Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Grau en Matemàtiques

Treball de fi de grau

Grau de commutativitat de grups finitament generats

Pere Llorens i Domingo

Supervisat per Enric Venura Capell

Juny, 2023

Al meu tutor, l'Enric Ventura, que m'ha guiat en la realització del treball i ajudat en el que feia falta. A la meva família, pel suport en els estudis i per cuidar-me sempre.

Sumari

Aquest treball tracta del grau de commutativitat de grups no abelians finitament generats. Provarem al primer capítol un resultat clàssic de Gustafson per al grau de commutativitat de grups finits, en concret veurem que el grau de commutativitat està fitat per $5/8$ per a grups finits no abelians. Al segon capítol farem la construcció del grup lliure de rang arbitrari i introduirem el concepte de presentació d'un grup, per tal de poder, al tercer capítol, traslladar la noció de grau de commutativitat a grups finitament generats. Finalment, també veurem que per a grups finitament generats de creixement subexponencial i residualment finits, si el grup és no abelià aleshores el seu grau de commutativitat està fitat també per $5/8$, i que el seu grau de commutativitat és positiu si i només si és un grup virtualment abelià.

Índex

Introducció

Donats dos elements qualssevol d'un grup no abelià, en general no commuten. Tot i això, en tot grup hi ha parells d'elements que commuten, com per exemple l'element neutre amb qualsevol altre o un element i el seu invers, i a part d'aquests, n'hi poden haver més. El grau de commutativitat, que serà la definició central d'aquest treball, captura "quant de commutatiu"és un grup. És a dir, que serà una manera de veure quan aquesta commutativitat que hem mencionat té un pes important en el grup o quan és molt residual. I d'aquesta noció en poden sorgir resultats interessants. En particular es pot veure que el grau de commutativitat té fites superiors o inferiors per a certs tipus de grups, i això implica, és clar, que no pot prendre qualsevol valor. Per als grups no abelians, és bastant clar quins elements almenys han de commutar sempre, que són el neutre amb altres elements i els parells d'inversos que ja hem esmentat, però en canvi, no és tan evident quin és el màxim de commutativitat que podem tenir en un grup que sigui no abelià, és per això que les fites superiors del grau de commutativitat poden ser particularment interessants.

Respecte a aquest tema, hi ha articles clàssics com el ja esmentat de Gustafson [8], del qual partirem en aquest treball. Però també en els darrers anys encara hi ha nova recerca al respecte, com en [4] o [5]: en el primer s'estudia el grau de commutativitat dels p-elements de grups finits, i en el segon, el grau de commutativitat de l'anell de grup. Per les característiques d'aquest treball, no veurem els resultats d'aquests últims articles més recents, però sí que ens indiquen que el tema que introduirem és un tema actiu i amb potencial en la recerca.

1. Probabilitat que dos elements d'un grup finit commutin

Aquest primer capítol ens servirà per motivar el treball amb alguns resultats per a grups finits. Començarem amb un seguit de definicions i proposicions preliminars bàsiques de teoria de grups que no demostrarem, però que ens serviran per establir la notació que es farà servir al llarg del treball i presentar eines conegudes, però útils de cara a demostracions posteriors. Seguidament, definirem el grau de commutativitat (per a grups finits) que serà central al llarg del treball i veurem un resultat clàssic de Gustafson [8] per a grups no abelians finits, que estableix que el seu grau de commutativitat és com a molt $5/8$. Prèviament, també veurem, per tal de poder fer la demostració del teorema, alguns resultats referents a les mides que poden tenir els centres d'un grup no abelià [9]. Acabarem el capítol amb un resultat per a grups finits de Gallagher [7] que relaciona els graus de commutativitat d'un grup, dels seus subgrups normals i dels respectius quocients. Aquest ens serà útil més endavant per a la demostració del resultat principal del treball que veurem al tercer capítol, que és un teorema més general que el de Gustafson sobre el grau de commutativitat en grups infinits [1].

1.1 Preliminars

En aquest apartat introductori no inclourem les demostracions, ja que treballarem resultats bàsics i coneguts, per a veure-les, podeu consultar els primers capítols de [10] o els apunts del professor de la UPC Pep Burillo, de l'assignatura d'Estructures Algebraiques del Grau de Matemàtiques [3].

Definició 1.1. Un **grup** és un parell $(G, \cdot)$ on G és un conjunt no buit i $\cdot$ és una operació interna:

$$\begin{aligned} G \times G &\to G \\ (a, b) &\mapsto a \cdot b, \end{aligned}$$

i que satisfà les següents propietats:

- associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in G$,
- element neutre: $\exists 1 \in G$ tal que $g \cdot 1 = 1 \cdot g = g$, $\forall g \in G$,
- tot element té un invers: $\forall g \in G$, $\exists g^{-1} \in G$ tal que $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Si a més el grup satisfà la propietat commutativa ($a \cdot b = b \cdot a$, $\forall a, b \in G$) direm que és un **grup abelià** o commutatiu.

Remarca. Quant l'operació del grup sigui clara o es dedueixi pel context escriurem G en lloc de $(G, \cdot)$. A més, sovint escriurem ab en lloc de $a \cdot b$. Quan el grup sigui abelià, sovint farem servir la notació additiva, és a dir, expressarem l'operació amb $+$ i l'element neutre amb 0.

Remarca. Si tenim un parell $(G, \cdot)$ satisfent totes les propietats d'un grup, excepte l'existència d'un invers per a cada element, direm que és un **monoide**.

