}\}$ de $H \cap K$. Així doncs, hem obtingut un subgrup no finitament generat com a intersecció de dos subgrups $H$ i $K$ finitament generats i, en conseqüència, $F_2 \times \mathbb{Z}$ no compleix la propietat de Howson. L'exemple donat és, a més, en certa manera minimal, ja que utilitza una única lletra abeliana i tant $H$ com $K$ són de rang 2.

En ser-ne $F_2 \times \mathbb{Z}$ subgrup, és evident que el mateix contraexemple és aplicable a tots els grups de la forma $F_n \times \mathbb{Z}^m$ amb $n \geq 2$ i $m \geq 1$, que tampoc compliran, per tant, la propietat de Howson. □

Observació 11. Tant els dos subgrups donats al darrer exemple com la seva intersecció són, en realitat, lliures. Així, curiosament, l'anterior és un cas de subgrups lliures finitament generats amb intersecció lliure no finitament generada. Evidentment això no constitueix cap contraexemple del resultat original de Howson, sinó que, més aviat al contrari, ens indica que no és possible submergir aquests dos subgrups en un ambient lliure comú. Per una descripció completa d'aquesta situació i la seva aplicació a l'exemple considerat, veure el corol.lari 3.6 i l'observació posterior.

Acabem de constatar que un parell de subgrups finitament generats de $F_n \times \mathbb{Z}^m$ no sempre tindran intersecció finitament generada. Resulta natural, per tant, tractar de decidir algorísmicament, donats dos d'aquests subgrups (mitjançant generadors), si la seva intersecció és o no finitament generada i, en cas afirmatiu, determinar-ne algorísmicament una base. Això és el que ens proposem a continuació.

Tal i com hem vist a la secció 4, podem suposar que els subgrups finitament generats de partida, venen ja donats en termes d'una base. Siguin doncs

$$E_1 = \{\mathbf{t}^{\mathbf{a_1}} u_1, \ldots, \mathbf{t}^{\mathbf{a_{n_1}}} u_{n_1}, \mathbf{t}^{\mathbf{b_1}}, \ldots, \mathbf{t}^{\mathbf{b_{m_1}}}\} \text{ base de } H_1 \leqslant F_n \times \mathbb{Z}^m \text{ i}$$
$$E_2 = \{\mathbf{t}^{\mathbf{a}'_1} u'_1, \ldots, \mathbf{t}^{\mathbf{a}'_{n_2}} u'_{n_2}, \mathbf{t}^{\mathbf{b}'_1}, \ldots, \mathbf{t}^{\mathbf{b}'_{m_2}}\} \text{ base de } H_2 \leqslant F_n \times \mathbb{Z}^m \ ;$$

tenim que

$$\{u_1, \ldots, u_{n_1}\} \text{ és base de } H_1\pi \leqslant F_n\,, \quad \{\mathbf{t}^{\mathbf{b_1}}, \ldots, \mathbf{t}^{\mathbf{b_{m_1}}}\} \text{ és base de } H_1 \cap \mathbb{Z}^m,$$
$$\{u'_1, \ldots, u'_{n_2}\} \text{ és base de } H_2\pi \leqslant F_n \text{ i} \quad \{\mathbf{t}^{\mathbf{b}'_1}, \ldots, \mathbf{t}^{\mathbf{b}'_{m_2}}\} \text{ és base de } H_2 \cap \mathbb{Z}^m.$$

Per brevetat, escriurem

$$L_1 = \langle \mathbf{b_1}, \ldots, \mathbf{b_{m_1}} \rangle \text{ subgrup de rang } m_1 \text{ de } \mathbb{Z}^m \ ,$$
$$L_2 = \langle \mathbf{b}'_1, \ldots, \mathbf{b}'_{m_2} \rangle \text{ subgrup de rang } m_2 \text{ de } \mathbb{Z}^m$$

i també

$$\mathbf{A_1} = \begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_{n_1}} \end{pmatrix} \in \mathcal{M}_{n_1 \times m}(\mathbb{Z}) \quad \text{ i } \quad \mathbf{A_2} = \begin{pmatrix} \mathbf{a}'_1 \\ \vdots \\ \mathbf{a}'_{n_2} \end{pmatrix} \in \mathcal{M}_{n_2 \times m}(\mathbb{Z}) \ .$$

Recordem (lema 4.3) que podem recuperar $H_1$ a partir de la base $E_1 = \{\mathbf{t}^{\mathbf{a_1}} u_1, \ldots, \mathbf{t}^{\mathbf{a_{n_1}}} u_{n_1}, \mathbf{t}^{\mathbf{b_1}}, \ldots, \mathbf{t}^{\mathbf{b_{m_1}}}\}$ considerant els elements $\mathbf{t}^{\mathbf{a}} w \in G$, amb $w$ recorrent el subgrup $H_1\pi$ generat pels $u_i$ (projeccions a la part lliure dels elements de la base), i amb $\mathbf{a}$ satisfent una certa relació lineal que, per una banda fa un recompte absolut de l'aparició de cadascuna de les $u_i$ a $w$, i les hi assigna tantes $\mathbf{t}$'s com estipula el corresponent exponent $\mathbf{a_i}$, i per altra admet totes les $\mathbf{t}$'s que provinguin de la part abeliana de la base

$$H_1 = \{\, \mathbf{t}^{\mathbf{a}}\, \omega(u_1, \ldots, u_{n_1}) \mid \omega \in F_{n_1} \ , \ \mathbf{a} \in \boldsymbol{\omega} \mathbf{A_1} + L_1 \,\} \ .$$

És a dir, $H_1$ està descrit per les paraules $w$ en $\{u_1, \ldots, u_{n_1}\}$ acompanyades de les seves respectives complecions abelianes a $H_1$, $\mathfrak{c}_{w,H_1}$.

Raonant idènticament per $H_2$, és ja evident que la intersecció $H_1 \cap H_2$ vindrà donada per les paraules de $G$ amb part lliure $w$ pertanyent a la intersecció

$H_1\pi \cap H_2\pi$ tals que les respectives complecions $\mathfrak{c}_{w,H_1}$ i $\mathfrak{c}_{w,H_2}$ siguin compatibles (no disjuntes), completades per qualsevol element d'aquesta intersecció. Serà, no obstant, només la projecció a la part lliure, $(H_1 \cap H_2)\pi$, la que determinarà el caràcter finitament generat de la intersecció $H_1 \cap H_2$. Aquest és, de fet, el cas per a qualsevol subgrup de $F_n \times \mathbb{Z}^m$ tal i com mostra el corol.lari 2.3.

Així, el nostre primer objectiu passa per entendre quan $(H_1 \cap H_2)\pi$ és finitament generat, i la descripció anterior suggereix fer-ho a través de l'estudi de la inclusió $(H_1 \cap H_2)\pi \leqslant H_1\pi \cap H_2\pi$, ja que per a aquest darrer subgrup disposem d'una prou precisa descripció algorísmica. Concretament, donat que $H_1\pi = \langle u_1, \ldots, u_{n_1} \rangle$ i $H_2\pi = \langle u'_1, \ldots, u'_{n_2} \rangle$ són subgrups finitament generats de $F_n$, podem usar la tècnica del *pull-back* de grafs de Stallings per a obtenir algorísmicament una base (que serà finita) $\{v_1, \ldots, v_{n_3}\}$ de $H_1\pi \cap H_2\pi$ amb els seus elements expressables en termes tant de la base de $H_1\pi$ com de la base de $H_2\pi$. Així, tota paraula $\omega$ en $\{v_1, \ldots, v_{n_3}\}$ podrà ser reescrita de forma única tant en termes de $\{u_1, \ldots, u_{n_1}\}$ com en termes de $\{u'_1, \ldots, u'_{n_2}\}$. Concretament si és

$v_k = \nu_k(u_1, \ldots, u_{n_1})$ amb $\nu_k \in F_{n_1}$ grup lliure abstracte de rang $n_1$, i
$v_k = \nu'_k(u'_1, \ldots, u'_{n_2})$ amb $\nu'_k \in F_{n_2}$ grup lliure abstracte de rang $n_2$,

per a tot $k = 1, \ldots, n_3$, anomenarem $\mu_1$ i $\mu_2$ als morfismes formals definits de $F_{n_3} = \langle s_1, \ldots, s_{n_3} \mid \rangle$ a $F_{n_1} = \langle y_1, \ldots, y_{n_1} \mid \rangle$ i a $F_{n_2} = \langle z_1, \ldots, z_{n_2} \mid \rangle$ respectivament, donats per

$$\begin{array}{ccccc} F_{n_1} & \xleftarrow{\mu_1} & F_{n_3} & \xrightarrow{\mu_2} & F_{n_2} \\ \nu_k(y_1, \ldots, y_{n_1}) & \longleftarrow & s_k & \longmapsto & \nu'_k(z_1, \ldots, z_{n_2}) \end{array} ,$$

on $k = 1, \ldots, n_3$. Amb les notacions introduïdes, tindrem que una paraula $\omega(\vec{v})$ en les $\{v_1, \ldots, v_{n_3}\}$, un cop substituïdes les $v_k$ per les corresponents $\nu_k(\vec{u})$, pren la forma $\omega(\vec{\nu}(\vec{u}))$; aquesta serà una paraula en les $\{u_1, \ldots, u_{n_1}\}$ que anomenarem $\omega_1(\vec{u})$. Procedint de forma anàloga amb l'altra substitució obtenim que, en resum, com a elements de $G$

$$\omega(\vec{v}) = \omega(\vec{\nu}(\vec{u})) =: \omega_1(\vec{u}) \quad \text{i} \quad \omega(\vec{v}) = \omega(\vec{\nu}'(\vec{u}')) =: \omega_2(\vec{u}') \ .$$

Aquest llenguatge permet ja precisar la descripció anterior dels elements pertanyents a la intersecció de dos subgrups finitament generats en termes de les respectives bases.

Proposició 3.2. *El subgrup $H_1 \cap H_2$ està constituït pels elements de $G$ amb part lliure pertanyent a $H_1\pi \cap H_2\pi$, i per tant expressable com a paraula de la forma $\omega_1(\vec{u}) = \omega_2(\vec{u}')$, tal que*

$$(\boldsymbol{\omega_1}\mathbf{A_1} + L_1) \cap (\boldsymbol{\omega_2}\mathbf{A_2} + L_2) \neq \varnothing, \tag{24}$$

*completada abelianament pels membres d'aquesta mateixa intersecció; és a dir*

$$H_1 \cap H_2 = \left\{ \mathbf{t}^{\mathbf{a}}\, w \in G \;\middle|\; \begin{array}{l} w = \omega_1(\vec{u}) = \omega_2(\vec{u}') \in H_1\pi \cap H_2\pi \\ \mathbf{a} \in (\boldsymbol{\omega_1}\mathbf{A_1} + L_1) \cap (\boldsymbol{\omega_2}\mathbf{A_2} + L_2) \end{array} \right\} ,$$

*on $\omega_1(\vec{u})$ i $\omega_2(\vec{u}')$ són les expressions dels elements $w \in H_1\pi \cap H_2\pi$ com a paraules en termes de les bases $\{u_1, \ldots, u_{n_1}\}$ de $H_1\pi$ i $\{u'_1, \ldots, u'_{n_2}\}$ de $H_2\pi$ respectivament, i $\boldsymbol{\omega_1} \in \mathbb{Z}^{n_1}$ i $\boldsymbol{\omega_2} \in \mathbb{Z}^{n_2}$ denoten les abelianitzacions de $\omega_1 \in F_{n_1}$ i $\omega_2 \in F_{n_2}$.*

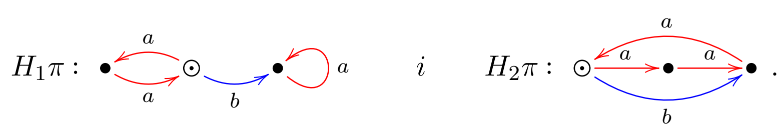
Demostració. Es tracta només d'aplicar el lema 4.3 considerant les descripcions en termes de les noves bases. □

Observació 12. La construcció del *pull-back* mostra clarament (i de forma algorísmica) el caràcter finitament generat de $H_1\pi \cap H_2\pi$, de manera que si la condició lineal (24) fos supèrflua i $(H_1 \cap H_2)\pi$ recobrís en realitat tota la intersecció, hauríem acabat. Veurem però, mitjançant un exemple, que la inclusió $(H_1 \cap H_2)\pi \leqslant H_1\pi \cap H_2\pi = \langle v_1, \ldots, v_{n_3} \rangle$ pot ser estricta. Això, donat que $F_n$ té subgrups no finitament generats, obre la possibilitat de que $(H_1 \cap H_2)\pi$ (i per tant $H_1 \cap H_2$) tampoc ho siguin.

