Grau en Matemàtiques

TREBALL DE FI DE GRAU

Títol: Problemes Irresolubles en Teoria de Grups

Autor: Josep Miquel Porcar

Director: Enric Ventura

Departament: Matemàtica Aplicada III

Convocatòria: 2013 - 2014

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Treball de fi de grau

Problemes Irresolubles en Teoria de Grups

Josep Miquel Porcar

Director: Enric Ventura

Departament de Matemàtica Aplicada III

Índex general

Resum

Paraules clau: Problemes de Dehn, problema de la paraula, grups lliures

MSC2010: 20E06, 20F05, 20F10

Aquest recull és el conjunt d'uns quants resultats de la teoria dels problemes de decisió en grups, els quals sempre han estat d'interés dins la teoria de grups. Partint de la teoria básica de grups lliures i d'alguns fets que suposarem donats, anem obtenint resultats relacionats amb els *problemes fonamentals de Dehn*. Un cop presentats aquests problemes i demostrat que existeixen grups finitament presentats amb *problema de la paraula* irresoluble, introduim les *propietats de Markov*, les quals són recursivament irreconeixibles. I partint de la demostració obtenim uns quants resultats sobre la inclusió de grups en grups generats per dos elements. Finalment partint de la construcció de Miller, obtenim uns resultats relacionats amb el *problema de l'òrbita* i el *problema de conjugació*. Hem de precisar que aquest recull va desde problemes i resultats clàssics (com el *problema de la paraula*), fins a resultats més moderns (demostrarem que hi ha un grup generat per 14 matrius de $GL_4(\mathbb{Z})$ que té *problema de l'òrbita* irresoluble).

Abstract

Keywords: Dehn's fundamental problems, word problem, free groups

MSC2010: 20E06, 20F05, 20F10

This work presents a collection of results about decision problems in groups, an area of research that has been always active and interesting within groups theory. Based on the elementary theory of free groups, we keep collecting results about *Dehn's fundamental problems*. After those problems are presented and the existence of a finitely presented group with unsolvable *word problem* is proven, we introduce and study the so called *Markov properties*. Using those techniques, we also give some results about groups embeddings into two-generated groups. Finally, using Miller's construction, we obtain some results about the *conjugacy problem* and the *orbit problem*. We want to emphasize that the present manuscript collects from very classical results (about *word problem*, for example) to much modern ones (like the existence of the 14 matrix of $GL_4(\mathbb{Z})$ generating an *orbit undecidable linear group*).

Capítol 1
Preliminars

En aquest treball assumirem que el lector està familiaritzar amb la teoria bàsica de grups, no obstant en aquest capítol recordarem unes quantes propietats bàsiques. Abans d'això presentarem una definició que està present en tota la teoria dels problemes irresolubles.

Definició 1.1 Un *algoritme* és un conjunt finit d'instruccions o passos que serveixen per a executar una tasca o resoldre un problema. Un algoritme ha de tenir clarament definits els següents tres aspectes::

- **Context:** és el que es suposa que no canvia (l'estructura algebràica i el marc on haurem de fer càlculs),
- **Entrada:** és el que es dóna a l'algoritme (el conjunt de possibles entrades vàlides ha d'estar ben determinat), i
- **Sortida:** és el que l'algoritme donarà com a resposta a partir d'una entrada donada.

Normalment escriurem l'operació del grup com la multiplicació. L'element neutre l'escriurem com a 1 i l'invers d'un element g serà g^{-1}.

Definició 1.2 Per a qualssevols u, v d'un grup G, anomenarem *commutador* $[u, v] = u^{-1}v^{-1}uv$. Si aquests dos elements commuten, el seu commutador serà 1.

Definició 1.3 L'element $v^{-1}uv$ s'anomena el *conjugat* de u per v. Dos elements u, w d'un grup G s'anomenen *conjugats* si existeix $v \in G$ tal que $w = v^{-1}uv$. Per a un $v \in G$ la funció $\gamma_v : G \to G$ definida per $\gamma_v(g) = v^{-1}gv$ s'anomena *conjugació per v.*

Si S és un subconjunt d'un grup G, notarem per $\langle S\rangle$ el subgrup de G més petit contenint S anomenat el *subgrup generat per* S; es pot caracteritzar per:

$$\{g \in G | g = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} \text{ per alguns } s_i \in S \text{ i } \epsilon_i = \pm 1\}$$

Definició 1.4 Sigui G un grup i g un element de G, el *centralitzador de* g és el subgrup:

$$C_G(a) = \{x \in G \mid xa = ax\}.$$

Definició 1.5 Sigui G un grup, H un subgrup de G i sigui $g \in G$. La *classe lateral* de g mòdul H és el conjunt:

$$gH = \{gh | h \in H\}$$

També es pot definir de manera similar Hg.

Definició 1.6 Anomenarem l'*índex* d'un subgrup H d'un grup G al nombre de classes laterals.

Definició 1.7 Sigui G un grup. El *rang de* G $rank(G)$ és el nombre mínim de generadors que necessitem per a generar G:

$$rank(G) = min\{|X| : X \subseteq G, \langle X\rangle = G\} \quad .$$

1.1 Grups lliures

Definició 1.1.1 Direm que un subconjunt S d'un grup F és una *base lliure* de F si per tot funció $\varphi : S \to G$ es pot extendre únicament a un homomorfisme $\tilde{\varphi} : F \to G$ tal que $\tilde{\varphi}(s) = \varphi(s)$, $\forall s \in S$.
Un grup F s'anomena *grup lliure* si té bases lliures per F.

Teorema 1.1.2 *Si S és un conjunt, existeix un grup lliure F_S amb S com a base lliure.*

Teorema 1.1.3 *Tot grup és quocientd d'un grup lliure. En particular, si G és un grup, existeix un grup lliure F i un subgrup normal N tal que $G \cong F/N$.*

Definició 1.1.4 Una paraula està *lliurement reduïda* si no conté cap subparaula de la forma xx^{-1} o $x^{-1}x$.

Teorema 1.1.5 *Sigui G un grup, i S un subconjunt de G. Aleshores G és lliure amb base S si i només si es compleix:*

(1) S genera G,
(2) Si w és una paraula en S i $w =_G 1$, aleshores w no està lliurement reduïda.

1.2 Producte directe i producte lliure

Necessitarem definir el producte directe i el producte lliure ja que els utilitzarem en diferents teoremes i demostracions.

Definició 1.2.1 Donats dos grups K i H amb presentacions $K = \langle S|D\rangle$ i $H = \langle T|E\rangle$ i assumint que S i T són disjunts, anomenarem el *producte directe* de K i H al grup presentat per:

$$K \times H = \langle\ S,T\ |D,E,\ st = ts\ \forall s \in S, t \in T\ \rangle.$$

Aquesta definició és equivalent a:
M és el producte directe de K i H si existeixen homomorfismes $p_H : M \to H$, $p_K : M \to K$ tals que, per tot grup G i per qualsevol par d'homomorfismes $\alpha : G \to H$, $\beta : G \to K$, existeix un únic homomorfisme $\gamma : G \to M$ tal que $\alpha = p_H \circ \gamma$ i $\beta = p_K \circ \gamma$.

Definició 1.2.2 Donats dos grups K i H amb presentacions $K = \langle S|D\rangle$ i $H = \langle T|E\rangle$ i assumint que S i T són disjunts, anomenarem el *producte lliure* de K i H al grup generat per:

$$K * H = \langle\ S \cup T\ |D \cup E\ \rangle.$$

Aquesta definició és equivalent a:
L és el producte lliure de K i H si existeixen homomorfismes $\iota_H : H \to L$, $\iota_K : K \to L$ tals que, per tot grup G i per qualsevol par d'homomorfismes $\alpha : H \to G$, $\beta : K \to G$, existeix un únic homomorfisme $\gamma : L \to G$ tal que $\alpha = \gamma \circ \iota_H$ i $\beta = \gamma \circ \iota_K$.

Suposem ara que H i K tenen un subgrup isomorf, anomenarem M a aquest subgrup. Per tant tenim dues inclusions $\sigma : M \to H$ i $\tau : M \to K$; siguin $A = \sigma(M)$ i $B = \tau(M)$ i volem fer el producte lliure identificant els dos subgrups isomorfs $A = B$ via $\phi = \tau \circ \sigma^{-1}$.

Definició 1.2.3 Donats dos grups K i H amb presentacions $K = \langle S|D\rangle$ i $H = \langle T|E\rangle$ i assumint que S i T són disjunts, i sigui A un subgrup de K isomorf a un subgrup B de H anomenarem el *producte lliure amalgamat per* $A = B$ de K i H al grup generat per:

$$K \underset{A=B}{*} H = \langle\ S \cup T\ |D \cup E, a = \phi(a)\ \forall a \in A\ \rangle.$$

Aquesta definició és equivalent a:

L és el producte lliure de H i K amalgamat pel subgrup M si existeixen $\iota_H : H \to L$ i $\iota_K : K \to L$ tals que $\iota_H \circ \sigma = \iota_K \circ \tau$ i satisfent que, per qualsevol par d'homomorfismes $\alpha : H \to G$ i $\beta : K \to G$ complint $\alpha \circ \sigma = \beta \circ \tau$ on G és un grup qualsevol, existeix un únic homomorfisme $\gamma : L \to G$ tal que $\alpha = \gamma \circ \iota_H$ i $\beta = \gamma \circ \iota_K$.
Normalment notarem $A = \sigma(M) \leq H$ i $B = \tau(M) \leq K$. Notarem el producte lliure de H i K amalgamat per $A = B$ com a $H \underset{A=B}{*} K$ (i els morfismes σ i τ usats per a la identificació es donaran per sobreentesos).

Definició 1.2.4 Siguin dos grups H i K. Anomenarem *paraula alternada* en el producte lliure $H * K$ a una paraula $h_1k_1 \cdots h_mk_m$ on cada $h_i \in H$ i cada $k_i \in K$.

Direm que una paraula $h_1k_1 \cdots h_mk_m$ en $H \underset{A=B}{*} K$ és reduïda si $h_i \notin A$ i $k_i \notin B$ per tot $i = 1, \ldots, m$.

Definició 1.2.5 Sigui $G = H \underset{A=B}{*} K$. Siguin Y i Z dos conjunt de representants elegits de les classes laterals de H mòdul A i de K mòdul B, respectivament. Un element és una *forma normal* si és de la forma $ah_1k_1 \cdots h_mk_m$ amb $1 \neq_G h_i \in Y$, $1 \neq_G k_i \in Z$ i a és un element de $A = B$.

Lema 1.2.6 ([**1**]) *Sigui $h_1k_1 \cdots h_mk_m$ una expressió alternada de $G = H \underset{A=B}{*} K$. Si $h_1k_1 \ldots h_mk_m =_G 1$ aleshores $h_1k_1 \cdots h_mk_m$ no és reduïda.*

Seguint amb la notació de la definició 1.2.5 tenim el teorema següent:

Teorema 1.2.7 (Normal form Theorem for amalgams) *Tot element de* $G = H \underset{A=B}{*} K$ *és igual a una única forma normal reduïda* $ah_1k_1 \dots h_mk_m$ *amb* $1 \neq_G h_i \in Y$, $1 \neq_G k_i \in Z$ *i* $a \in A$.

Demostració. Primer provarem que tot element de G és igual a una forma normal reduïda:
Sigui w una paraula qualsevol de G, aplicant reduccions suposem que tenim una paraula reduïda de w de la forma $h_1k_1 \cdots h_mk_m$ tal que cap h_i ni cap k_i pertanyen a $A = B$, o sigui, començant de dreta a esquerra sigui i l'index del primer element h_i o k_i que no sigui dels conjunts Y o Z (suposarem que es h_i), suposem que tenim una paraula alternada $h_1k_1 \cdots k_{i-1}h_ik_i \cdots h_mk_m$ amb tots els termes a la dreta de h_i són de Y o de Z i diferents de 1. Escrivim $h_i = ah_i'$ on $a \in A$ i $h_i' \in Y$. Com que la paraula és reduïda $h_i \notin A$ i per tant $h_i' \neq 1$. Sigui $b = \phi(a) \in K$ on ϕ és l'isomorfisme de A a B. Substituim ah_i' per bh_i' en la paraula i agrupem b amb la k_i' i tenim $h_1k_1 \dots h_{i-1}(k_{i-1}b)h_i'k_i \dots h_mk_m$, segueix sent reduïda ja que $k_{i-1} \notin B$ implica que $k_{i-1}b \notin B$. Repetint aquest procés per inducció obtenim una forma normal.
L'unicitat es demostra suposant que existeixen dues formes normals d'una mateixa paraula i veient que són la mateixa.
Si tenim dues formes normals d'una mateixa paraula aleshores:

$$ah_1k_1 \cdots h_mk_m =_G a'h_1'k_1' \cdots h_n'k_n'$$

i per tant:

$$ah_1k_1 \cdots h_m(k_mk_n'^{-1})h_n'^{-1} \cdots k_1'^{-1}(h_1'^{-1}a'^{-1}) =_G 1$$

aquesta paraula segueix sent alternada i pel lema 1.2.6 no és reduïda i per tant $k_mk_n'^{-1} \in B$ i aleshores $k_m = k_n'$ ja que els dos pertanyen a Z. Eliminant $k_mk_n'^{-1}$ i repetint l'argument, obtenim que cada $k_i' = k_i$, cada $h_i' = h_i$ i $n = m$, finalment $a = a'$. □

El resultat següent serà important en la demostració del Main Technical Lema:

Teorema 1.2.8 (Inclusió [**1**]) *Sigui* $G = H \underset{A=B}{*} K$ *un producte lliure amalgamat. Aleshores* ι_H *i* ι_K *indueixen monomorfismes de* H *i* K *en* G.

Demostració. Ho provarem per a ι_h i H (per a K és el mateix).
Sigui $h \in H$ i sigui $\iota_H(h)$ la seva imatge. Com que $h = ah'$ per certs $a \in A$ i $h' \in Y$, veiem que la seva forma normal $\iota_H(h)$ és ahí. Això automàticament prova que ι_H és

injectiu: si $h_1 = a_1 h_1'$ i $h_2 = a_2 h_2'$ complissin $\iota_H(h_1) = \iota_H(h_2)$ llavors aquesta imatge comú en G admetria les dues formes normals $a_1 h_1'$ i $a_2 a_2'$. Per la unicitat de la forma normal, $a_1 = a_2$ i $h_1' = h_2'$ i, per tant $h_1 = a_1 h_1' = a_2 h_2' = h_2$. □

Capítol 2
Problemes fonamentals de Dehn

En aquest treball treballarem normalment en grups descrits per una *presentació*, que consisteix en escriure els elements que generen el grup i amb *relacions* que tenen aquests elements.
Una presentació té la forma:

$$\langle\ a_1, a_2, \ldots | R_1, R_2, \ldots\ \rangle$$

Per ser més formals donada una presentació $P = \langle S|D\rangle$ on S són els *generadors* i D són les *relacions*, el *grup presentat per* P, $gp(P)$, és el grup F_S/N_D on F_S és el grup lliure amb base S i N_D és la *clausura normal* de D en F_S, que és el subgrup normal més petit que conté D. Nosaltres no distinguirem entre la presentació d'un grup i el grup.

Definició 2.1 Sigui X un conjunt. Un subconjunt $A \subseteq X$ s'anomena *decidible* si existeix un algoritme que, donat un element $x \in X$ decideix si x pertany a A o no.

Definició 2.2 Un conjunt s'anomena *enumerable* si existeix un algoritme que llista tots i cada un dels elements del conjunt.

Definició 2.3 Un grup G es diu que és *finitament generat* si admet una presentació $G = \langle S|D\rangle$ amb $|S| < \infty$.

Definició 2.4 Un grup G es diu que és *finitament presentable* si admet una presentació $G = \langle S|D\rangle$ amb $|S| < \infty$ i $|D| < \infty$.

Definició 2.5 Un grup G es diu que és *recursivament presentat* si admet una presentació $G = \langle S|D\rangle$ amb $|S| < \infty$ i $D \subseteq F_S$ és enumerable.