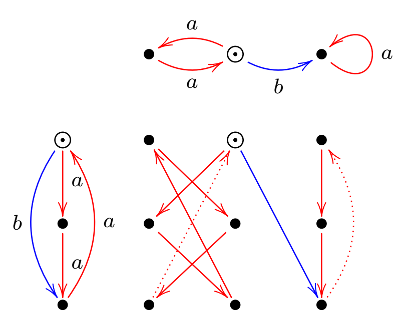
Exemple 6. Considerem a $F_2 \times \mathbb{Z} = \langle a, b \mid \rangle \times \langle t \mid \rangle$ els subgrups $H_1 = \langle ta^2, bab^{-1}, t^2 \rangle$ i $H_2 = \langle t^2a^3, ba, t^2 \rangle$, aleshores tenim que

$$\begin{array}{lcl} H_1\pi = \langle a^2, bab^{-1} \rangle & , & L_1 = 2\mathbb{Z} \ , \\ H_2\pi = \langle a^3, ba \rangle & \text{i} & L_2 = 2\mathbb{Z} \ . \end{array}$$

Ara, el *pull-back* dels *folded graphs* de Stallings corresponents als subgrups $H_1\pi$ i $H_2\pi$ proporciona la base $\{a^6, ba^3b^{-1}\}$ de la seva intersecció. En efecte, tenim




I el *pull-back*




és un *folded graph* connex sense vèrtexs de valència 1, i per tant, el *folded graph* de Stallings de $H_1\pi \cap H_2\pi$. Prenent ara l'arbre maximal obtingut eliminant del *pull-back* les arestes representades amb línia discontínua és ja evident la base esmentada.

És a dir, tenim

$$(H_1 \cap H_2)\pi \leqslant H_1\pi \cap H_2\pi = \langle a^6, ba^3b^{-1} \rangle \ .$$

Veurem a continuació que $a^6 \notin (H_1 \cap H_2)\pi$ i per tant la inclusió és estricta. En efecte $a^6 \in (H_1 \cap H_2)\pi$ si i només si existeix un $p \in \mathbb{Z}$ tal que $t^p a^6 \in H_1 \cap H_2$, això és, si les complecions abelianes de $a^6$ a $H_1$ i $H_2$ tenen algun element comú.

Ara, com que $\{a^2, bab^{-1}\}$ és base de $H_1\pi$, és clar que a $H_1$ una paraula amb part lliure $a^6$ expressada en termes dels generadors donats: no admet la participació no trivial del generador $bab^{-1}$, involucra exactament tres aparicions (netes) del generador $a^2$ i admet qualsevol nombre d'aparicions del generador $t^2$ ja que aquest només afecta a la part abeliana.

Així doncs, la compleció abeliana de $a^6$ a $H_1$ aglutina les tres $t$'s provinents de les corresponents aparicions netes de $ta^2$ i el nombre indeterminat de parells de $t$'s provinents de les aparicions de $t^2$, en resum, $\mathfrak{c}_{a^6,H_1} = \{p \in \mathbb{Z} \mid t^p a^6 \in H_1\} = 3 + 2\mathbb{Z} = 1 + 2\mathbb{Z}$, és a dir, $a^6$ només pot aparèixer a $H_1$ completada per un (de fet qualsevol) sencer senar. Arguments pràcticament idèntics sobre els generadors de $H_2$ condueixen a la següent compleció abeliana de $a^6$ a $H_2$, $\mathfrak{c}_{a^6,H_2} = \{p \in \mathbb{Z} \mid t^p a^6 \in H_2\} = 4 + 2\mathbb{Z} = 2\mathbb{Z}$, això és, $a^6$ només pot aparèixer a $H_2$ completada per un (de fet qualsevol) sencer parell. En definitiva, no serà possible completar $a^6$ de manera que es satisfacin les dues pertinences, per tant $a^6 \notin (H_1 \cap H_2)\pi$ i la inclusió $(H_1 \cap H_2)\pi \leqslant H_1\pi \cap H_2\pi$ és estricta, tal i com volíem veure.

Per tant, el nostre coneixement de $H_1\pi \cap H_2\pi$ no conclou i haurem de recórrer a la descripció explícita de $(H_1 \cap H_2)\pi$ donada per la proposició 3.2 per tractar d'identificar sota quines condicions és finitament generada.

El següent diagrama permet una visualització bastant aclaridora de la situació,

$$
\begin{tikzcd}
 & (H_1 \cap H_2)\pi \arrow[d, phantom, "\rotatebox{90}{$\leqslant$}"] & \\
H_1\pi \arrow[d, phantom, "\rotatebox{90}{$\cong$}"] & H_1\pi \cap H_2\pi \arrow[d, phantom, "\rotatebox{90}{$\cong$}"] & H_2\pi \arrow[d, phantom, "\rotatebox{90}{$\cong$}"] \\
F_{n_1} \arrow[d, two heads, "\rho_1"'] \arrow[dr, phantom, "///"] & F_{n_3} \arrow[l, "\mu_1"'] \arrow[r, "\mu_2"] \arrow[d, two heads, "\rho_3"'] \arrow[dr, phantom, "///"] & F_{n_2} \arrow[d, two heads, "\rho_2"'] \\
\mathbb{Z}^{n_1} \arrow[dr, "\mathbf{A_1}"'] & \mathbb{Z}^{n_3} \arrow[l, dotted, "\mathbf{M_1}"'] \arrow[r, dotted, "\mathbf{M_2}"] & \mathbb{Z}^{n_2} \arrow[dl, "\mathbf{A_2}"] \\
 & \mathbb{Z}^m &
\end{tikzcd}
\tag{25}
$$

on hem designat:

- $\rho_i$ les abelianitzacions $F_{n_i} \to \mathbb{Z}^{n_i}$ $(i = 1, 2, 3)$,
- $\mathbf{M_i}\colon \mathbb{Z}^{n_3} \to \mathbb{Z}^{n_i}$ l'abelianització del morfisme $\mu_i$ $(i = 1, 2)$ que pensarem com a producte per l'esquerra de la matriu corresponent, $\mathbf{v} \mapsto \mathbf{vM_i}$, i
- $\mathbf{A_i}\colon \mathbb{Z}^{n_i} \to \mathbb{Z}^m$ el morfisme $\mathbf{v} \mapsto \mathbf{vA_i}$ corresponent a multiplicar per l'esquerra de la matriu homònima $(i = 1, 2)$.

Si interpretem la proposició 3.2 en termes d'aquest diagrama, en particular, obtenim el següent lema.

Lema 3.3. *$(H_1 \cap H_2)\pi$ està descrit per les paraules $\omega(\vec{v}) \in H_1\pi \cap H_2\pi$ tals que*

$$(24') \qquad (\omega\mu_1\rho_1\mathbf{A_1} + L_1) \cap (\omega\mu_2\rho_2\mathbf{A_2} + L_2) \neq \varnothing\ . \quad \square$$

Utilitzant ara el camí alternatiu donat per les línies discontinues a (25) podem traslladar el problema essencialment a l'àmbit abelià. Anomenant $\mathbf{R_1} = \mathbf{M_1A_1}$ i $\mathbf{R_2} = \mathbf{M_2A_2}$ (calculables a partir de les dades de que disposem) obtenim

$$\begin{tikzcd}
(H_1 \cap H_2)\pi \\
H_1\pi \cap H_2\pi \arrow[u, phantom, "\geqslant" rotate=90] \\
F_{n_3} \arrow[u, phantom, "\cong" rotate=90] \arrow[d, "\rho_3"'] \\
\mathbb{Z}^{n_3} \arrow[d, bend right, "\mathbf{R_1}"'] \arrow[d, bend left, "\mathbf{R_2}"] \\
\mathbb{Z}^m.
\end{tikzcd}$$

Aleshores, la condició (24') queda

$$(24'') \qquad (\omega\rho_3\mathbf{R_1} + L_1) \cap (\omega\rho_3\mathbf{R_2} + L_2) \neq \varnothing\ ,$$

i hem reduït la intersecció $(H_1 \cap H_2)\pi$ buscada a la preimatge per $\rho_3$ del conjunt de solucions d'un problema abelià (i algorísmic).

Proposició 3.4. *Amb les notacions usades,*

$$(26) \qquad (H_1 \cap H_2)\pi = \{\omega(\vec{v}) \in H_1\pi \cap H_2\pi \mid \omega \in M\rho_3^{-1}\} \cong M\rho_3^{-1} \leqslant F_{n_3}\ ,$$

*on $M = \{\, \mathbf{c} \in \mathbb{Z}^{n_3} \mid\ (\mathbf{cR_1} + L_1) \cap (\mathbf{cR_2} + L_2) \neq \varnothing \,\}$ és un subgrup de $\mathbb{Z}^{n_3}$ del que podem calcular efectivament una base. Concretament $M$ és el conjunt de preimatges per $\mathbf{R_1} - \mathbf{R_2}$ del subgrup $L_1 + L_2 \leqslant \mathbb{Z}^m$, és a dir*

$$M = (L_1 + L_2)(\mathbf{R_1} - \mathbf{R_2})^{-1} \leqslant \mathbb{Z}^{n_3}\ .$$

Demostració. La igualtat (26) no és més que l'establerta al lema 3.3 amb la condició equivalent (24''). És obvi que $M \subseteq \mathbb{Z}^{n_3}$; amb més precisió $\mathbf{c} \in M$

si i només si $\mathbf{c}\mathbf{R_1}+\mathbf{l_1}=\mathbf{c}\mathbf{R_2}+\mathbf{l_2}$ per a certs $\mathbf{l_1}\in L_1$ i $\mathbf{l_2}\in L_2$, o equivalentment, si $\mathbf{c}(\mathbf{R_1}-\mathbf{R_2})\in L_1+L_2$.

Per tant

$$M=(L_1+L_2)(\mathbf{R_1}-\mathbf{R_2})^{-1}\ .$$

És a dir, obtenim $M$ com a preimatge per una aplicació lineal calculable $(\mathbf{R_1}-\mathbf{R_2})$, de la suma de dos subgrups $L_1$ i $L_2$ que tenim donats en termes de bases respectives. En aquestes condicions és ja evident que $M$ és subgrup de $\mathbb{Z}^{n_3}$ i el càlcul d'una base és un senzill exercici d'àlgebra lineal. □

El següent diagrama resumeix la situació i posa en context el resultat anterior

$$\begin{array}{ccccccc} H_1\pi\cap H_2\pi & \cong & F_{n_3} & \overset{\rho_3}{\twoheadrightarrow} & \mathbb{Z}^{n_3} & \xrightarrow{\mathbf{R_1}-\mathbf{R_2}} & \mathbb{Z}^m \\ \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} \\ (H_1\cap H_2)\pi & \cong & M\rho_3^{-1} & \longleftarrow\!\shortmid & M & \longleftarrow\!\shortmid & L_1+L_2\ . \end{array} \tag{27}$$

Passem a donar el resultat que converteix el nostre problema (la determinació del caràcter finitament generat de la intersecció de dos subgrups finitament generats de $F_n\times\mathbb{Z}^m$) en un de plenament abelià, i resoluble algorísmicament sempre que els subgrups ens hagin estat donats mitjançant una família finita de generadors.

TEOREMA 3.5. *Siguin $H_1$ i $H_2$ subgrups finitament generats de $F_n\times\mathbb{Z}^m$ amb $n_3$ i $M$ com abans. Tenim que*

(a) *$(H_1\cap H_2)\pi$ és trivial si i només si $n_3=0,1$ i $M=0$,*
(b) *si $(H_1\cap H_2)\pi\neq 1$, aleshores la intersecció $H_1\cap H_2$ és finitament generada si i només si $M$ té índex finit a $\mathbb{Z}^{n_3}$.*

DEMOSTRACIÓ. (*a*) Observem en primer lloc que l'abelianització $\rho_3\colon F_{n_3}\to\mathbb{Z}^{n_3}$ és injectiva si i només si $n_3=0$ o 1. Trivialment, per als casos considerats $\rho_3$ ha de ser igual a la corresponent identitat i per tant injectiva, mentre que per $n_3\geq 2$, $\ker(\rho_3)=\langle[F_{n_3},F_{n_3}]\rangle$ ni tan sols té rang finit. Així, si $(H_1\cap H_2)\pi\cong M\rho_3^{-1}=1$, ha de ser, per una banda $\ker(\rho_3)=1$ i per tant $n_3=0$ o 1 (ja que en ser $M$ subgrup de $\mathbb{Z}^{n_3}$, el $\ker(\rho_3)$ ha d'estar inclòs a $M\rho_3^{-1}$); i per altra $M=M\rho_3^{-1}\rho_3=1\rho_3=\mathbf{0}$ (en ser $\rho_3$ exhaustiva). La implicació cap a l'esquerra és evident de la caracterització inicial de la injectivitat de $\rho_3$.