2.1 Problemes de Dehn

Sigui $G = \langle S|D\rangle$ un grup finitament presentat. Sigui $\phi : G \to G$ un automorfisme donat per les imatges dels generadors. Sigui $F \leq G$.
Els següents problemes són els problemes clàssics que utilitzarem en aquest treball:

- El **problema de la paraula** $WP(G)$ (word problem) per a G: donat un paraula w en S, decidir si aquesta paraula representa l'element trivial en G.
- El **problema de conjugació** $CP(G)$ (conjugacy problem) per a G: donades dues paraules u, v en S, decidir si representen dos elements conjugats de G. Aquest problema donaria la solució al $WP(G)$.
- El **problema de conjugació ϕ-torçada**, $TCP_\phi(G)$ (twisted conjugacy problem) per a G: donades dues paraules u, v en S, decidir si representen elements conjugats ϕ-torçats de G, és a dir, si existeix $g \in G$ tal que $v = \phi(g)^{-1}ug$. Si $\phi = I$ el $TCP_I(G)$ és igual al $CP(G)$.
- El **problema de la pertinença** de F en G, $MP(F, G)$ (membership problem): donada una paraula w en S, decidir si l'element de G que representa pertany a F o no.

Sigui ara A un subgrup de $Aut(G)$ i sigui $N \trianglelefteq G$ un sugrup normal. Finalment presentarem uns problemes més especifics però igualment importants per a aquest treball:

- El **problema de la intersecció de les classes laterals** $CIP(G)$ (coset intersection problem) per G: donats dos conjunts finits d'elements $\{a_1, \ldots, a_r\}$ i $\{b_1, \ldots, b_s\}$ en G i dos elements $x, y \in G$ decidir si les classes laterals xA i yB s'intersequen, on $A = \langle a_1, \ldots, a_r\rangle$ i $B = \langle b_1, \ldots, b_s\rangle \leq G$.
- El **problema de conjugació per a G restringit a N**, $CP_N(G)$ (conjugacy problem for G restricted to N): donats dos elements de $u, v \in N$, decidir si són conjugats en G.
- El **problema de l'òrbita** per A, $OD(A)$ (orbit decidability problem): donats dos elements $u, v \in G$, decidir si existeix un $\varphi \in A$ tal que $\varphi(u)$ i v són conjugats en G.
- El **problema d'isomorfisme** (isomorphism problem): donades dues presentacions finites, decidir si els grups que presenten són isomorfs.

Hem de notar que els problemes originals de Dehn eren tres: el problema de la paraula, el problema de la conjugació i el problema d'isomorfisme. Amb el temps aquests problemes han donat lloc a multitud de variancions. Les recollides aquí seran les que utilitzarem.

2.2 Part positiva d'alguns problemes de decisió

Sempre que els grups vénen donats per presentacions finites i els morfismes vénen donats per les imatges dels generadors, la *part positiva* d'algun dels problemes presentats en la secció 2.1 sempre es pot resoldre, és a dir, si el problema consisteix a dir si es compleix una propietat per a una entrada donada i aquesta es compleix, l'algoritme per resoldre la part positiva acabarà afirmant-ho. Per contra, si no es compleix la propietat aquest algoritme no acabarà mai.

Si tinguérem un algoritme per a la part positiva i un per a la part negativa, el problema seria resoluble.
En els problemes presentats, la part positiva sempre es pot resoldre. Donats $G = \langle x_1, \dots, x_n | r_1, \dots, r_m \rangle$ i $F \leq G$ un subgrup donat per un nombre finit de generadors $\{f_1(x_1, \dots, x_n), \dots, f_t(x_1, \dots, x_n)\}$, tenim:

- La **part positiva del problema de la paraula** ($WP^+(G)$) per a G: donada una paraula reduïda en els generadors de G $w(x_1, \dots, x_n) \in G$, de la qual sabem que representa l'element trivial, trobar una expressió de w en termes de les relacions r_i. Enumerant la clausura normal $R = \langle\langle r_1, \dots, r_m \rangle\rangle$ en el grup lliure $\langle x_1, \dots, x_n | \rangle$ i mirant un per un si els elements són iguals a la paraula w l'algoritme acabarà.
- La **part positiva del problema de conjugació** ($CP^+(G)$) per G: donades duess paraules $u(x_1, \dots, x_n), v(x_1, \dots, x_n)$ de les quals sabem que representen elements conjugats, trobar $w(x_1, \dots, x_n)$ tal que $w^{-1}uw =_G v$. Per resoldre-ho, com abans, enumerem tots els elements del grup lliure $\langle x_1, \dots, x_n | \rangle$ i apliquem el $WP^+(G)$ a cada $v^{-1}w^{-1}uw$.
- La **part positiva del problema de conjugació torçada** ($(TCP^+(G))$) per a G es defineix i es resol de la mateixa forma que el $CP^+(G)$.
- La **part positiva del problema de la pertinença** ($MP^+(F, G)$) per F en G: donada una paraula $w(x_1, \dots, x_n)$ de la qual sabem que pertany a F, expressar-la en termes dels f_i. De la mateixa manera que abans, es resol enumerant totes

les paraules en les f_i's, i una per una, mirant si representa el mateix element que w en G (amb el $WP^+(G)$ que hem donat més amunt.

2.3 Problema de la paraula

En aquesta secció demostrarem que existeixen grups finitament presentats amb problema de la paraula irresoluble. Començarem parlant de conjunts decidibles i enumerables de naturals que després utilitzarem per obtindre resultats. El primer resultat dóna la relació entre aquests dos conceptes:

Teorema 2.3.1 *Sigui $S \subseteq \mathbb{N}$, aleshores:*

(1) S és decidible $\Rightarrow$ S és enumerable.
(2) S és decidible $\Leftrightarrow$ S i S^c són enumerable (on S^c és el complementari de S).

Demostració. S decidible $\Rightarrow \exists$ un algoritme A tal que $\forall n \in \mathbb{N}$ ens diu si n pertany a S o no. Fem un algoritme que recorri tots els naturals i que executi A per cada un d'ells. El posarem a la llista si pertany a S i si no, no el posarem. Tenim la primera afirmació.
És obvi que si S és decidible aleshores S^c també és decidible. Com S^c és decidible, també és enumerable per (1). Per l'altra implicació, per un $n \in \mathbb{N}$, engeguem els dos algoritmes d'enumeració al mateix temps, hi haurà un (i només un) algoritme d'enumeració que en algun moment ens donarà el nostre n. □

L'apartat (1) està contingut en (2) però hem volgut emfatitzar que el reciproc de (1) no és cert. Això està a la base de la construcció que farem d'un grup amb problema de la paraula irresoluble.

Comentari 2.3.2 Sigui $G = \langle X|R\rangle$ una presentació finita. Dins del grup lliure $F = \langle X|\rangle$ (que és enumerable) considerem el subconjunt $S = \{w \in F | w =_G 1\}$. Aleshores:

(1) S és enumerable.
(2) S és decidible $\Leftrightarrow$ el problema de la paraula de G es resoluble.

(1) és justament la solució del $WP^+(G)$ i (2) és per definició.

Per tant, darrera de tot grup amb problema de la paraula irresoluble hi ha un conjunt enumerable i no decidible. És a dir, un conjunt S enumerable però tal que S^c no és enumerable.

Primer demostrarem que a $\mathbb{N}$ existeixen subconjunts enumerables tals que el seu complementari no ho sigui. I amb un d'aquests conjunts fabricarem un grup finitament presentat amb problema de la paraula irresoluble.

Definició 2.3.3 Una funció $f : \mathbb{N} \to \mathbb{N}$ (amb $Dom(f) \subseteq \mathbb{N}$ però no necessàriament $Dom(f) = \mathbb{N}$) és *computable* si $\exists A$ algoritme tal que donat $n \in \mathbb{N}$ respongui $f(n)$ si $n \in Dom(f)$ i que no fagi res en cas contrari.