(*b*) Ja sabem que $H_1\cap H_2$ és finitament generat si i només si ho és $(H_1\cap H_2)\pi\cong M\rho_3^{-1}$. Suposem que $M\rho_3^{-1}\neq 1$; donat que $M$ és subgrup de $\mathbb{Z}^{n_3}$ (abelià), és normal, i per tant també serà normal a $F_{n_3}$, la seva preimatge (que estem suposant no trivial) pel morfisme $\rho_3$; és a dir tindrem $1\neq M\rho_3^{-1}\trianglelefteq F_{n_3}$. Ara bé, és ben sabut (veure per exemple [**11**], pàgs. 16-18) que tot subgrup normal no trivial d'un grup lliure de rang finit és finitament generat si i només si és d'índex finit. Per tant, quan $M\rho_3^{-1} \neq 1$, $H_1 \cap H_2$ serà finitament generat si i només si $M\rho_3^{-1}$ té índex finit a $F_{n_3}$. I, com que $\rho_3 \colon F_{n_3} \to \mathbb{Z}^{n_3}$ és exhaustiu, el segon apartat del lema 2.1 conclou la demostració. En efecte, d'acord amb el lema, $M\rho_3^{-1}$ té índex finit a $F_{n_3}$ si i només si $M$ té índex finit a $\mathbb{Z}^{n_3}$. □

Remarquem que les condicions del teorema són expressables abelianament (a partir de $M$) i calculables si disposem de generadors per $H_1$ i $H_2$.

Restringint la nostra atenció només als subgrups lliures de rang finit podem donar una versió més senzilla del teorema 3.5.

COROL.LARI 3.6. *Siguin $H_1$ i $H_2$ subgrups lliures no abelians de rang finit de $F_n \times \mathbb{Z}^m$, aleshores la seva intersecció és finitament generada si i només si té projecció trivial a la part lliure o $\mathbf{R_1} = \mathbf{R_2}$.*

DEMOSTRACIÓ. En les condicions de l'enunciat existiran bases de $H_1$ i $H_2$ amb les corresponents $L_1$ i $L_2$ satisfent $L_1 = L_2 = 0$. Aleshores $M = (L_1 + L_2)(\mathbf{R_1} - \mathbf{R_2})^{-1} = \{0\}(\mathbf{R_1} - \mathbf{R_2})^{-1} = \ker(\mathbf{R_1} - \mathbf{R_2})$ té índex finit a $\mathbb{Z}^{n_3}$ si i només si $\ker(\mathbf{R_1} - \mathbf{R_2})$ té rang màxim, és a dir si $\mathbf{R_1} - \mathbf{R_2} = \mathbf{0}$, i el teorema 3.5 pren, en aquest cas, la forma donada. □

Podem ara revisar alguns resultats coneguts amb les noves eines.

OBSERVACIÓ 13. Recuperem en primer lloc l'exemple 5 (en què la intersecció de dos subgrups lliures de rang 2 de $F_2 \times \mathbb{Z}$ era no finitament generada) per analitzar-lo sota la llum del corol.lari anterior. Teníem a $F_2 \times \mathbb{Z} = \langle a, b \mid \ \rangle \times \langle t \mid \ \rangle$ els subgrups $H$ amb base $\{ta, b\}$ i $K$ amb base $\{t^{-1}a, b\}$. Aleshores és clar que $\mathbf{A_1} = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ i $\mathbf{A_2} = \left(\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right)$, mentre que $H\pi = K\pi = H\pi \cap K\pi = F_2$ i podem prendre $\{a, b\}$ com a base de tots ells (en particular $n_3 = 2$ i per tant $(H_1 \cap H_2)\pi \neq 1$). En aquestes circumstàncies $\mu_1 = \mu_2 = \mathrm{id}_{F_2}$, $\mathbf{M_1} = \mathbf{M_2} = \mathbf{I_2}$ i per tant $\mathbf{R_1} = \mathbf{I_2}\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right) = \mathbf{I_2}\left(\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right) = \mathbf{R_2}$. Obtenim, doncs, del corol.lari anterior, que la intersecció $H_1 \cap H_2$ no és finitament generada tal i com ja havíem vist calculant-la explícitament.

De forma similar, si considerem $H_1$ i $H_2$ subgrups finitament generats de $F_n \leqslant F_n \times \mathbb{Z}^m$ serà $\mathbf{A_1} = \mathbf{0}$ i $\mathbf{A_2} = \mathbf{0}$ (no necessàriament de les mateixes dimensions). Per tant, independentment de l'expressió de $\mu_1$ i $\mu_2$, tindrem $\mathbf{R_1} = \mathbf{0} = \mathbf{R_2}$ i el corol.lari no fa més que corroborar la propietat de Howson per als grups lliures finitament generats.

Obtenim finalment, com a conseqüència del teorema 3.5, la solució als problemes algorísmics proposats al principi de la secció.

PROPOSICIÓ 3.7. *Si $H_1$ i $H_2$ són subgrups de $F_n \times \mathbb{Z}^m$ donats per dues famílies finites de generadors, aleshores podem decidir algorísmicament si la* *intersecció $H_1 \cap H_2$ és finitament generada i, en cas afirmatiu, calcular-ne una base.*

Demostració. Per la proposició 4.2 podem suposar $H_1$ i $H_2$ donats per bases respectives. Aleshores, podem calcular algorísmicament $n_3$ (és el cardinal de la base de $H_1\pi \cap H_2\pi$ obtinguda per *pull-back*) i una base del subgrup $M \leqslant \mathbb{Z}^m$ associat a les bases de partida (proposició 3.4).

Amb aquesta informació juntament amb el teorema 3.5(a) podrem decidir algorísmicament si $(H_1 \cap H_2)\pi = 1$. Si és aquest el cas conclourem que $H_1 \cap H_2$ és finitament generat i haurem conclòs el problema de decisió. Si no, segons el teorema 3.5, per decidir només haurem de determinar (algorísmicament) la finitud o no de $[M : \mathbb{Z}^{n_3}]$. Però l'índex d'un subgrup $M$ a $\mathbb{Z}^{n_3}$ és finit si i només si el rang de $M$ és $n_3$. Així doncs, serà suficient amb comprovar si la base de $M$ (obtinguda algorísmicament) té cardinal $n_3$. En cas afirmatiu la intersecció $H_1 \cap H_2$ serà finitament generada i no ho serà en cas contrari.

Descrivim a continuació un procediment per calcular una base de la intersecció $H_1 \cap H_2$ quan és finitament generada. Observem en primer lloc que del corol.lari 2.2 i la proposició 4.1

$$H_1 \cap H_2 = (H_1 \cap H_2)\pi\alpha \times (H_1 \cap H_2 \cap \mathbb{Z}^m) ,$$

i obtindrem una base de $H_1 \cap H_2$ reunint una base de cada factor. Pel que fa al factor de la part abeliana, $H_1 \cap H_2 \cap \mathbb{Z}^m = (H_1 \cap \mathbb{Z}^m) \cap (H_2 \cap \mathbb{Z}^m)$ i serà suficient calcular una base de la intersecció de dos subgrups, $L_1 = H_1 \cap \mathbb{Z}^m$ i $L_2 = H_2 \cap \mathbb{Z}^m$, de $\mathbb{Z}^m$ que tenim, per hipòtesi, donats mitjançant bases. Aquest és un procediment estàndard (i evidentment algorísmic) en àlgebra lineal.

Ara, si $(H_1 \cap H_2)\pi = 1$ (un dels supòsits en què $H_1 \cap H_2$ és finitament generada) l'anterior és tot, i la base obtinguda és base de $H_1 \cap H_2$. En cas de ser $(H_1 \cap H_2)\pi$ (o equivalentment $M\rho_3^{-1}$) no trivial i finitament generat, haurem de completar la base abeliana anterior amb una base de $(H_1 \cap H_2)\pi\alpha$ que (observació 3) podrem obtenir sempre de forma algorísmica a partir d'una base de $(H_1 \cap H_2)\pi \cong M\rho_3^{-1}$. Aquest últim serà doncs el nostre objectiu.

En aquest segon cas, sabem que el subgrup $M \leqslant \mathbb{Z}^{n_3}$, del que tenim calculada una base, té rang màxim. Podem per tant suposar que disposem d'una base $\{\mathbf{e_1}, \dots, \mathbf{e_{n_3}}\}$ de $M$ que, per files, determinarà una matriu $\mathbf{E} \in \mathcal{M}_{n_3}(\mathbb{Z})$ amb determinant no nul. Ara, aplicant adequadament transformacions elementals 'fila' a la matriu $\mathbf{E}$ es pot obtenir una matriu $\mathbf{D}$ diagonal

$$\mathbf{D} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_{n_3} \end{pmatrix} = \begin{pmatrix} \mathbf{d_1} \\ \vdots \\ \mathbf{d_{n_3}} \end{pmatrix} , \text{ amb } d_k > 0, \; k = 1, \dots, n_3 ,$$

les files de la qual, $\{\mathbf{d_1}, \ldots, \mathbf{d_{n_3}}\}$, constituiran una nova base de $M$. En aquesta darrera base es veu clarament que el conjunt

$$C = \{(r_1, \ldots, r_{n_3}) \in \mathbb{Z}^{n_3} \mid r_k = 0, \ldots, d_k - 1,\ k = 1, \ldots, n_3\}$$

constitueix un sistema complet de representants de les classes laterals de $\mathbb{Z}^{n_3}$ mòdul $M$ i, en particular, que l'índex de $M$ a $\mathbb{Z}^{n3}$ (finit com ja sabíem) és exactament

$$[\mathbb{Z}^{n3} : M] = \prod_{k=1}^{n_3} d_k = \det(\mathbf{D}) = |\det(\mathbf{E})| \ .$$

Anomenant $d$ al determinant de $\mathbf{D}$, tenim doncs una col.lecció explícita de representants de les classes laterals de $\mathbb{Z}^{n_3}$ mòdul $M$:

$$\mathbb{Z}^{n_3} = \bigsqcup_{\mathbf{c} \in C} M\mathbf{c} = M\mathbf{c_1} \sqcup \cdots \sqcup M\mathbf{c_d} \ .$$

Ara, com que $\rho_3$ és exhaustiva, d'acord amb el lema 2.1(b), podem usar-la per traslladar la partició anterior a $F_{n_3}$. En efecte, serà

$$F_{n_3} = (M\rho_3^{-1})\, z_1 \sqcup \cdots \sqcup (M\rho_3^{-1})\, z_d \qquad (28)$$

per qualsevol $z_l \in F_{n_3}$ que abelianitzi a $\mathbf{c_l}$, $l = 1, \ldots, d$. (Podem prendre, per exemple, com a preabelianitzat de cada $\mathbf{c_l} = (r_1, r_2, \ldots, r_{n_3})$ l'element $s_1^{r_1} s_2^{r_2} \cdots s_3^{r_{n_3}}$ de $F_{n_3} = \langle s_1, \cdots, s_{n_3} \mid \ \rangle$).

La situació actual és la següent: busquem una base per al subgrup $M\rho_3^{-1}$ del qual sabem que és normal a $F_{n_3}$, coneixem el seu índex i disposem d'un conjunt complet de representants de les classes laterals. Ara bé, del que acabem de comentar es dedueix que el graf de Stallings de $M\rho_3^{-1}$ serà transitiu, complet i amb els vèrtexs en bijecció amb les classes laterals. Si aconseguim construir-lo amb la informació de la que disposem, haurem acabat donat que qualsevol arbre maximal proporcionarà una base de $M\rho_3^{-1}$.

Considerem un graf (inicialment sense arcs) amb vèrtexs les classes laterals a (28). Ara, per cada lletra $s_k$ i cada vèrtex $z_l$ afegim un arc amb etiqueta $s_k$ de $(M\rho_3^{-1})\, z_l$ a $(M\rho_3^{-1})\, z_l s_k$ (que haurem d'identificar entre els vèrtexs usant el *membership* a $M\rho_3^{-1}$ sobre cadascun d'ells. Notem que el *membership problem* a $M\rho_3^{-1}$ és decidible sense més que abelianitzar i aplicar el *membersip problem* a $M$). Un cop recorregudes totes les etiquetes possibles sortint de tots els vèrtexs quedarà el graf de Stallings de $M\rho_3^{-1}$ completament dibuixat d'on podrem ja sense dificultat obtenir la base buscada. □

## 4. Punts fixos per un automorfisme

En aquesta secció estudiarem el caràcter finit del subgrup de punts fixos per un automorfisme de $F_n \times \mathbb{Z}^n$. En cas de ser-ho, usarem el resultat homòleg de Maslakova [**12**] a $F_n$, per determinar-ne una base.