Teorema 2.3.4 $\exists S \subseteq \mathbb{N}$ *enumerable però no decidible.*

Demostració. Es poden enumerar totes les funcions computables, anem a veure-ho: Si fixem un llenguatge qualsevol, un algoritme és un text finit en els símbols permesos pel llenguatge, numerem tots els possibles textos per ordre lexicogràfic i llencem tots els que no siguin sintàcticament correctes, els que van quedant seran una llista exhaustiva de tots els algoritmes que existeixen. Considerant aquesta enumeració ens quedem només amb els algoritmes que computen funcions (és a dir, que accepten naturals com a entrada i que retornen un natural o rés), i així obtenim una llista exhaustiva de totes les funcions computables $f_1, f_2, \ldots$. Fem la tabla següent:

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \vdots \\ A_3 & f_3 & f_3(1) & f_3(2) & f_3(3)\ldots \\ A_2 & f_2 & f_2(1) & f_2(2) & f_2(3)\ldots \\ A_1 & f_1 & f_1(1) & f_1(2) & f_1(3)\ldots \end{array}$$

on $f_i(j)$ pot ser un natural o $*$ si $j \notin Dom(f_i)$. Considerem ara el conjunt:

$$S = \{n \in \mathbb{N} | f_n(n) \neq *\} = \{n \in \mathbb{N} | n \in Dom(f_n)\} \subseteq \mathbb{N}.$$

Aquest conjunt és enumerable però no decidible. En efecte, l'enumerem de la següent manera: Per cada $n = 1, 2, 3, \ldots$ construim l'algoritme A_n tal com ho hem descrit abans, l'engeguem amb n, si ens dóna un natural, posarem n a la llista, i si ens dona $*$ no.
Però S no és decidible. Suposem que ho fos i que A fos un un algoritme per decidir si $n \in S$. Aleshores la funció:

$$g(n) = \begin{cases} f_n(n) + 1 & \text{si } n \in S \\ 1 & \text{si } n \notin S \end{cases}$$

seria computable. Per tant estaria a la nostra llista i per tant $g = f_k$ per a algun k. Però $g(k) \neq f_k(k)$ ja que o bé seria $1 \neq *$ o bé $f_k(k) + 1 \neq f_k(k)$. La contradicció ve de suposar S decidible, per tant S no és decidible. □

Ara construirem un grup amb problema de la paraula irresoluble. Aquest grup ve donat per la construcció de Higman:

Sigui $S \subseteq \mathbb{N}$ un conjunt enumerable però no decidible. Agafem $F_2 = \langle a, b| \rangle$, $F_2 = \langle c, d| \rangle$ i considerem el producte lliure amalgamat sobre els subgrups:

$$H = \langle a^{-i}ba^i | i \in S \rangle \leq F_2,\ K = \langle c^{-i}dc^i | i \in S \rangle \leq F_2$$

identificant $a^{-i}ba^i = c^{-i}dc^i$:

$$G = F_2 \underset{H=K}{*} F_2 = \langle a, b, c, d | a^{-i}ba^i = c^{-i}dc^i, i \in S \rangle$$

Teorema 2.3.5 *El problema de la paraula de G és irresoluble.*

Demostració. Necessitarem dos resultats per demostrar el teorema:

I) a F_2, $\{a^iba^{-i}\ i \in \mathbb{N}\}$ és una base del subgrup que genera (que és $\cong F_\infty$), per tant si treiem uns quants generadors obtenim un factor lliure:
$$H = \langle a^{-i}ba^i\ i \in S \rangle \leq \langle a^{-i}ba^i\ i \in \mathbb{N} \rangle$$
i clarament $a^{-i}ba^i \in H \Leftrightarrow i \in S$.
$\{a^iba^{-i}\ i \in \mathbb{N}\}$ és una base ja que si multipliques aquestos generadors i els seus inversos entre ells mai donarà l'element trivial ja que els b's centrals mai es cancel·laran.

II) Sigui $G = H \underset{A=B}{*} K$ i $w = a_1b_1 \cdots a_rb_r$ una expressió alternada de G, $a_i \in H, b_i \in K$. Si $w =_G 1$ aleshores $\exists i \in \mathbb{N}$ tal que $a_i \in A$ ó $b_i \in B$.
Pel lema 1.2.6.

Suposem que el problema de la paraula de G és resoluble. Donat $i \in \mathbb{N}$ apliquem l'algoritme del problema de la paraula per decidir si $a^{-i}ba^ic^id^{-1}c^{-i} =_G 1$.

- si $a^{-i}ba^ic^id^{-1}c^{-i} \neq_G 1 \Rightarrow i \notin S$ clarament.

- si $a^{-i}ba^ic^id^{-1}c^{-i} =_G 1 \Rightarrow$ com que $(a^{-i}ba^i)(c^id^{-1}c^{-i})$ és una forma alternada, per II deduïm que $a^{-i}ba^i \in H$ ó $c^id^{-1}c^{-i} \in K$, i per I, en ambdós casos es dedueix $i \in S$.

I per tant tindriem un algoritme per decidir S, per tant S seria decidible. La contradicció ve de suposar que G té problema de la paraula resoluble, per tant G té problema de la paraula irresoluble. □

Aquest grup és un grup finitament generat amb problema de la paraula irresoluble. Per passar d'un grup finitament generat a un finitament presentat necessitem el clàssic Higman's embedding theorem.

Teorema 2.3.6 (Higman's Embedding Theorem [**5**]) *Un grup H finitament generat es pot incloure dins d'un grup finitament presentat si i només si H està presentat recursivament.*

Corol·lari 2.3.7 *$\exists G$ finitament presentat tal que el seu problema de la paraula és irresoluble.*

Demostració. El grup G d'abans era un grup amb 4 generadors i presentat recursivament. Pel Higman's Embedding Theorem G es pot incloure en un grup finitament presentat G'. Com G té problema de la paraula irresoluble G' també tindrà problema de la paraula irresoluble. □

Capítol 3
Propietats de Markov

En aquest capítol presentarem les propietats de Markov, les quals són molt senzilles de presentar però que veurem que no seran *recursivament reconeixibles*.

3.1 Propietats de Markov

Definició 3.1.1: Una propietat abstracta P dels grups finitament presentats és una *Propietat de Markov* si existeixen dos grups finitament presentats G_+ i G_- tals que:

(1) G_+ té la propietat P.
(2) Si G_- està inclos dins d'un grup H, aleshores H no té la propietat P.

Aquests grups G_+ i G_- s'anomenen respectivament el *test positiu* i el *test negatiu* de la propietat de Markov P.

Definició 3.1.2 Una propietat abstracta P dels grups finitament presentats és *hereditària* si per a tot grup G amb aquesta propietat, i tot $A \leq G$, A també té la propietat P.

Lema 3.1.3 *Si P és una propietat hereditària no trivial, aleshores P és una propietat de Markov.*

Demostració. Si P no es trivial, existeix un grup G_+ que la té i un grup G_- que no la té. Però G_- està inclòs en un altre grup H finitament presentat, H no pot tenir la propietat P perquè P és hereditària. Per tant P és una propietat de Markov amb tests G_+ i G_-. □

Lema 3.1.4 Si $\emptyset \neq P_1 \subseteq P_2$ són propietats dels grups finitament presentats i P_2 és una propietat de Markov, aleshores P_1 és una propietat de Markov.

Demostració. Sigui G_- el test negatiu de P_2 i sigui un grup K finitament presentat que té la propietat P_1. Aleshores P_1 és una propietat de Markov amb tests K i G_-. □

Definició 3.1.5 Una propietat abstracta P és *recursivament reconeixible* si existeix un mètode efectiu per decidir si, donada una presentació finita π, el grup que presenta té la propietat P.

Teorema 3.1.6 *Les següents propietats dels grups finitament presentats són propietats de Markov:*

- *Ser isomorf al grup trivial.*
- *Ser finit.*
- *Ser resoluble.*
- *Ser lliure.*
- *Ser simple.*
- *Tindre problema de la paraula irresoluble.*
- *Ser nilpotent.*
- *Ser abelià.*

Teorema 3.1.7 (Adian-Rabin): *Si P és una propietat de Markov dels grups finitament presentats, aleshores P no és recursivament reconeixible.*

Demostració. Per demostrar aquest teorema, suposarem que P és una propietat de Markov, i G_+ i G_- són els seus tests, també tindrem un grup U finitament presentat amb problema de la paraula irresoluble.
Construirem una família recursiva de presentacions finites $\{\pi_w | w \in U\}$ indexada per les paraules de U tal que si $w =_U 1$ aleshores $\pi_w \cong G_+$ mentres que si $w \neq_U 1$ aleshores $G_- \leq \pi_w$. Per tant $\pi_w \in P \iff w =_U 1$. I com que U té problema de la paraula irresoluble tindrem que P no és recursivament reconeixible.

Per a construir aquesta família de presentacions i així demostrar el teorema utilitzarem el lema següent:

Lema 3.1.8 (Main Technical Lemma): *Sigui K un grup donat per una presentació d'un conjunt finit o numerable de generadors i relacions.*

$$K = \langle x_1, x_2, \ldots \mid R_1 = 1, R_2 = 1, \ldots \rangle.$$

Per qualsevol paraula w donada en els generadors de K, sigui L_w el grup amb la

presentació donada per K afegint tres nous generaors a, b, c amb les relacions:

$$a^{-1}ba = c^{-1}b^{-1}cbc \tag{1}$$

$$a^{-2}b^{-1}aba^{-2} = c^{-2}b^{-1}cbc^{-2} \tag{2}$$

$$a^{-3}[w, b]a^3 = c^{-3}bc^3 \tag{3}$$

$$a^{-(3+i)}x_iba^{(3+i)} = c^{-(3+i)}bc^{(3+i)} \tag{4}$$

on $[w, b]$ és el commutador de w i b. Aleshores:

1) Si $w \neq_K 1$ aleshores $K \leq L_w$ per la injecció canònica $(x_i \mapsto x_i)$.
2) La clausura normal de w en L_w és tot L_w; en particular, si $w =_K 1$ aleshores $L_w \cong 1$.
3) L_w està generat pels elements b i ca^{-1}.

Si la presentació de K és finita, aleshores la presentació L_w és també finita.

DEMOSTRACIÓ. Suposem primer que $w \neq_K 1$. Considerem el grup lliure $\langle b, c|\rangle$, i considerem el subgrup C generat per b i pels termes de la dreta de les equacions (1),...,(4), aquests elements són generadors lliures de C.
De la mateixa manera, fem el producte lliure $K * \langle a, b|\rangle$, i considerem el subgrup A d'aquest producte generat per b i els termes de la esquerra de les equacions (1),...,(4). Utilitzant que $w \neq_K 1$ es pot veure que aquests elements són generadors lliures de A. Tal com l'hem definit, és clar que L_w és el següent producte amalgamat:

$$L_w = (K * \langle a, b \mid \rangle) \underset{A=C}{*} \langle b, c \mid \rangle$$

Notem que la primera relació de l'amalgama, $b = b$, fa que hi hagi una sola lletra b, no dues de diferents.
Així si $w \neq_k 1$ $K \leq L_w$ i tenim la primera afirmació demostrada.
Sigui ara N_w la clausura normal de w en L_w. $[w, b] \in N_w$ i per la equació (3), $b \in N_w$. I les equacions (1) i (2) ens diuen que a, b i c estan dins de N_w. I en la equació (4) cada x_i pot estar expressat en termes de a, b, c i per tant $x_i \in N_w$ per a $i = 1, \ldots$. Com cada generador de L_w està en N_w tenim que $L_w = N_w$. Si $w =_K 1$ aleshores $w =_{L_w} 1$ perquè totes les relacions de K són també relacions de L_w i per tant $1 = N_w = L_w$.
Finalment, sigui M el subgrup de L_w generat per b i ca^{-1}; de l'equació (1) tenim que $c = b(ca^{-1})b(ca^{-1})^{-1}b^{-1}$ i per tant $c \in M$, però aleshores $a \in M$. Finalment de l'equació (4) podem expressar x_i en termes de a, b, c i per tant $x_i \in M$ per a $i = 1, \ldots$, per tant $M = L_w$ i obtenim que L_w és un grup generat per dos elements. □

Utilitzant aquest lema completarem la demostració del teorema de Adian-Rabin. Podem assumir que els tres grups finitament presentats que tenim U, G_+ i G_- estan presentats de la forma següent:

$$U = \langle y_1, \dots, y_k | Q_1 = 1, \dots Q_q = 1 \rangle$$
$$G_+ = \langle u_1, \dots, u_m | S_1 = 1, \dots S_s = 1 \rangle$$
$$G_- = \langle v_1, \dots, v_n | T_1 = 1, \dots T_t = 1 \rangle$$

Sigui $K = U * G_-$ el producte lliure de U i G_-, presentat com la unió de les presentacions. Com que U té problema de la paraula irresoluble, K també tindrà problema de la paraula irresoluble. U i G_- estan inclosos en K per la injecció canònica. Per qualsevol paraula w(en generadors de U) tindrem una presentació L_w com la que hem donat en el Main Techincal Lemma. També formarem el producte lliure $L_w * G_+$, i considerem-ne la presentació π_w obtinguda unint les de L_w i de G_+.
Si $w \neq_U 1$ aleshores $w \neq_K 1$ i, pel lema anterior, $G \leq K \leq \pi_w$ i per tant, $\pi_w \notin P$. Per un altre costat, si $w =_U 1$ aleshores $w =_K 1$ i $L_w \cong 1$ i per tant $\pi_w \cong G_+$, i tindrem que $\pi_w \in P$.
Tenim doncs, una família de presentacions $\{\pi_w | w \in U\}$ que té la propietat que $\pi_w \in P \Leftrightarrow w =_U 1$. I com que U té problema de la paraula irresoluble hem acabat la demostració. □

3.2 Conseqüències del Main Technical Lemma

El Main technical lema que hem utilitzat ens donarà també altres resultats.

Corol·lari 3.2.1 (Higman, Neuman) *Tot grup K contable es pot incloure dins d'un grup L generat per dos elements. Si K està presentat amb n relacions, aleshores L es pot presentar amb n relacions.*

Demostració. Com que K és contable, es pot presentar com l'utilitzat en el Main Technical Lemma. Formem L com en el lema però ometent les relacions (2) i (3). Només l'equació (3) inclou w i ni (2) ni (3) s'utilitzen en la demostració de que L està generat per dos elements. Tenim que $K \leq L$ i L està generat pels dos elements b i ca^{-1}. Tenim la primera afirmació.
L'equació (1) del lema defineix c en termes d'aquests dos generadors. Podem obtindre

a com a reducció de $(ca^{-1})^{-1}c$. En l'equació (4) tenim x_i en termes dels generadors donats. Per tant podem eliminar aquestes dues relacions deixant només les R_j que ja teniem però en termes dels generadors b i ca^{-1}. □

Combinant la prova del corol·lari 3.2.1 i el Higman's Embedding Theorem obtenim el següent corol·lari.

Corol·lari 3.2.2 *Si el grup K es pot presentar per un conjunt recursiu de generadors subjecte a un conjunt recursiu i enumerable de relacions, aleshores K es pot incloure en un grup L finitament presentat generat per dos elements. En particular els generadors de K estan representats per un conjunt recursiu de paraules de L.*

Demostració. K es pot incloure en un grup generat per dos elements i recursivament presentat, l'anomenarem L_1. Pel Higman Embedding Theorem aquest grup L_1 es pot incloure en un grup K_1 finitament presentat. Aplicant un altre cop el corol·lari, K_1 es pot incloure en un grup L generat per dos elements i finitament presentat. □

Definició 3.2.3 Siguin P i Q dos conjunts disjunts de nombres naturals. Aquest parell de conjunts s'anomenen *recursivament inseparables* si no existeix cap conjunt decidible $R \subseteq \mathbb{N}$ tal que $P \subseteq R$ i $Q \cap R = \emptyset$.

Comentari 3.2.4 Aquests conjunts existeixen ja que si tenim un conjunt A no decidible, A i A^c són conjunts recursivament inseparables.