Sigui $\Psi$ un automorfisme de $F_n \times \mathbb{Z}^m$ donat mitjançant imatges dels generadors. Sabem (teorema 4.1) que podem identificar $\Psi$ amb una terna $(\phi, \mathbf{Q}, \mathbf{P}) \in \mathrm{Aut}(F_n) \times \mathrm{GL}_m(\mathbb{Z}) \times \mathcal{M}_{n\times m}(\mathbb{Z})$, concretament

$$\mathbf{t}^{\mathbf{a}}\, u \ \overset{\Psi}{\longmapsto}\ \mathbf{t}^{\mathbf{aQ}+\mathbf{uP}} u\phi \ .$$

Aleshores un element $\mathbf{t}^{\mathbf{a}}u$ és fix per $\Psi = (\phi, \mathbf{Q}, \mathbf{P})$ si i només si $\mathbf{t}^{\mathbf{aQ}+\mathbf{uP}} u\phi = \mathbf{t}^{\mathbf{a}}\, u$, condició que separant les parts lliure i abeliana pren la forma

$$\begin{cases} u\phi = u \\ \mathbf{a}(\mathbf{I_m} - \mathbf{Q}) = \mathbf{uP} \ . \end{cases}$$

És a dir,

$$\mathrm{Fix}\,\Psi = \{\mathbf{t}^{\mathbf{a}}u \in F_n \times \mathbb{Z}^m \mid u \in \mathrm{Fix}\,\phi \ \wedge\ \mathbf{a}(\mathbf{I_m} - \mathbf{Q}) = \mathbf{uP}\} \ .$$

Com hem vist al lema 2.3, $\mathrm{Fix}\,\Psi$ serà finitament generat si i només si ho és la seva projecció sobre la part lliure

$$(\mathrm{Fix}\,\Psi)\pi = \mathrm{Fix}\,\phi \cap \{u \in F_n \mid \mathbf{uP} \in \mathrm{im}(\mathbf{I_m} - \mathbf{Q})\} \ .$$

Anomenant $\rho$ a l'abelianització de $F_n$, $\mathbf{I_m} - \mathbf{Q}$ a l'endomorfisme de $\mathbb{Z}^m$ corresponent a multiplicar per l'esquerra de la matriu homònima, i $M$ a la seva imatge, obtenim el següent esquema

$$\begin{tikzcd}
\mathrm{Fix}\,\phi \leqslant F_n \arrow[r, two heads, "\rho"] & \mathbb{Z}^n \arrow[r, "\mathbf{P}"] & \mathbb{Z}^m \arrow[loop above, "\mathbf{I_m}-\mathbf{Q}"] \\
M\mathbf{P}^{-1}\rho^{-1} \arrow[u, phantom, sloped, "\leqslant"] & M\mathbf{P}^{-1} \arrow[u, phantom, sloped, "\leqslant"] \arrow[l, mapsto] & M = \mathrm{im}(\mathbf{I_m} - \mathbf{Q}) \ . \arrow[u, phantom, sloped, "\leqslant"] \arrow[l, mapsto]
\end{tikzcd}$$

Aleshores podem reescriure, més senzillament

$$(\mathrm{Fix}\,\Psi)\pi = \mathrm{Fix}\,\phi \cap M\mathbf{P}^{-1}\rho^{-1} \ .$$

Observem que si aconseguim expressar el conjunt anterior com a preimatge completa (de quelcom calculable) per una abelianització, podrem, tal i com hem fet abans per a la intersecció de subgrups, decidir si $\mathrm{Fix}\,\Psi$ és de tipus finit amb un senzilla comprovació abeliana. Per aconseguir-ho cal restringir adequadament els morfismes involucrats.

LEMA 4.1. *Si $\Psi = (\phi, \mathbf{Q}, \mathbf{P})$ és un automorfisme de $F_n \times \mathbb{Z}^m$, aleshores $(\mathrm{Fix}\,\Psi)\pi$ és calculable com a preimatge completa d'un epimorfisme sobre un grup lliure-abelià, concretament*

$$(\mathrm{Fix}\,\Psi)\pi = N{\mathbf{P_1}}^{-1}\rho_1^{-1} \tag{29}$$

*on $\rho_1$ és la restricció a $\mathrm{Fix}\,\phi$ de l'abelianització ambient $\rho$, $\mathbf{P_1}$ la restricció de $\mathbf{P}$ a $\mathrm{im}\,\rho_1$ i $N = M \cap \mathrm{im}\,\mathbf{P_1}$.*

Demostració. Volem veure que $\mathrm{Fix}\,\phi \cap M\mathbf{P}^{-1}\rho^{-1} = N\mathbf{P_1}^{-1}\rho_1^{-1}$. Clarament, intersecar el domini de $\rho$ amb $\mathrm{Fix}\,\phi$ és prendre la preimatge per la seva restricció $\rho_1$ a $\mathrm{Fix}\,\phi$; i és el mateix prendre-la de tot $M\mathbf{P}^{-1}$ que de la part de $M$ que recorre $\rho_1$, $(M \cap \mathrm{im}\,\mathbf{P_1})\mathbf{P_1}^{-1}$. □

El diagrama següent detalla la situació:

$$\begin{tikzcd}
 & F_n \arrow[r, two heads, "\rho"] & \mathbb{Z}^n \arrow[r, "\mathbf{P}"] & \mathbb{Z}^m \arrow[loop above, "\mathbf{I_m}-\mathbf{Q}"] \geqslant M = \mathrm{im}(\mathbf{I_m}-\mathbf{Q}) \\
 & \mathrm{Fix}\,\phi \arrow[u, phantom, sloped, "\leqslant"] \arrow[r, two heads, "\rho_1"] & \mathrm{im}\,\rho_1 \arrow[u, phantom, sloped, "\trianglelefteqslant"] \arrow[r, two heads, "\mathbf{P_1}"] & \mathrm{im}\,\mathbf{P_1} \arrow[u, phantom, sloped, "\trianglelefteqslant"] \\
(\mathrm{Fix}\,\Psi)\pi = & N\mathbf{P_1}^{-1}\rho_1^{-1} \arrow[u, phantom, sloped, "\trianglelefteqslant"] & N\mathbf{P_1}^{-1} \arrow[u, phantom, sloped, "\trianglelefteqslant"] \arrow[l, mapsto] & N = M \cap \mathrm{im}\,\mathbf{P_1}\ . \arrow[u, phantom, sloped, "\trianglelefteqslant"] \arrow[l, mapsto]
\end{tikzcd}$$

Amb el darrer refinament i el lema que segueix, podrem ja donar el resultat principal de la secció.

Lema 4.2. *Amb les notacions anteriors, $\rho_1$ és injectiva (i, per tant, bijectiva) si i només si* $\mathrm{Fix}\,\phi$ *és cíclic i no abelianitza a zero, o és trivial. A més, podem verificar aquesta injectivitat algorísmicament.*

Demostració. La implicació cap a l'esquerra és evident. Per a l'altra, és clar que ha de ser $\mathrm{rang}(\mathrm{Fix}\,\phi) \leq 1$, ja que si no el commutador seria no trivial. En el cas $\mathrm{Fix}\,\phi = \langle w_1 \rangle$, és necessari imposar (recordem que $\rho_1$ és restricció de l'abelianització ambient) que $w_1$ no abelianitzi a zero. Notem que podem verificar algorísmicament si $\rho_1$ és injectiva usant l'equivalència anterior sobre una base obtinguda mitjançant l'algorisme que proporciona Maslakova a [**12**]. □

Proposició 4.3. *Si $\Psi$ és un automorfisme de $F_n \times \mathbb{Z}^m$, aleshores podem decidir algorísmicament si el subgrup* $\mathrm{Fix}\,\Psi$ *és finitament generat i, en cas afirmatiu, calcular-ne una base.*

Demostració. D'acord amb el lema 2.3, es tracta de decidir sobre el caràcter finitament generat de $(\mathrm{Fix}\,\Psi)\pi$ que, com acabem de veure, és igual a $N\mathbf{P_1}^{-1}\rho_1^{-1}$.

Observem ara que podem decidir algorísmicament si $N\mathbf{P_1}^{-1}\rho_1^{-1} = 1$, ja que ho és si i nomes si $\rho_1$ és injectiva i $N\mathbf{P_1}^{-1} = \{\mathbf{0}\}$. La primera condició és decidible pel lema 4.2 i la segona mitjançant un càlcul rutinari.

Ara, si $N\mathbf{P_1}^{-1}\rho_1^{-1}$ és trivial, també ho serà $(\mathrm{Fix}\,\Psi)\pi$; i en conseqüència tant ell com $\mathrm{Fix}\,\Psi$ seran finitament generats.

Si $N\mathbf{P_1}^{-1}\rho_1^{-1} \neq 1$, sabem ([**11**], pàgs. 16-18) que serà finitament generat si i només si té índex finit a $\mathrm{Fix}\,\phi$ (notem que és normal en ser preimatge completa d'un subgrup de $\mathbb{Z}^m$). Ara bé, pel lema 2.1.(b), això equival a que

$N$ tingui índex finit a $\operatorname{im} \mathbf{P_1}$, i com que ambdós són subgrups calculables de $\mathbb{Z}^m$, podrem decidir comprovant si tenen el mateix rang (de nou un procés algorísmic estàndard a $\mathbb{Z}^m$).

Per a obtenir una base de $\operatorname{Fix} \Psi$, procedim de la forma habitual (proposició 4.2) a partir de bases obtingudes per a les projeccions lliure $(\operatorname{Fix} \Psi)\pi$ i lliure-abeliana $(\operatorname{Fix} \Psi)\tau$. Per a les dues parts és clau disposar de la base $\{w_1, \ldots, w_r\}$ de $\operatorname{Fix} \phi$ que proporciona algorísmicament Maslakova. Aleshores podem procedir, tal i com hem fet a la demostració de la proposició 3.7, a construir el *folded graph* de Stallings de $(\operatorname{Fix} \Psi)\pi$ com a subgrup de $\operatorname{Fix} \phi = \langle w_1, \ldots, w_r \rangle$ provant (via *membership problem*) entre els vèrtexs donats per les classes laterals mòdul $N \mathbf{P_1}^{-1} \rho_1^{-1}$, els arcs donats pels elements de la base $\{w_1, \ldots, w_r\}$. A partir del *folded graph* de Stallings i de la base $\{w_1, \ldots, w_r\}$ de $\operatorname{Fix} \phi$, la determinació de bases de $(\operatorname{Fix} \Psi)\pi$ i $(\operatorname{Fix} \Psi)\tau$ respectivament, és rutinària. □

## 5. Twisted conjugacy problem

Recordem que per un grup $G$ qualsevol, donat $\varphi$ un automorfisme de $G$, diem que dos elements $x, y \in G$ són $\varphi$-conjugats (ho denotem $x \sim_\varphi y$) si existeix un $z \in G$ tal que $(z\varphi)^{-1} x z = y$, aleshores també es diu que $z$ és un $\varphi$-conjugador de $x$ amb $y$. És una comprovació senzilla que la $\varphi$-conjugació $\sim_\varphi$ és una relació d'equivalència. Per suposat, $\sim_{\mathrm{id}_G}$ correspon a la conjugació estàndard a $G$.

El *twisted conjugacy problem*, $\mathrm{TCP}(G)$, d'un grup $G$ donat per una presentació finita $G \cong \langle X \mid R \rangle$, és el problema consistent en decidir, donats dos elements $x, y \in G$ i un automorfisme $\varphi \in \mathrm{Aut}(G)$ expressats en termes dels generadors, si $u$ i $v$ són $\varphi$-conjugats. El problema restringit obtingut fixant la família $\mathcal{A} \subseteq \mathrm{Aut}(G)$ de la que podem prendre l'automorfisme $\varphi$ l'anomenarem $\mathcal{A}$-(twisted) conjugacy problem *de* $G$ i el designarem $\mathcal{A}$-$\mathrm{TCP}(G)$. Conseqüentment, si $\mathcal{A} = \{\varphi\}$ (és a dir si $\varphi$ és fixat d'entrada) tindrem el $\varphi$-(twisted) conjugacy problem *de* $G$, $\varphi$-$\mathrm{TCP}(G)$.

Remarquem que per al cas dels grups $F_n \times \mathbb{Z}^m$ és coneguda la decidibilitat del TCP d'ambdós factors. Concretament la del $\mathrm{TCP}(F_n)$ va ser demostrada per Bogopolski, Martino, Maslakova i Ventura a [**3**] com a preludi de la del *conjugacy problem* dels grups *[f.g. free]-by-cyclic*, mentre que la del $\mathrm{TCP}(\mathbb{Z}^m)$ es redueix a la resolubilitat d'un sistema d'equacions diofàntiques, evidentment decidible. Aquests dos fets juntament amb la simplicitat de l'extensió considerada fan bastant previsible la decidibilitat del $\mathrm{TCP}(F_n \times \mathbb{Z}^m)$.

Observem, no obstant, que no és suficient considerar independentment les decidibilitats dels $\mathrm{TCP}^{\text{'s}}$ dels factors per concloure la del $\mathrm{TCP}(F_n \times \mathbb{Z}^m)$.

Així, anomenant $\mathcal{A} = \{(\phi, \mathbf{I_m}, \mathbf{0}) : \phi \in \mathrm{Aut}(F_n)\}$ i $\mathcal{B} = \{(\mathrm{id}_{F_n}, \mathbf{Q}, \mathbf{0}) : \mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})\}$, és immediat de la caracterització que donarem a (30) que, preses per separat, les decidibilitats dels TCP de $F_n$ i $\mathbb{Z}^m$ es tradueixen en les decidibilitats del $\mathcal{A}$-TCP$(F_n \times \mathbb{Z}^m)$ i el $\mathcal{B}$-TCP$(F_n \times \mathbb{Z}^m)$ respectivament, subcasos que evidentment no cobreixen tot el grup d'automorfismes (de fet, tal i com es dedueix fàcilment de (17) ni tan sols en constitueixen una família de generadors). Caldrà, per tant, una aproximació no tan grollera per assolir el resultat.

Donada la decidibilitat del TCP$(F_n)$ sempre podrem, en cas que n'hi hagi, trobar algorísmicament (per un procediment de força bruta) un $w_0$ que $\phi$-conjugui dos elements $u, v \in F_n$ donats qualssevol. Veurem que aleshores el conjunt de $\phi$-conjugadors de $u$ amb $v$ és la classe lateral per la dreta de $w_0$ mòdul $\mathrm{Fix}(\phi\gamma_u)$.

Lema 5.1. *Donats $u, v \in F_n$, $\phi \in \mathrm{Aut}(F_n)$ i $w_0$ un $\phi$-conjugador de $u$ en $v$, aleshores per a tot $w \in F_n$,*

$$(w^{-1})\phi\ u\ w = v \ \Leftrightarrow\ w \in \mathrm{Fix}(\phi\gamma_u)\ w_0\ .$$

*És a dir, els $\phi$-conjugadors de $u$ en $v$, en cas d'haver-n'hi, constitueixen una classe lateral de $\mathrm{Fix}(\phi\gamma_u)$.*

Demostració. En efecte, donat $w_0 \in F_n$ tal que $(w_0^{-1})\phi\ u\ w_0 = v$,

$$\begin{aligned} (w^{-1})\phi\ u\, w = v \quad &\Leftrightarrow\quad (w_0^{-1})\phi\ u\ w_0 = (w^{-1})\phi\ u\ w \\ &\Leftrightarrow\quad u^{-1}\ (ww_0^{-1})\phi\ u = ww_0^{-1} \\ &\Leftrightarrow\quad ww_0^{-1} \in \mathrm{Fix}(\phi\gamma_u) \\ &\Leftrightarrow\quad w \in \mathrm{Fix}(\phi\gamma_u)\ w_0 \end{aligned}$$

□

El lema següent és, com veurem a la demostració del teorema 5.3, bàsicament una versió compacta del problema de decisió en el que queda reduït el TCP$(F_n \times \mathbb{Z}^m)$ un cop aplicada la caracterització (16) que hem obtingut per als endomorfismes de $F_n \times \mathbb{Z}^m$ i separades les parts lliure i abeliana.

Lema 5.2. *El problema consistent en decidir, donats $u, v \in F_n$, $\phi \in \mathrm{Aut}(F_n)$, $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$, $\mathbf{d} \in \mathbb{Z}^m$ i $H \leqslant \mathbb{Z}^m$, si existeix un $w$ $\phi$-conjugador de $u$ amb $v$ tal que $\mathbf{wP} + \mathbf{d} \in H$, és algorísmicament resoluble.*

*És a dir, podem decidir algorísmicament si*

$$\exists w \in F_n \ \textit{tal que} \left\{ \begin{array}{l} (w\phi)^{-1} u w = v \\ \mathbf{wP} + \mathbf{d} \in H\ . \end{array} \right.$$

Demostració. Com que el TCP$(F_n)$ és resoluble, podem decidir sobre l'existència de $\phi$-conjugadors i, en cas afirmatiu, trobar-ne un (que anomenarem $w_0$). Si la resposta al TCP$(F_n)$ és negativa, també ho serà automàticament la nostra i haurem acabat. En cas contrari, usant el lema 5.1

el problema es converteix en el de decidir si

$$\exists w \in F_n \text{ tal que } \begin{cases} w \in \mathrm{Fix}(\phi\gamma_u)\ w_0 \\ \mathbf{wP} + \mathbf{d} \in H \ . \end{cases}$$

Ara, usant un resultat de Maslakova [**12**] podem trobar algorísmicament un conjunt de generadors de $\mathrm{Fix}(\phi\gamma_u)$ i per tant obtenir una base del subgrup $K = (\mathrm{Fix}(\phi\gamma_u))^{\mathrm{ab}} \leqslant \mathbb{Z}^n$, imatge de $\mathrm{Fix}(\phi\gamma_u)$ per l'abelianització ambient $F_n \overset{ab}{\to} \mathbb{Z}^n$ . D'aquesta forma el nostre problema queda reduït a decidir si

$$\exists \mathbf{z} \in \mathbb{Z}^n \text{ tal que } \begin{cases} \mathbf{z} \in K + \mathbf{w_0} \\ \mathbf{zP} + \mathbf{d} \in H \ , \end{cases}$$

i.e., a comprovar si un sistema d'equacions diofàntiques lineals té solució, i és, per tant, decidible. □

Teorema 5.3. *El* twisted conjugacy problem *de* $F_n \times \mathbb{Z}^m$ *és resoluble.*

Demostració. Donats dos elements $\mathbf{t^a}\, u$, $\mathbf{t^b}\, v \in F_n \times \mathbb{Z}^m$ i un automorfisme $\Psi \in \mathrm{Aut}(F_n \times \mathbb{Z}^m)$, volem decidir si existeix un $\mathbf{t^c}\, w \in F_n \times \mathbb{Z}^m$ tal que

$$(\mathbf{t^c}\, w\Psi)^{-1}\ \mathbf{t^a}\, u\ \mathbf{t^c}\, w = \mathbf{t^b}\, v \ .$$

Tenint en compte que tot automorfisme de $F_n \times \mathbb{Z}^m$ és de la forma $\Psi = (\phi, \mathbf{Q}, \mathbf{P})$ amb $\phi \in \mathrm{Aut}(F_n)$, $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$, obtenim la següent expressió equivalent,

$$\mathbf{t^{a+c(I_m-Q)-wP}}\ (w\phi)^{-1}\ u\ w = \mathbf{t^b}\ v$$

on, com sempre, $\mathbf{w}$ designa l'abelianitzat de $w \in F_n$. Ara, separant les parts lliure i abeliana, el $\mathrm{TCP}(F_n \times \mathbb{Z}_m)$ queda reduït a: donats $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^m$, $u, v \in F_n$, $\phi \in \mathrm{Aut}(F_n)$, $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$, decidir si existeixen $\mathbf{c} \in \mathbb{Z}^m$ i $w \in F_n$ tals que

$$\begin{cases} (w\phi)^{-1}\ u\ w = v \\ \mathbf{wP} + \mathbf{b} - \mathbf{a} = \mathbf{c}(\mathbf{I_m} - \mathbf{Q}) \ , \end{cases} \tag{30}$$

que no és res més que un cas particular del lema 5.2 amb $H = \mathrm{im}(\mathbf{I_m} - \mathbf{Q})$ i $\mathbf{d} = \mathbf{b} - \mathbf{a}$. □

## 6. El primer problema de Whitehead

Ens plantejarem per $F_n \times \mathbb{Z}^m$ certs problemes sobre el seu grup d'automorfismes inicialment proposats per Whitehead sobre el del lliure. Els enunciarem per a un grup $G$ general, donat (com sempre) per una presentació finita. Es tracta essencialment de, donats parells d'objectes de certs tipus (algorísmics) al grup, decidir sobre l'existència d'automorfismes que enviïn un a l'altre.

Depenent de l'arietat (*simple* o *múltiple*), el tipus d'objectes involucrats (*paraules* en els generadors o *subgrups* donats per famílies finites de paraules) i de si considerem o no el problema mòdul conjugació, obtenim diferents variants del problema a les que ens referirem genèricament com a *problemes de Whitehead* a $G$.

És habitual parlar de *primer* o *segon* problema de Whitehead depenent de si els objectes considerats són, respectivament, *paraules* o *subgrups*; afegint els adjectius (*'múltiple'* o *'per tuples'*) i *'mòdul conjugació'* en els casos corresponents, i sobreentenent que la seva omissió correspon al cas contrari.

Així, per exemple, el *problema de Whitehead múltiple per paraules* (o *primer problema de Whitehead per tuples*) consisteix en, donades dues tuples $U = (u_1, \ldots, u_s)$ i $V = (v_1, \ldots, v_s)$ de paraules en els generadors de $G$, decidir si existeix un automorfisme $\varphi$ de $G$ que transformi $U$ en $V$, és a dir, tal que $u_k\varphi = v_k$ per $1 \le k \le s$; el cas $s = 1$ correspon òbviament al *problema de Whitehead (simple) per paraules*, o simplement, *primer problema de Whitehead.*

Comencem donant unes caracteritzacions (en termes del màxim comú divisor de les seves components) dels elements primitius de $\mathbb{Z}^m$, i dels transformats d'un determinat element per morfismes generals o bijectius. Si $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$, escriurem $\mathrm{mcd}(\mathbf{a})$ el màxim comú divisor positiu de $\{a_1, \ldots, a_m\}$.

LEMA 6.1. *Un element* $\mathbf{a}$ *és primitiu de* $\mathbb{Z}^m$ *si i només si* $\mathrm{mcd}(\mathbf{a}) = 1$.

DEMOSTRACIÓ. [$\Rightarrow$] En efecte, si fos $1 \ne d = \mathrm{mcd}(\mathbf{a})$, aleshores $\mathbf{a} = d \cdot \mathbf{a}'$, i per a tot $\mathbf{v_2}, \ldots, \mathbf{v_m} \in \mathbb{Z}^m$ tindríem

$$\det(\mathbf{a}, \mathbf{v_2}, \ldots, \mathbf{v_m}) = d \cdot \det(\mathbf{a}', \mathbf{v_2}, \ldots, \mathbf{v_m}) \ne \pm 1 \ ,$$

i per tant $\{\mathbf{a}, \mathbf{v_2}, \ldots, \mathbf{v_m}\}$ no és base de $\mathbb{Z}^m$.

[$\Leftarrow$] Sigui $\mathrm{mcd}(\mathbf{a}) = d = 1$ i considerem la matriu $\mathbf{a}^T$, aleshores sabem (veure, per exemple la secció 12.4 a [**1**]) que existeix una matriu $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ tal que

$$\mathbf{Q}\,\mathbf{a}^T = \mathbf{Q}\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ ,$$

és a dir, $\mathbf{a}^T$ és la primera columna de $\mathbf{Q}^{-1}$, i per tant membre de la base constituïda per les columnes de $\mathbf{Q}^{-1} \in \mathrm{GL}_m(\mathbb{Z})$. □

LEMA 6.2. *Si* $\mathbf{u} \in \mathbb{Z}^n$ *i* $\mathbf{a} \in \mathbb{Z}^m$*, aleshores*

(a) $\{\, \mathbf{uP} \,/\, \mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z}) \,\} = \{\, \tilde{\mathbf{u}} \in \mathbb{Z}^m \,/\, \mathrm{mcd}(\mathbf{u}) \mid \mathrm{mcd}(\tilde{\mathbf{u}}) \,\}$, *i*
(b) $\{\, \mathbf{aQ} \,/\, \mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z}) \,\} = \{\, \tilde{\mathbf{a}} \in \mathbb{Z}^m \,/\, \mathrm{mcd}(\tilde{\mathbf{a}}) = \mathrm{mcd}(\mathbf{a}) \,\}$.