Necessitarem d'aquesta definició i dels tres resultats obtinguts per obtindre el resultat següent:

Corol·lari 3.2.5 *Existeix un grup G finitament presentat tal que tot grup quocient no trivial de G té problema de la paraula irresoluble.*

Demostració. Siguin dos conjunts de naturals P i Q enumerables i recursivament inseparables. Podem suposar que $0 \in P$ i $1 \in Q$. Definim K_0 el grup presentat com:

$$K_0 = \langle e_0, e_1, \dots \mid e_0 = e_i \ \forall i \in P,\ e_1 = e_j \ \forall j \in Q \rangle$$

Com que P i Q són enumerables, el corol·lari anterior implica que K_0 es pot incloure dins d'un grup finitament presentat K generat per dos elements. Seguirem amb la notació e_k per a la imatge del generador e_k per l'aplicació que inclou el grup K_0 al K. Utilitzem el Main Technical Lemma a K amb la paraula $e_0e_1^{-1}$ i obtenim el grup finitament presentat $G = L_{e_0e_1^{-1}}$. Com que P i Q són disjunts, $e_0 \neq_K e_1$ o equivalentment $e_0e_1^{-1} \neq_K 1$, per tant, $K \leq L_{e_0e_1^{-1}}$.
Sigui ara H un grup quocient no trivial de G (vist amb els mateixos generadors que G). Per la segona afirmació del Main Technical Lemma tenim, que la clausura normal de $e_0e_1^{-1}$ és tot G, per tant $e_0 \neq_H e_1$, ja que si no, H seria trivial. Definim $R = \{i | e_0 =_H e_i\}$. Com que H és quocient de G tindrem que $P \subseteq R$. Però com que $e_0 \neq_H e_1$ tindrem que $Q \cap R = \emptyset$. I com P i Q són recursivament inseparables R no és recursiu. Ara $\{e_k\}$ és un conjunt recursiu de paraules en termes dels generadors de H i per tant si H tinguera problema de la paraula resoluble tindriem que R seria recursiu. Per tant H té problema de la paraula irresoluble. □

Recordem el lema de Zorn.

Lema 3.2.6 (Zorn): *Cada conjunt parcialment ordenat en el que tota cadena (i.e. subconjunt totalment ordenat) té una cota superior, conté com a mínim un element maximal.*

Corol·lari 3.2.7 *Tot grup contable K es pot incloure en un grup simple generat per dos elements.*

Demostració. Si $K \cong 1$ la conclusió és obvia. Suposem que $K \ncong 1$ i siguin $x_1, x_2, \ldots$ la llista de tots els elements no trivials de K. Agafem K presentat amb aquests generadors. Formem un grup L com en el Main Technical Lemma exceptuant les equacions (3) i (4) les quals les remplaçarem respectivament per:

$$a^{-(3+2i)}[x_i, b]a^{(3+2i)} = c^{-(3+2i)}dc^{(3+2i)}$$
$$a^{-(4+2i)}x_iba^{(4+2i)} = c^{-(3+2i)}dc^{(3+2i)}$$

Per a $i = 1, 2, \ldots$, notem que $[x_i, b]$ té ordre infinit ja que $x_i \neq_K 1$. Amb un argument anàleg al del Main Technical Lemma (part 1) $K \leq L$.
Pel lema de Zorn elegim un subgrup normal N de L maximal respecte a la propietat $K \cap N = 1$. La clausura normal en L de qualsevol x_i conté $[x_i, b]$ i d i per tant és tot L. Per tant tenim que L/N és un grup simple generat per dos elements que conté una còpia isomorfa a K. □

Capítol 4
Problemes de decisió

En aquest capítol estudiarem primer com es comporten els problemes irresolubles en el producte directe, i finalment estudiarem algun resultat interesant en grups finitament presentats.

4.1 Problemes de decisió en productes directes

El Lema següent serà clau per demostrar tots els resultats següents.

Lema 4.1.1 *Sigui M un grup amb un conjunt de generadors $\{s_1, \ldots, s_n\}$ tenint un grup quocient H amb la presentació donada:*

$$H = \langle\ s_1, \ldots, s_n \mid R_1 = 1, \ldots, R_m = 1\ \rangle$$

Sigui $G = M \times M$ el grup format pel producte directe i sigui L_H el subgrup de G generat pels elements:

$$(s_1, s_1), (s_2, s_2), \ldots, (s_n, s_n)$$
$$(R_1, 1), (R_1, 1), \ldots, (R_m, 1)$$

Aleshores per qualsevol par de paraules u, v en generadors,

$$(u, v) \in L_H \Leftrightarrow u =_H v$$

Demostració. Clarament si $(u, v) \in L_H$ aleshores $u =_H v$ ja que és veritat per cada un dels generadors de L_H.
Per l'altra implicació, suposem $w =_H 1$. Aleshores

$$w =_M \prod_{k=1}^{r} X_k(s_i)^{-1} R_{j_k}^{\epsilon_k} X_k(s_i)$$

Per a certes paraules X_k en els generadors donats. Però en $G = M \times M$ tenim:

$$(w, 1) =_G \prod_{k=1}^{r} X_k((s_i, s_i))^{-1}(R_{j_k}, 1)^{\epsilon_k} X_k((s_i, s_i)) \in L_H.$$

Si suposem que $u =_H v$ aleshores $uv^{-1} =_H 1$ i per tant $(uv^{-1}, 1) \in L_H$. Ja que L_H conté els (v, v), tindrem $(u, v) \in L_H$. □

Teorema 4.1.2 *Sigui M un grup finitament presentat que té un grup quocient H amb problema de la paraula irresoluble. Aleshores el grup $G = M \times M$ té un subgrup finitament generat L_H tal que $MP(H, G)$ és irresoluble.*

Demostració. Seguirem la mateixa notació que el lema anterior, $(w, 1) \in L_H \Leftrightarrow w =_H 1$. Com que el problema de la paraula per H és irresoluble, el problema de pertinença de L_H en G també és irresoluble. □

Corol·lari 4.1.3 (Mihailova) *Sigui F un grup lliure finitament generat de rang almenys 2. Aleshores el grup $G = F \times F$ té un subgrup L finitament generat tal que el $MP(L, G)$ és irresoluble.*

Teorema 4.1.4 (Miller) *Sigui F un grup lliure amb rang $n \geq 2$ i sigui $G = F \times F$. El problema de decidir si un conjunt donat d'elements genera G és irresoluble.*

Demostració. Aplicarem la demostració del teorema d'Adian-Rabin amb la propietat de Markov "ser trivial", i per tant $G_+ = 1$. Obtenim una família recursiva de presentacions $\{\pi_w | w \in U\}$ indexades per les paraules d'un grup U amb problema de la paraula irresoluble, on $\pi_w \cong 1 \Leftrightarrow w =_U 1$. A més sigui $\{s_1, \ldots, s_n\}$ una base lliure de F i per tant cada presentació π_w es pot escriure amb els mateixos símbols com a generadors. Pel Main Techncal Lema les presentacions es poden donar amb dos generadors, anomenem s_1 i s_2. En el cas $n > 2$ el mateix grup es pot presentar afegint els generadors $\{s_3, \ldots, s_n\}$ i definin les relacions $s_3 = 1, \ldots s_n = 1$. Aplicant el lema 4.1.1 prenem $M = F$ i sigui H_w el subgrup generat pels elements indicats utilitzant la presentació π_w com a H. Sigui $L_w = \pi_w$. Aleshores pel lema i les propietats de π_w tindrem:

$$\begin{aligned} H_w = G &\Leftrightarrow \forall u, v \in F((u,v) \in H_w) \\ &\Leftrightarrow \forall u, v \in F(u =_{L_w} v) \\ &\Leftrightarrow L_w \cong 1 \\ &\Leftrightarrow w =_U 1 \end{aligned}$$

I com U té problema de la paraula irresoluble, s'acaba la demostració. □

Continuant amb la notació de la demostració anterior, sigui N_w el nucli de l'homomorfisme natural de F a L_w. Pel lema 4.1.1 $(y,1) \in H_w \Leftrightarrow y \in N_w$, aleshores $H_w \cap (F \times \{1\}) = (N_w \times \{1\}$. Si $w \neq_U 1$, aleshores de la demostració del teorema de Adian-Rabin sabem que $U \leq L_w$ i en particular H_w és infinit, així que si $w \neq_U 1$ aleshores N_w no està finitament generat.