DEMOSTRACIÓ. (a) [$\subseteq$] Siguin $d = \mathrm{mcd}(\mathbf{u})$ i $\mathbf{u} = d \cdot \mathbf{u}'$, aleshores $\mathbf{uP} = d \cdot \mathbf{u}'\mathbf{P}$; per tant $d \mid \mathbf{uP}$ i $d \mid \mathrm{mcd}(\mathbf{uP})$. [$\supseteq$] Siguin $d = \mathrm{mcd}(\mathbf{u})$ i $\tilde{d} = \mathrm{mcd}(\tilde{\mathbf{u}})$, aleshores tenim $\mathbf{u} = d \cdot \mathbf{u}'$ i $\tilde{\mathbf{u}} = \tilde{d} \cdot \tilde{\mathbf{u}}'$ on $\mathrm{mcd}(\mathbf{u}') = \mathrm{mcd}(\tilde{\mathbf{u}}') = 1$ i $\tilde{d} = \alpha \cdot d$, per a un cert $\alpha \in \mathbb{Z}$. Ara, donat que tant $\mathbf{u}'$ com $\tilde{\mathbf{u}}'$ són elements primitius de $\mathbb{Z}^n$

i $\mathbb{Z}^m$ respectivament, existirà una matriu $\mathbf{Q} \in \mathcal{M}_{n\times m}(\mathbb{Z})$ tal que $\tilde{\mathbf{u}}' = \mathbf{u}'\mathbf{Q}$; aleshores

$$\tilde{\mathbf{u}} = \tilde{d} \cdot \tilde{\mathbf{u}}' = \alpha \cdot d \cdot \mathbf{u}'\mathbf{Q} = \mathbf{u}'(\alpha \mathbf{Q}) \ ,$$

i serà suficient prendre $\mathbf{P} = \alpha \mathbf{Q}$.

(b) [$\subseteq$] És suficient prendre, a l'apartat (a), $\mathbf{P}$ igual a $\mathbf{Q}$ i $\mathbf{Q}^{-1}$. [$\supseteq$] Directa del lema 6.1. □

Proposició 6.3. *El primer problema de Whitehead a $F_n \times \mathbb{Z}^m$ és decidible.*

*És a dir, donats $\mathbf{t}^{\mathbf{a}}\, u, \mathbf{t}^{\mathbf{b}}\, v \in F_n \times \mathbb{Z}^m$, podem decidir algorísmicament si existeix un automorfisme $\Psi \in \mathrm{Aut}(F_n)$ tal que $(\mathbf{t}^{\mathbf{a}}\, u)\Psi = \mathbf{t}^{\mathbf{b}}\, v$.*

Demostració. Utilitzant la caracterització dels automorfismes de $F_n \times \mathbb{Z}^m$ com a ternes $(\phi, \mathbf{Q}, \mathbf{P})$ donada al teorema 4.1 i separant les parts lliure i abeliana, el problema es redueix a decidir, donats $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$ i $u, v \in F_n$, si existeixen $\phi \in \mathrm{Aut}(F_n)$, $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$, tals que

$$\begin{cases} u\phi = v \\ \mathbf{aQ} + \mathbf{uP} = \mathbf{b} \end{cases}$$

Observem que apareix com a subproblema l'original de Whitehead sobre el grup lliure $F_n$, que com és ben sabut (veure proposició I.4.19 a [**11**]) és decidible. Tenim, per tant, el següent procediment de decisió per al problema plantejat:

(1) Usem l'algorisme clàssic de Whitehead per decidir, donats els $u, v \in F_n$, si existeix un automorfisme $\phi \in \mathrm{Aut}(F_n)$ que enviï $u$ a $v$.
(2) En el cas que tal $\phi$ no existeixi, és clar que tampoc existirà el $\Psi$ que busquem, i haurem acabat.
(3) En cas que existeixi un $\phi \in \mathrm{Aut}(F_n)$ tal que $u\phi = v$, només caldrà saber decidir si donats $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^m$ i $\mathbf{u} \in \mathbb{Z}^n$ ($\mathbf{u}$ és l'abelianitzat de $u \in F_n$), existeixen $\mathbf{P}$ i $\mathbf{Q}$ dels tipus indicats tals que $\mathbf{aQ} + \mathbf{uP} = \mathbf{b}$. Notem que aquesta condició és independent de $\phi$.
Equivalentment (d'acord amb el lema 6.2) serà suficient decidir, donats $\alpha, \mu \in \mathbb{Z}$ i $\mathbf{b} \in \mathbb{Z}^m$, si existeixen $\tilde{\mathbf{a}}, \tilde{\mathbf{u}} \in \mathbb{Z}^m$ amb $\alpha = \mathrm{mcd}(\tilde{\mathbf{a}})$ i $\mu \mid \mathrm{mcd}(\tilde{\mathbf{u}})$ tals que $\tilde{\mathbf{a}} + \tilde{\mathbf{u}} = \mathbf{b}$. Escrivint $\tilde{\mathbf{a}} = \alpha\,\mathbf{x}$ i $\tilde{\mathbf{u}} = \mu\,\mathbf{y}$, amb $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m$ i $\mathrm{mcd}(\mathbf{x}) = 1$, el problema queda reduït a veure si el següent sistema diofàntic lineal

$$(31) \qquad \left.\begin{array}{ccccc} \alpha\, x_1 & + & \mu\, y_1 & = & b_1 \\ & \vdots & & & \vdots \\ \alpha\, x_m & + & \mu\, y_m & = & b_m \end{array}\right\}$$

té solucions senceres $x_1, \ldots, x_m, y_1, \ldots, y_m$ tals que

$$\mathrm{mcd}(x_1, \ldots, x_m) = 1.$$

Observem que, en estar format per equacions independents, el sistema (31) tindrà solució si i només si en tenen totes les equacions que el constitueixen, és a dir si i només si per a tot $j = 1, \ldots, m$,

$$\mathrm{mcd}(\alpha, \mu) \mid b_j.$$

Si alguna d'aquestes $m$ condicions falla, no existiran les matrius $\mathbf{P}$ i $\mathbf{Q}$ buscades i, per tant, tampoc cap automorfisme de $F_n \times \mathbb{Z}^m$ que enviï $\mathbf{t}^{\mathbf{a}} u$ a $\mathbf{t}^{\mathbf{b}} v$.

En cas contrari, anomenant $\rho = \mathrm{mcd}(\alpha, \mu)$, $\alpha = \rho\alpha'$ i $\mu = \rho\mu'$, la solució general de l'equació $j$-èssima vindrà donada per

$$(x_j, y_j) = (x_j^0, y_j^0) + \lambda_j(\mu', -\alpha'), \quad \lambda_j \in \mathbb{Z}$$

amb $(x_j^0, y_j^0)$ una solució particular, per a tot $j = 1, \ldots, m$. Així, ara només es tracta de decidir si existeixen $\lambda_1, \ldots, \lambda_m \in \mathbb{Z}$ tals que

$$\mathrm{mcd}(x_1^0 + \lambda_1 \mu', \ldots, x_m^0 + \lambda_m \mu') = 1. \tag{32}$$

Per acabar, anem a veure que aquesta condició és equivalent a

$$\mathrm{mcd}(x_1^0, \ldots, x_m^0, \mu') = 1, \tag{33}$$

i per tant, decidible algorísmicament.

En efecte, per la implicació directa, només cal reagrupar adequadament una identitat de Bezout de (32) per obtenir-ne una de (33).

Recíprocament, donats $x_1^0, \ldots, x_m^0, \mu' \in \mathbb{Z}$ coprimers, podem satisfer la condició (32) prenent $\lambda_1 = \cdots = \lambda_{m-1} = 0$ i $\lambda_m$ igual al producte dels primers que divideixin a $x_1^0, \ldots, x_{m-1}^0$ i no a $x_m^0$ (amb el producte buit igual a 1).

Serà suficient veure que tot $p$ factor primer de $x_1^0, \ldots, x_{m-1}^0$ no ho és de $x_m^0 + \lambda_m \mu'$. Sigui doncs un tal $p$, distingirem dos casos: 1) si $p \mid x_m^0$, aleshores $p \nmid \mu'$ ($p$ divideix $x_1^0, \ldots, x_m^0$ i $\mathrm{mcd}(x_1^0, \ldots, x_m^0, \mu') = 1$) i $p \nmid \lambda_m$ (per construcció). En definitiva, $p$ divideix a $x_m^0$ i no a $\lambda_m \mu'$ i per tant $p \nmid x_m^0 + \lambda_m \mu'$; 2) si $p \nmid x_m^0$, aleshores $p$ divideix $\lambda_m$ (per construcció). És a dir $p$ divideix a $\lambda_m \mu'$ i no a $x_m^0$ i per tant $p \nmid x_m^0 + \lambda_m \mu'$.

Evidentment, donades dues paraules arbitràries en els generadors, només caldrà escriure-les en forma normal $\mathbf{t}^{\mathbf{a}} u, \mathbf{t}^{\mathbf{b}} v$ i decidir sobre l'existència d'un automorfisme que enviï una a l'altra mitjançant el procediment descrit. □

## 7. Orbit problem

Si $G$ és un grup qualsevol i $A \leqslant \mathrm{Aut}(G)$ és un subgrup d'automorfismes de $G$, anomenem *orbit problem* per a $A$ (a $G$), $\mathrm{OP}(A)$, al problema consistent en decidir, donats dos elements $u, v \in G$ qualssevol en termes dels generadors, si existeix un automorfisme $\varphi \in A$ tal que $u\varphi$ i $v$ siguin conjugats a $G$.

$$\mathrm{OP}(A) \;\equiv\; ¿\; \exists \varphi \in A \mid u\varphi \sim_G v \;?_{\;(u,v\in G)} \;.$$

Quan l'*orbit problem* per $A$ és decidible algorísmicament diem simplement que $A$ és *òrbita-decidible.*

Observació 14. Tenim la següent cadena d'equivalències:

$$\begin{aligned} & \exists \varphi \in A \mid u\varphi \sim_G v \\ \Leftrightarrow\; & \exists \varphi \in A,\; \exists \gamma \in \mathrm{Inn}(G) \mid u\varphi\gamma =_G v \\ \Leftrightarrow\; & \exists \psi \in A \cdot \mathrm{Inn}(G) \mid u\psi =_G v \;. \end{aligned}$$

Per tant, si $A \cdot \mathrm{Inn}(G) = B \cdot \mathrm{Inn}(G)$ les *òrbita-decidibilitats* de $A$ i $B$ són equivalents. Dit d'una altra forma, l'òrbita-decidibilitat és una propietat dels subgrups de $\mathrm{Out}(G)$. Observem que, en particular, s'obté l'equivalència entre les òrbita-decidibilitats dels subgrups $A$ i $A\cdot\mathrm{Inn}(G)$, per a tot $A \leqslant \mathrm{Aut}(G)$.

Obtenim també, com a conseqüència directa de la darrera observació, la coincidència entre el problema de Whitehead per paraules en $G$ i l'*orbit problem* de $\mathrm{Aut}(G)$.

Considerem una successió exacta curta de grups,

$$1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1 \;.$$

Donat que $F\alpha$ és normal a $G$, per a tot $g \in G$ la restricció a $F\alpha$ de la conjugació $\gamma_g$ a $G$ proporciona un automorfisme, $x\alpha \mapsto g^{-1}x\alpha\, g$, de $F\alpha$, que, a través de $\alpha$, indueix un automorfisme $\varphi_g$ a $F$. Amb més detall, per a tot $g \in G$, podem definir $\varphi_g := \alpha\, \gamma_{g_{|F\alpha}}\, \alpha^{-1}$,

$$x \overset{\alpha}{\longmapsto} x\alpha \overset{\gamma_{g|F\alpha}}{\longmapsto} g^{-1}\,(x\alpha)\,g \overset{\alpha^{-1}}{\longmapsto} (g^{-1}\,(x\alpha)\,g)\alpha^{-1} \;.$$

Identificant, com es fa habitualment, $x$ i $x\alpha$, tenim que per a tot $g \in G$, $\varphi_g : x \mapsto g^{-1}xg$ és un automorfisme (no necessàriament interior) de $F$. És clar que el conjunt format per aquests automorfismes,

$$A_G = \{\varphi_g \mid g \in G\} \;,$$

és un subgrup de $\mathrm{Aut}(F)$ que conté a $\mathrm{Inn}(F)$. L'anomenarem el *subgrup d'acció* de la successió exacta curta donada.

Suposant certes hipòtesis sobre la successió anterior i els grups involucrats, el proper teorema mostra que la decidibilitat del *conjugacy problem* per $G$ és equivalent a l'òrbita-decidibilitat del *subgrup d'acció* $A_G \leqslant \mathrm{Aut}(F)$.

Teorema 7.1 (Bogopolski, Martino i Ventura [**4**]). *Sigui*

$$1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

*una successió exacta curta de grups (donada per presentacions finites), tal que*

(a) *el* $\mathrm{TCP}(F)$ *és decidible.*
(b) *el* $\mathrm{CP}(H)$ *és decidible.*
(c) *per a tot* $1 \neq h \in H$*, el subgrup* $\langle h \rangle$ *té índex finit en el seu centralitzador* $C_H(h)$*, i hi ha un algorisme que computa un nombre finit de representants de classe,* $z_{h,1}, \ldots, z_{h,t_h} \in H$*,*

$$C_H(h) = \langle h \rangle z_{h,1} \sqcup \cdots \sqcup \langle h \rangle z_{h,t_h}$$

*Aleshores, el* $\mathrm{CP}(G)$ *és decidible si i només si ho és el* $\mathrm{OP}(A_G)$*.* □

Lema 7.2. $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$ *és òrbita-decidible.*

Demostració. La decidibilitat del problema de Whitehead per paraules a $F_n \times \mathbb{Z}^m$ ha estat demostrada a 6.3 i, tal i com hem comentat a l'observació 14, per qualsevol grup la decidibilitat del seu problema del Whitehead per paraules és equivalent a l'òrbita-decidibilitat del seu grup d'automorfismes. □

Corol.lari 7.3. *Si* $\Phi_1, \ldots, \Phi_r$ *és una família de generadors de* $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$*, aleshores el* conjugacy problem *del grup* $(F_n \times \mathbb{Z}^m) \rtimes_{\alpha_1,\ldots,\alpha_r} F_r$ *és decidible*

Demostració. Només s'ha d'aplicar el teorema 7.1 sobre la successió exacta curta següent

$$1 \longrightarrow F_n \times \mathbb{Z}^m \longrightarrow (F_n \times \mathbb{Z}^m) \rtimes_{\Phi_1,\ldots,\Phi_r} F_r \longrightarrow F_r \longrightarrow 1 \ .$$

Notem que en aquest cas el subgrup d'acció és $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$ i es compleixen els requisits del teorema:

- el $\mathrm{TCP}(F_n \times \mathbb{Z}^m)$ és decidible: teorema 5.3.
- el $\mathrm{CP}(F_r)$ és decidible: veure per exemple la proposició I.2.14 a [**11**].
- per a tot $1 \neq w \in F_r$, $\langle \mathrm{root}(w) \rangle = C_{F_r}(w)$ i el tercer punt es compleix trivialment.
- el $\mathrm{OP}(\mathrm{Aut}(F_n \times \mathbb{Z}^m))$ és decidible: lema 7.2.

Podem concloure, per tant, que el $\mathrm{CP}((F_n \times \mathbb{Z}^m) \rtimes_{\alpha_1,\ldots,\alpha_r} F_r)$ és decidible. □

# Capítol 4
# Problemes no resolts

> "That's like asking the square root of a million. No one will ever know."
>
> Nelson Muntz

## 1. El primer problema de Whitehead per tuples

Recordem que per a un grup $G$ arbitrari, el *problema de Whitehead múltiple per paraules* (o *primer problema de Whitehead per tuples*) consisteix en, donades dues tuples $U = (u_1, \ldots, u_s)$ i $V = (v_1, \ldots, v_s)$ de paraules en els generadors de $G$, decidir si existeix un automorfisme $\varphi$ de $G$ que transformi $U$ en $V$, és a dir, tal que $u_k\varphi = v_k$ per $1 \leq k \leq s$.

En el cas de $G = F_n \times \mathbb{Z}^m$, el problema consisteix doncs en, donades dues tuples $(\mathbf{t}^{\mathbf{a_1}} u_1, \ldots, \mathbf{t}^{\mathbf{a_s}} u_s)$ i $(\mathbf{t}^{\mathbf{b_1}} v_1, \ldots, \mathbf{t}^{\mathbf{b_s}} v_s)$ d'elements de $G$, decidir sobre l'existència d'un un automorfisme de $F_n \times \mathbb{Z}^m$ – que d'acord amb el teorema 4.1 pensarem com una terna $(\phi, \mathbf{Q}, \mathbf{P})$ amb $\phi \in \operatorname{Aut}(F_n)$, $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$ – que transformi una tupla en l'altra.

Així doncs, pretenem determinar si existeixen $\phi$, $\mathbf{Q}$ i $\mathbf{P}$ dels tipus anteriors, tals que:

$$\left\{ \begin{array}{l} u_1\phi = v_1 \\ \mathbf{a_1}\,\mathbf{Q} + \mathbf{u_1}\,\mathbf{P} = \mathbf{b_1} \end{array} \right. , \ \ldots \ , \left\{ \begin{array}{l} u_s\phi = v_s \\ \mathbf{a_s}\,\mathbf{Q} + \mathbf{u_s}\,\mathbf{P} = \mathbf{b_s} \end{array} \right. .$$

Obtenim com a subproblema del nostre, el primer problema de Whitehead per tuples a $F_n$. Ara, com aquest és resoluble (veure, per exemple, la secció I.4 a [**11**]) el problema queda reduït a decidir, donats $\mathbf{a_1}, \ldots, \mathbf{a_s}, \mathbf{b_1}, \ldots, \mathbf{b_s} \in \mathbb{Z}^m$ i $\mathbf{u_1}, \ldots, \mathbf{u_s} \in \mathbb{Z}^n$, si existeixen matrius $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$ tals que

$$\begin{cases} \mathbf{a_1}\,\mathbf{Q} + \mathbf{u_1}\,\mathbf{P} = \mathbf{b_1} \\ \quad\vdots \\ \mathbf{a_s}\,\mathbf{Q} + \mathbf{u_s}\,\mathbf{P} = \mathbf{b_s}\ . \end{cases}$$

Escrivint

$$\mathbf{A} = \begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_s} \end{pmatrix}\ ,\ \mathbf{U} = \begin{pmatrix} \mathbf{u_1} \\ \vdots \\ \mathbf{u_s} \end{pmatrix}\ \text{ i }\ \mathbf{B} = \begin{pmatrix} \mathbf{b_1} \\ \vdots \\ \mathbf{b_s} \end{pmatrix}\ ,$$

el problema queda reduït a decidir, donades matrius $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{s\times m}(\mathbb{Z})$ i $\mathbf{U} \in \mathcal{M}_{s\times n}(\mathbb{Z})$, si existeixen $\mathbf{Q}$ i $\mathbf{P}$ dels tipus requerits tals que

$$\mathbf{A}\,\mathbf{Q} + \mathbf{U}\,\mathbf{P} = \mathbf{B}\ .$$

Agrupant l'anterior en un únic producte matricial queda el problema de decidir, donades $\tilde{\mathbf{A}} = (\mathbf{A}\ \ \mathbf{U}) \in \mathcal{M}_{s\times(m+n)}(\mathbb{Z})$ i $\mathbf{B} \in \mathcal{M}_{s\times m}(\mathbb{Z})$, si existeixen $\mathbf{Q} \in \mathrm{GL}_m(\mathbb{Z})$ i $\mathbf{P} \in \mathcal{M}_{n\times m}(\mathbb{Z})$ tals que

$$\tilde{\mathbf{A}} \begin{pmatrix} \mathbf{Q} \\ \mathbf{P} \end{pmatrix} = \mathbf{B}\ . \tag{34}$$

Aquest és un problema de decisió perfectament delimitat dintre de l'àmbit matricial, que esperem poder resoldre properament. Sembla, per exemple, que l'ús de la forma normal de Smith sobre les matrius de dades de l'expressió (34) pot simplificar-la sensiblement i apropar-nos a aquest objectiu.

## 2. El problema de Brinkmann

El *problema de Brinkmann* a un grup arbitrari $G$, $\mathrm{BrP}(G)$, és el problema consistent en decidir, donats dos elements $u, v \in G$ qualssevol en termes dels generadors i un automorfisme $\varphi \in \mathrm{Aut}(G)$ qualsevol, si existeix un $k \in \mathbb{Z}$ tal que $u\varphi^k$ i $v$ siguin conjugats a $G$.

$$\mathrm{BrP}(G)\ \equiv\ ¿\ \exists k \in \mathbb{Z} \mid u\varphi^k \sim_G v\ ?_{\,(u,v\in G,\,\varphi\in\mathrm{Aut}(G))}$$

Peter Brinkmann dóna nom al problema en resoldre'l a [**5**] per al grup lliure $F_n$, concretament enuncia el teorema següent.

TEOREMA 2.1 (Brinkmann, [**5**]). *Sigui $\varphi$ un automorfisme d'un grup lliure finitament generat $F_n$, aleshores*

(a) *Existeix un algoritme explícit que, donats dos elements $u, v \in F_n$ qualssevol decideix si existeix algun exponent $k$ tal que $u\varphi^k = v$.*
(b) *Existeix un algoritme explícit que, donats dos elements $u, v \in F_n$ qualssevol decideix si existeix algun exponent $k$ tal que $u\varphi^k$ és conjugat a $v$.*

*Si tal exponent existeix, els algoritmes també el calcularan. Les paraules $u, v$ estan donades en termes dels generadors de $F_n$, i $\varphi$ està donada en termes de les imatges dels generadors.*

OBSERVACIÓ 15. Notem que el punt (b) del teorema anterior estableix que, donat $\varphi \in \mathrm{Aut}(F_n)$, el $\mathrm{OP}(\langle\varphi\rangle, F_n)$ és resoluble. És a dir que $\langle\varphi\rangle \leqslant \mathrm{Aut}(F_n)$ és òrbita-decidible.

**2.1. El grup $(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}$ i el seu subgrup d'acció.** Un cop assolida la resolubilitat del $\mathrm{TCP}(F_n \times \mathbb{Z}^m)$ resulta natural intentar usar el teorema 7.1 per tal d'estudiar la resolubilitat del CP a extensions seves per grups $H$ que satisfacin les hipòtesis del teorema, reduint així la resolubilitat del *conjugacy problem* del nou grup a l'òrbita-decidibilitat del seu subgrup d'acció.

Un primer pas en la direcció comentada és el producte semidirecte per $H = \mathbb{Z}$, que satisfà trivialment les condicions. Sigui doncs $\Psi \in \mathrm{Aut}(F_n \times \mathbb{Z}^m)$ i considerem el grup

$$(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z} = \left\langle x_1, \ldots, x_n, t_1, \ldots, t_m, s \;\middle|\; \begin{array}{ll} [x_i, t_k]\,, & [t_j, t_k]\,, \\ s^{-1} x_i\, s = x_i \Psi\,, & s^{-1} t_k\, s = t_k \Psi \end{array} \right\rangle$$

per als elements del qual, reordenant convenientment les lletres (les $s$ mòdul l'acció de $\Psi$ que correspongui) obtenim la forma normal

$$s^k\, \mathbf{t}^{\mathbf{a}}\, u \quad \text{amb } k \in \mathbb{Z},\ \mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m \text{ i } u \in F_n\ ,$$

on recuperem la notació $\mathbf{t}^{\mathbf{a}}\, u$ descrita al lema 1.1 per als elements de $F_n \times \mathbb{Z}^m$.