Podem veure que en $F \times F$ el centralitzador d'un element està finitament generat. També tenim que el centralitzador d'un element $(1,z) \in H_w$ tindrà la forma $N_w \times \mathbb{Z}$. Per tant si $w \neq_U 1$ aleshores el centralitzador d'un element de H_w no serà finitament generat. I per tant si $w \neq_U 1$ aleshores H_w i $G = F \times F$ no són isomorfs, i tindrem el resultat següent:

Teorema 4.1.5 *Sigui F un grup lliure de rang al menys dos i sigui $G = F \times F$. Aleshores el problema per decidir si un conjunt finit de paraules genera un subgrup isomorf a G és irresoluble. Per tant el problema de l'isomorfisme per subgrups de G donats per conjunts finits de generadors és irresoluble.*

Definició 4.1.6 Donat un grup $F = \langle X|R\rangle$ i m automorfismes $\varphi_1, \varphi_2, \ldots, \varphi_m \in Aut(F)$, l'*extensió lliure* de F per $\varphi_1, \ldots, \varphi_m$ és el grup anomenat F-by-F_m:

$$F \rtimes_{\varphi_1,\ldots,\varphi_m} F_m = \langle X, t_1, \ldots, t_m | R, t_i^{-1} x t_i = \varphi_i(x)\ (x \in X, i = 1, \ldots m)\rangle.$$

Ara presentarem la *construcció de Miller*:
Donada una presentació finita $H = \langle s_1, \ldots, s_n | R_1, \ldots, R_m\rangle$. Sigui $F_{n+1} = \langle q, s_1, \ldots, s_n|\rangle$

i sigui $F_{m+n} = \langle t_1, \ldots, t_m, d_1, \ldots, d_n | \rangle$ els grups lliures de rang $n+1$ i $n+m$ respectivament. Considerem ara els automorfismes de F_{n+1} donats per:

$$\begin{aligned} \alpha_i : F_{n+1} &\to F_{n+1} \\ q &\mapsto qR_i \\ s_k &\mapsto s_k \end{aligned}$$

$$\begin{aligned} \beta_j : F_{n+1} &\to F_{n+1} \\ q &\mapsto s_j^{-1} q s_j \\ s_k &\mapsto s_k \end{aligned}$$

per a $i = 1, \ldots, m$ i $j, k = 1, \ldots, n$. Anomenem $A(H) \leq Aut(F_{n+1})$ al grup d'automorfismes que generen. I considerem el grup:

$$G(H) = F_{n+1} \rtimes_{\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n} F_{n+m}$$

Teorema 4.1.7 (Miller [**4**]) *Si H té problema de la paraula irresoluble, aleshores $G(H)$ té problema de conjugació irresoluble.*

4.2 Problema de l'òrbita

Definició 4.2.1 Una *successió exacta curta* és una successió de grups de la forma:

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

tal que:

- α és injectiva.
- $Im(\alpha) = ker(\beta)$.
- β és exhaustiva.

Teorema 4.2.2 *Sigui*

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

una successió exacta curta de grups tal que:

i) F té problema de la conjugació torçada resoluble.

ii) H té problema de conjugació resoluble.

iii) per tot $1 \neq h \in H$, el subgrup $\langle h \rangle$ té index finit en el centralitzador $C_H(h)$, i existeix un algoritme que dona un conjunt finit de representants de les classes laterals $z_{h,1}, \ldots, z_{h,t_h} \in H$,

$$C_H(h) = \langle h \rangle z_{h,1} \cup \ldots \cup \langle h \rangle z_{h,t_h}$$

Aleshores, són equivalents:

(1) el problema de conjugació per a G és resoluble,
(2) el problema de conjugació restringit a F per a G és resoluble,
(3) el subgrup d'accions $A_G = \{\varphi_g | g \in G\} \leq Aut(F)$ té problema de l'òrbita resoluble. On φ_g és l'automorfisme de conjugació $\varphi_g(x) = g^{-1}xg$.

Demostració. Identifiquem F amb $\alpha(F) \leq G$. Per definició $\varphi_g(x) = g^{-1}xg$, per a cada $g \in G$ i $x \in F$. Així donats dos $x, x' \in F$ trobar $g \in G$ tal que $x' = g^{-1}xg$ és el mateix que trobar $\varphi \in A_G$ tal que $x' = \varphi(x)$. Per tant el problema de l'òrbita és resoluble en A_G i per tant (2) i (3) són equivalents. Només cal veure que (2) implica (1) ja que (1) implica (2) clarament.
Assumim (2). Sigui $g, g' \in G$ anem a veure si són conjugats en G.
Utilitzant (ii) podem decidir si $\beta(g)$ i $\beta(g')$ són conjugats en H. Si no ho són, g i g' no seran conjugats en G. (ii) ens dona un element de H que conjuga $\beta(g)$ a $\beta(g')$. Calculant una pre-imatge d'aquest element $u \in G$ és satisfa que $\beta(g^u) = (\beta(g))^{\beta(u)} = \beta(g')$ i canviant g per g^u tenim que $\beta(g) = \beta(g')$. Si aquest element és el element trivial en H (ho podem saber per (ii)), aleshores g i g' estan a $Im(\alpha)$ i aplicant (2) està fet. Per tant ens restringim al cas $\beta(g) = \beta(g') \neq_H 1$.
Ara calculant $f \in F$ tal que $g' = gf$. Com $\beta(g) \neq_H 1$, podem usar (iii) per a calcular els elements $z_1, \ldots, z_t \in H$ tal que $C_H(h) = \langle \beta(g) \rangle z_1 \cup \ldots \cup \langle \beta(g) \rangle z_t$ i aleshores calculant una pre-imatge $y_i \in G$ per cada z_i, $i = 1, \ldots, t$. Comentar que, per construcció, les imatges per β de g i y_i (respectivament $\beta(g)$ i z_i) commuten en H, així que $y_i^{-1}gy_i = gp_i$ per algun element $p_i \in F$.
Com que $\beta(g) = \beta(g')$, tot possible conjugador de g a g' hauria de tenir imatge per β a $C_H(\beta(g))$, per tant ha de ser de la forma $g^r y_i x$ per algun enter r, algun $i \in \{1, \ldots, t\}$, i algun $x \in F$. Per tant:

$$gf = g' = (x^{-1}y_i^{-1}g^{-r})g(g^r y_i x) = x^{-1}(y_i^{-1}gy_i)x = x^{-1}gp_i x$$

Aleshores decidir si g i g' són conjugats en G és transforma a decidir si existeix $i \in \{1, \ldots, t\}$ i $x \in F$ satisfent que $gf = x^{-1}gp_i x$ que és equivalent a $f = (g^{-1}x^{-1}g)p_i x$ i per tant a $f = (\varphi_g(x))^{-1}p_i x$. Com que i pren un nombre finit de valors i la darrera equació significa exactament que f i p_i són conjugats φ_g-torçats, podem resoldre el problema algoritmicament per la hipotesis (i). □

Comentari 4.2.3 Els grups lliures compleixen les tres condicions:

- Els grups lliures tenen TCP resoluble. ([**7**])
- Els grups lliures tenen CP resoluble. És un fet ben conegut i elemental.
- Els grups lliures compleixen la condicio (iii). És també un fet elemental degut a que "per a tot $1 \neq x \in F$, el centralitzador de x és el subgrup cíclic generat per l'arrel maxima de x".

Sigui H un grup amb n generadors i m relacions i sigui $G(H) = F_{n+1} \rtimes_{\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n} F_{n+m}$. Considerem la successió exacta curta següent:

$$1 \to F_{n+1} \xrightarrow{\alpha} F_{n+1} \rtimes_{\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n} F_{n+m} \xrightarrow{\beta} F_m \to 1$$

Aquesta successió exacta curta compleix les condicions del teorema 4.2.2. Pel teorema 4.1.7, si apliquem la construcció de Miller a un grup H presentat amb n generadors i m relacions amb problema de la paraula irresoluble aleshores $G(H)$ té problema de conjugació irresoluble. Per les implicacions (1) $\Leftrightarrow$ (3) tindrem que el subgrup d'accions A_G té problema de l'òrbita irresoluble. On A_G és:

Per les implicacions (1) $\Leftrightarrow$ (3) tindrem que el subgrup d'accions A_G té problema de l'òrbita irresoluble. On A_G és:

$$A_G = \langle \varphi_g \mid g \in G \rangle \leq Aut(F_{n+1})$$

Recordem com hem definit G:

$$\begin{aligned} G &= F_{n+1} \rtimes_{\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n} F_{n+m} \\ &= \langle F_{n+1}, t_1, \ldots, t_m \mid t_i^{-1} x t_i = \alpha_i(x),\ t_i^{-1} x t_i = \beta_j(x),\ (x \in F, i = 1,\ldots,m,\ j = 1,\ldots,n) \rangle \end{aligned}$$

i per tant $A_G = \langle \alpha_1, \ldots, \alpha_m, \beta_1, \ldots \beta_n, Inn(F_{n+1}) \rangle$ on $Inn(F_{n+1})$ són els automorfismes interns de F_{n+1}. Notem també que si $\langle \alpha_1, \ldots, \alpha_m, \beta_1, \ldots \beta_n, Inn(F_{n+1}) \rangle$ té problema de l'òrbita irresoluble el grup $\langle \alpha_1, \ldots, \alpha_m, \beta_1, \ldots \beta_n \rangle$ també tindrà problema de l'òrbita irresoluble.

En 1968 V.Borisov va presentar un grup amb 4 generadors i amb 12 relacions amb problema de la paraula irresoluble, utilitzant el Higman's Embedding Theorem podem incloure aquest grup en un grup generat per dos elements i amb el mateix nombre de relacions. Com aquest grup té problema de la paraula irresoluble, utilitzant la construcció de Miller i el teorema 4.1.7 tenim que existeix un grup F_3-by-F_{14} que té problema de conjugació irresoluble. I pel teorema 4.2.2:

Corol·lari 4.2.4 *Existeix un subgrup $A \leq Aut(F_3)$ generat per 14 elements amb problema de l'òrbita irresoluble.*

Anem a construir exemples de grups així, però en un context abelià, i.e. dins de $Aut(\mathbb{Z}^n) = GL_n(\mathbb{Z})$.

Definició 4.2.5 L'*estabilitzador* $Stab(K)$ d'un subgrup $K \leq F$ donat és el subgrup:

$$Stab(K) = \{\varphi \in Aut(F) | \varphi(k) = k \ \forall k \in K\} \leq Aut(F)$$

Anomenarem *estabilitzador llevat conjugació* de K, $Stab^*(K)$, al conjunt de automorfismes que actuant com a conjugació sobre K.

Teorema 4.2.6 *Sigui F un grup. Siguin dos subgrups $A \leq B \leq Aut(F)$ i un element $v \in F$ tal que $B \cap Stab^*(v) = \{Id\}$. Si $A \leq Aut(F)$ és orbit resoluble, aleshores $MP(A, B)$ es pot resoldre.*

Demostració. Donat un $\varphi \in B \leq Aut(F)$, anem a veure si $\varphi \in A$ o no. Prenem $w = v\varphi$ i observem que:

$$\{\phi \in B | v\phi \sim w\} = B \cap (Stab^*(v) \cdot \varphi) = (B \cap Stab^*(v)) \cdot \varphi = \{\varphi\}$$

Per tant existeix $\phi \in A$ tal que $v\phi$ és conjugat de w en $F \Leftrightarrow \varphi \in A$. I per tant el problema de l'òrbita per $A \leq Aut(F)$ resol $MP(A, B)$. □

Teorema 4.2.7 *Per a $n \geqslant 4, GL_n(\mathbb{Z})$ conté subgrups finitament generats amb problema de l'òrbita irresoluble.*

Demostració. Necessitem uns quants fets clàssics sobre el grup de matrius 2×2; $GL_2(\mathbb{Z})$ admet la presentació:

$$\begin{aligned} GL_2(\mathbb{Z}) &\cong D_4 \underset{D_2}{*} D_6 \\ &= \langle t_4, x_4 | t_4^2, x_4^4, (t_4, x_4)^2 \rangle \underset{\langle t_4 = t_6, x_4^2 = x_6^3 \rangle}{*} \langle t_6, x_6 | t_6^2, x_6^6, (t_6, x_6)^2 \rangle \end{aligned}$$

on $t_4 = t_6 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $x_4 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i $x_6 \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Sigui $\varphi : GL_2(\mathbb{Z}) \to D_{12} = \langle t_{12}, x_{12} | t_{12}^2, x_{12}^{12}, (t_{12}x_{12})^2 \rangle$ donat per $t_4 = t_6 \mapsto t_{12}, x_4 \mapsto x_{12}^3, x_6 \mapsto x_{12}^2$. Si calculem el $ker(\varphi)$ veiem que és lliure amb rang dos i amb basse $P = [x_6, x_4] = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ i $Q = [x_6^2, x_4] = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.
Calculem $\langle P, Q \rangle \cap Stab^*((1,0))$. Tenim que $Stab^*((1,0)) = Stab((1,0)) = \{\left(\begin{smallmatrix} 1 & 0 \\ \pm n & 1 \end{smallmatrix}\right) | n \in \mathbb{Z}\}$ (i podem deixar de costat el cas negatiu perquè ens interessa la intersecció amb

$\langle P, Q\rangle \leq SL_2(\mathbb{Z})$. La imatge de $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right) = x_6^{-1}x_4$ per φ és $x_{12}^{-2}x_{12}^3 = x_{12} \in D_{12}$. Per tant:

$$\langle P, Q\rangle \cap Stab^*((1,0)) = ker(\varphi) \cap Stab((1,0)) = \langle (x_6^{-1}x_4)^{12}\rangle = \langle \left(\begin{smallmatrix}1 & 0\\ 12 & 1\end{smallmatrix}\right)\rangle$$

Elegim un subgrup lliure de rang 2 $\langle P', Q'\rangle \leq \langle P, Q\rangle$ intersecant trivialment amb el grup cíclic $\langle \left(\begin{smallmatrix}1 & 0\\ 12 & 1\end{smallmatrix}\right)\rangle$ a $n \geq 4$, definim:

$$B = \left\langle \left(\begin{array}{c|c} P' & 0 \\ \hline 0 & 1 \end{array}\right), \left(\begin{array}{c|c} Q' & 0 \\ \hline 0 & 1 \end{array}\right), \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P' \end{array}\right), \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q' \end{array}\right) \right\rangle \leq GL_4(\mathbb{Z}) \leq GL_n(\mathbb{Z})$$

que és isomorf a $F_2 \times F_2$. Per construcció B intersecta trivialment amb el centralitzador de $v = (1, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^n$. Finalment utilitzant la construcció de Mihailova, trovem un subgrup $A \leq B$ amb $MP(A, B)$ irresoluble. I per el teorema anterior aplicat a $F = \mathbb{Z}^n$, A és un subgrup de $Aut(\mathbb{Z}^n) = GL_n(\mathbb{Z})$ finitament generat amb problema de l'òrbita irresoluble. □

Bibliografia

[1] Charles F. Miller III, Combinatorial Group Theory *http://www.ms.unimelb.edu.au/ cfm/papers.html.*

[2] Charles F. Miller III, Decision problems for groups - survey and reflections *http://www.ms.unimelb.edu.au/ cfm/papers.html* (2004).

[3] O. Bogopolski, A. Martino, E. Ventura, *Orbit decidability and the conjugacy problem for some extensions of groups*, Transactions of the American Mathematical Society 362 (2010), 2003–2036.

[4] C.F. Miller, III, *On group-theoretic decision problems and their classification*, Annals of Math. Studies 68 (1971).

[5] G. Higman, *Subgroups of finitely presented groups*, Proc. Royal Soc. London Ser. A 262, 455-475 (1961).

[6] K. A. Mihailova, *The occurrence problem for direct products of groups*, Dokl. Akad. Nauk SSSR 119, 1103-1105 (1958).

[7] 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.