Aleshores la successió exacta curta

$$1 \longrightarrow F_n \times \mathbb{Z}^m \longrightarrow (F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 1$$

compleix clarament les condicions del teorema 7.1. Així doncs, la resolubilitat del $\mathrm{CP}((F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z})$ és equivalent a l'òrbita-decidibilitat del següent subgrup, $A_{(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}}$, d'automorfismes de $F_n \times \mathbb{Z}^m$

$$\{\, \gamma_{s^k \mathbf{t}^{\mathbf{a}} u} : F_n \times \mathbb{Z}^m \to F_n \times \mathbb{Z}^m \mid s^k\, \mathbf{t}^{\mathbf{a}}\, u \in (F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z} \,\}\ .$$

LEMA 2.2. *El subgrup d'acció és*

$$A_{(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}} = \langle\Psi\rangle\, \mathrm{Inn}(F_n \times \mathbb{Z}^m) \leqslant \mathrm{Aut}(F_n \times \mathbb{Z}^m)\ .$$

DEMOSTRACIÓ. A partir de l'acció de conjugació $\gamma\colon g \mapsto \gamma_g$, és clar que

$$\mathrm{Inn}(A_{(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}}) = \langle \{x_i\}_i \cup \{t_j\}_j \cup \{s\} \rangle\, \gamma = \langle \{\gamma_{x_i}\}_i \cup \{\gamma_{t_j}\}_j \cup \{\gamma_s\} \rangle\ .$$

I, per tant, el subgrup d'acció de $A_{(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}}$ (i.e. les seves restriccions a $F_n \times \mathbb{Z}^m$) és

$$\begin{aligned} A_{(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}} &= \langle \{\gamma_{x_i|F_n \times \mathbb{Z}^m}\}_i \cup \{\gamma_{t_j|F_n \times \mathbb{Z}^m}\}_j \cup \{\gamma_{s|F_n \times \mathbb{Z}^m}\} \rangle \\ &= \langle \gamma_{s|F_n \times \mathbb{Z}^m} \rangle \cdot \langle \{\gamma_{x_i|F_n \times \mathbb{Z}^m}\}_i \cup \{\gamma_{t_j|F_n \times \mathbb{Z}^m}\}_j \rangle\ , \end{aligned}$$

on $\langle \gamma_{s|F_n \times \mathbb{Z}^m} \rangle = \langle\Psi\rangle$, i $\langle \{\gamma_{x_i|F_n \times \mathbb{Z}^m}\}_i \cup \{\gamma_{t_j|F_n \times \mathbb{Z}^m}\}_j \rangle = \mathrm{Inn}(F_n \times \mathbb{Z}^m)$. $\square$

Així doncs, el *conjugacy problem* de $(F_n \times \mathbb{Z}^m) \rtimes_\Psi \mathbb{Z}$ es redueix a l'estudi de l'òrbita-decidibilitat de $\langle \Psi \rangle\, Inn(F_n \times \mathbb{Z}^m)$ que, con ja hem vist, equival a la de $\langle \Psi \rangle$.

**2.2. Òrbita-decidibilitat de $\langle \Psi \rangle \leqslant \mathrm{Aut}(F_n \times \mathbb{Z}^m)$.** Donats dos elements $\mathbf{t^a}\, u, \mathbf{t^b}\, v \in F_n \times \mathbb{Z}^m$ qualssevol, es tracta de decidir si existeix un $\Phi \in \langle \Psi \rangle$ tal que $(\mathbf{t^a} u)\Phi$ i $\mathbf{t^b} v$ siguin conjugats a $F_n \times \mathbb{Z}^m$. És a dir, volem veure si existeix un $k \in \mathbb{Z}$ tal que

$$(\mathbf{t^a} u)\Psi^k \sim \mathbf{t^b} v \ . \tag{35}$$

Aquest és precisament el problema de Brinkmann a $F_n \times \mathbb{Z}^m$, $\mathrm{BrP}(F_n \times \mathbb{Z}^m)$.

Escrivint $\Psi = (\phi, \mathbf{Q}, \mathbf{P})$, $\mathbf{A} = \phi^{\mathbf{ab}}$, $\mathbf{S}_k = \sum_{i=1}^{k} \mathbf{A}^{i-1}\, \mathbf{P}\, \mathbf{Q}^{k-i}$ i usant l'expressió donada al lema 1.5 per a la potència $k$-èssima d'un automorfisme de $F_n \times \mathbb{Z}^m$, obtenim les següents equivalències:

$$\begin{aligned} (\mathbf{t^a} u)(\phi, \mathbf{Q}, \mathbf{P})^k \sim \mathbf{t^b} v \quad &\Leftrightarrow \quad (\mathbf{t^a} u)(\phi^k, \mathbf{Q}^k, \mathbf{S_k}) \sim \mathbf{t^b} v \\ &\Leftrightarrow \quad \mathbf{t}^{\mathbf{a}\,\mathbf{Q^k} + \mathbf{u}\,\mathbf{S_k}}\, u\phi^k \sim \mathbf{t^b} v \ . \end{aligned}$$

Ara, considerant la conjugació i agrupant les parts lliure i abeliana, és clar que el problema de l'òrbita-decidibilitat queda reduït a decidir sobre l'existència d'un $k \in \mathbb{Z}$ tal que satisfaci les dues condicions següents

$$\begin{cases} u\phi^k \sim_{F_n} v \\ \mathbf{a}\,\mathbf{Q^k} + \mathbf{u}\,\mathbf{S_k} = \mathbf{b} \ . \end{cases}$$

Observem que restringint-nos a la primera, obtenim precisament el problema de Brinkmann, per al qual [**5**] estableix la resolubilitat, i en cas d'existir, en proporciona una solució. Així doncs, si l'algorisme de Brinkmann retorna `NO`, també serà negativa la resposta a l'òrbita-decidibilitat de $\langle \Psi \rangle$ i haurem acabat. En cas contrari, el conjunt

$$\mathrm{Br}(u, v, \phi) = \{\, k \in \mathbb{Z} \mid u\phi^k \sim v \,\} \ ,$$

és una classe lateral mòdul $\mathrm{Br}(u, u, \phi) \leqslant \mathbb{Z}$. Aleshores, si $\mathrm{Br}(u, u, \phi) = \{0\}$, la classe lateral $\mathrm{Br}(u, v, \phi)$ té un sol punt, i no tenim més que avaluar-lo a l'equació matricial per decidir. En cas contrari, serà

$$\mathrm{Br}(u, v, \phi) = k_0 + l_0 \cdot \mathbb{Z} \ ,$$

per a un cert $l_0 \in \mathbb{N}$, i un cert $k_0 \in \mathbb{N}$ que podem suposar no negatiu i minimal, calculables. Aleshores el problema queda reduït a decidir sobre l'existència d'un $k \in k_0 + l_0 \cdot \mathbb{Z}$ tal que

$$\mathbf{a}\,\mathbf{Q^k} + \mathbf{u}\,\mathbf{S_k} = \mathbf{b} \ .$$

Escrivint $k = k_0 + \lambda \cdot l_0$, es tractarà de decidir sobre l'existència d'un $\lambda \in \mathbb{Z}$ tal que

$$\mathbf{a}\,\mathbf{Q}^{k_0 + \lambda l_0} + \mathbf{u}\,\mathbf{S}_{\mathbf{k_0} + \boldsymbol{\lambda} \mathbf{l_0}} = \mathbf{b} \ . \tag{36}$$

Hem reduït, doncs, el problema de Brinkmann a $F_n \times \mathbb{Z}^m$ a un problema de decisió purament abelià, que fins al moment, només hem pogut resoldre per a certs casos particulars especialment senzills.

Observem, per acabar, que si definim la matriu $(n+m) \times (n+m)$

$$\mathbf{C} := \begin{pmatrix} \mathbf{A} & \mathbf{P} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix},$$

aleshores tenim

$$\mathbf{C}^k = \begin{pmatrix} \mathbf{A}^k & \sum_{i=1}^{k} \mathbf{A}^{i-1}\mathbf{P}\mathbf{Q}^{k-i} \\ \mathbf{0} & \mathbf{Q}^k \end{pmatrix} = \begin{pmatrix} \mathbf{A}^k & \mathbf{S}_k \\ \mathbf{0} & \mathbf{Q}^k \end{pmatrix}.$$

Igualtat que convida a intentar expressar l'equació (36) en termes d'una potència matricial; via encara no explorada que esperem pugui donar fruits en el futur.

# Conclusions

Aquest treball, que té com a objecte l'estudi dels grups lliure per lliure-abelians, consta de dues parts ben diferenciades.

A la primera s'analitza la seva estructura i els seus paral.lelismes i diferències amb la dels seus factors constituents: $F_n$ i $\mathbb{Z}^m$. Es mostra, per exemple, que els seus subgrups són també lliure-per lliure abelians i que es pot definir de manera natural sobre ells nocions que estenen les estàndard de rang i base.

A continuació analitzem els endomorfismes de $F_n \times \mathbb{Z}^n$ i els caracteritzem en dues classes disjuntes, donant expressions explícites tant per a ells com per a les seves composicions. Veiem que el segon d'aquests tipus és un cas degenerat; mentre que el primer, descrit només en termes de dos endomorfismes dels factors i un terme creuat que controla com s'entrellacen les parts lliure i lliure-abeliana, inclou tots els monomorfismes i epimorfismes de $F_n \times \mathbb{Z}^m$, per als quals obtenim també caracteritzacions explícites. D'aquestes caracteritzacions es dedueix immediatament la hopfianitat de $F_n \times \mathbb{Z}^m$, i per tant la caracterització del grups $\mathrm{Aut}(F_n \times \mathbb{Z}^m)$ per al que es demostra el seu caràcter finitament generat.

A la segona part, un cop establerta la connexió entre l'univers lliure per lliure-abelià i els seus factors, es fa palès que certs problemes de decisió algorísmica a $G = F_n \times \mathbb{Z}^m$ es traduiran en les respectives versions del problema sobre la part lliure (on ja es disposa de molts resultats) i la part lliure-abeliana (sobre la que alguns dels problemes de decisió prenen una forma trivial o resoluble fàcilment amb àlgebra lineal), juntament amb una certa complicació derivada de com estan entrellaçades a $G$ les parts lliures i lliure-abelianes del problema. Succeeix que aquest entrellaçament és, en molt casos, de tipus lineal i per tant atacable amb eines clàssiques. Així, tractem de reduir els problemes de decisió sobre $G = F_n \times \mathbb{Z}^m$, als problemes homònims sobre el grup lliure, juntament amb un problema abelià més o menys sofisticat.

La dificultat d'aquest darrer varia sensiblement amb cada problema atacat. Des de casos trivials (com ara el *word problem* i el conjugacy problem) o quasi (*isomorphism problem* i *membership problem*) fins a casos (com ara el *twisted conjugacy problem*, el primer problema de Whitehead i especialment els problemes de decisió sobre l'índex finit d'un subgrup, o el caràcter finitament generat del subgrup de punts fixos per un automorfisme o la intersecció de subgrups) que precisen d'un desenvolupament més elaborat.

A l'extrem final d'aquest espectre, apareixen problemes de decisió que, tot i que hem aconseguit reduir-los a problemes abelians raonables, encara no hem pogut resoldre. En particular, per al *segon problema de Whitehead* obtenim un problema matricial d'aspecte assequible que esperem poder resoldre properament. Per al darrer cas (*problema de Brinkmann*), d'aparença més seriosa, proposem alguna idea que esperem pugui contribuir a la seva resolució.

# Bibliografia


[1] M. Artin, “Algebra”, *Prentice Hall*, (1991).

[2] B. Baumslag, “Intersections of finitely generated subgroups in free products”, *J. London Math. Soc.*, **41**, 673-679 (1966).

[3] O. Bogopolski, A. Martino, O. Maslakova, E. Ventura, “Free-by-cyclic groups have solvable conjugacy problem”, *Bulletin of the London Mathematical Society*, **38**(5) (2006), 787-794.

[4] O. Bogopolski, A. Martino, E. Ventura, “Orbit decidability and the conjugacy problem for some extensions of groups”, *Transactions of the American Mathematical Society*, ISSN 0002-9947, Vol. 362, Nº 4, 2010, pàgs. 2003-2036.

[5] P. Brinkmann, “Detecting automorphic orbits in free groups”, *Journal of Algebra* 324 (2010) 1083-1097.

[6] M. B. Day, “Peak reduction and finite presentations for automorphism groups of right-angled Artin groups”, *Geometry & Topology* 13 (2009) 817-855.

[7] E.R. Green, “Graph Products of Groups”, *PhD thesis, University of Leeds*, (1990).

[8] A. G. Howson, “On the intersection of finitely generated free groups”, *J. London Math. Soc.* 29, 428-434 (1954).

[9] S.P. Humphries, “On representations of Artin groups and the Tits conjecture”, *J. Algebra* 169 (1994), no. 3, 847-862.

[10] M.R. Laurence, “A generating set for the automorphism group of a graph group”, *J. London Math. Soc.(2)* , 52(2):318-334 (1995).

[11] R.C. Lyndon, P.E. Schupp, “Combinatorial Group Theory”. *Springer-Verlag, Berlin-New York*, 1977. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89.

[12] O. Maslakova, “The fixed point group of a free group automorphism”, *Algebra Logic 42* (2003) 237-265.

[13] J.M. Tyrer, “On Direct products and the Hopf Property”, *D. Phil. Thesis, University of Oxford*, (1971).