Definició 1.2. Sigui G un grup i $H \subseteq G$ un subconjunt de G, direm que H és un **subgrup de** G i escriurem $H \leq G$ si $(H, \cdot)$ és un grup, on $\cdot$ és l'operació de G restringida a H.

Remarca. D'aquesta definició és fàcil veure que si $H \leq G$, els elements neutres i els inversos d'un element de H han de coincidir amb els de G (és a dir que $1_H = 1_G$, i que per tot $x \in H$, es té que $x_H^{-1} = x^{-1}$).

Definició 1.3. Donat un conjunt G, escriurem $\#G$ per designar el seu cardinal, és a dir, el nombre d'elements de G.

Proposició 1.4. *Sigui H un subconjunt del grup G. Aleshores, $H \leq G$ si i només si H no és buit i $xy^{-1} \in H$ per tots $x \in H$ i $y \in H$.*

Definició 1.5. Fixem-nos ara que donat un subgrup $H \leq G$ d'un grup G, es poden construir dues relacions que es pot veure fàcilment que és d'equivalència: $x \sim_H y$ si i només si $x = yh$ per algun $h \in H$ (resp. $x \sim_H y$ si i només si $x = hy$ per algun $h \in H$). Així doncs es poden definir les classes d'equivalència $xH = \{xh \mid h \in H\}$ (resp. $Hx = \{hx \mid h \in H\}$) i que anomenarem **classes laterals per l'esquerra (resp. per la dreta)**. Com que la relació és d'equivalència, les classes laterals són disjuntes i formen una partició de G. Podem definir a més l'**índex de H respecte de G**, que escriurem com a $[G : H]$, i que és el cardinal del conjunt de classes laterals per l'esquerra (o per la dreta). A més, l'índex respecte les classes laterals per la dreta i per l'esquerra coincideix, ja que $xH \to Hx^{-1}$ és clarament una bijecció. Quan un subgrup $H \leq G$ tingui $[G : H] < \infty$, direm que és un **subgrup d'índex finit** i escriurem $H \leq_{f.i.} G$. D'aquestes observacions en resulta el teorema de Lagrange que presentem a continuació.

Teorema 1.6 (Teorema de Lagrange)**.** *Si G és un grup i $H \leq G$ un subgrup, aleshores $\#G = [G : H] \cdot \#H$. Fixem-nos que en el cas que G sigui finit, tenim $[G : H] = \#G/\#H$. Per tant, l'ordre d'un subgrup sempre divideix l'ordre del grup si aquest és finit.*

Definició 1.7. Un subgrup $N \leq G$ de G s'anomena **subgrup normal**, i s'escriu aleshores $N \trianglelefteq G$, si per tot $g \in G$, es té $gN = Ng$.

Proposició 1.8. *Si $N \trianglelefteq G$, aleshores les dues relacions d'equivalència coincideixen mòdul N, són compatibles amb l'operació de G, i per tant el quocient G/N és un grup.*

Introduirem a continuació els homomorfismes, que són les aplicacions entre grups que en preserven l'estructura, i presentarem a continuació els tres teoremes d'isomorfisme.

Definició 1.9. Siguin $(G, \cdot_G)$ i $(H, \cdot_H)$ dos grups. Una funció $f : G \to H$ s'anomena **homomorfisme** si preserva l'estructura de G, és a dir si per qualssevol $x, y \in G$, es té $f(x \cdot_G y) = f(x) \cdot_H f(y)$.

Si a més f defineix una bijecció entre G i H direm que f és un **isomorfisme de grups** i que G i H són **isomorfs**, i escriurem $G \cong H$.

Proposició 1.10. *Si $f : G \to H$ és un homomorfisme, es té $\ker f \trianglelefteq G$.*

Teorema 1.11 (Primer teorema d'isomorfisme)**.** *Sigui $f : G \to H$ un homomorfisme. Aleshores l'aplicació induïda $\overline{f} : G/\ker f \to \operatorname{Im} f$ és un isomorfisme de grups. És a dir que*

$$G/\ker f \cong \operatorname{Im} f.$$

Teorema 1.12 (Segon teorema d'isomorfisme)**.** *Siguin H un subgrup i N un subgrup normal del grup G. Aleshores $N \cap H \trianglelefteq H$ i l'aplicació $(N \cap H)x \mapsto Nx$ és un isomorfisme de $H/N \cap H$ en NH/N.*

Teorema 1.13 (Tercer teorema d'isomorfisme)**.** *Siguin M i N subgrups normals d'un grup G tals que $N \leq M$. Aleshores $M/N \trianglelefteq G/N$ i*

$$(G/N)/(M/N) \cong G/M.$$

Acabem aquest capítol preliminar introduint els conceptes de centre d'un grup, centralitzador d'un element i classe de conjugació d'un element.

Definició 1.14. El **centre** de G és el conjunt dels elements de G que commuten amb tot element del grup, $Z(G) = \{x \in G | xy = yx\ \forall y \in G\}$.

Definició 1.15. El **centralitzador** de $x \in G$ és $C_G(x) = \{y \in G | xy = yx\}$.

Remarca. Per un subconjunt $S \subseteq G$ i un element $x \in G$, escriurem $C_S(x) = C_G(x) \cap S$

Proposició 1.16. *Donat un grup G, es té que el seu centre n'és subgrup normal, $Z(G) \trianglelefteq G$. Per altra banda, donat un element qualsevol del grup $x \in G$, el centralitzador de x n'és un subgrup, $C_G(x) \leq G$.*

Definició 1.17. Donats $x, y \in G$ dos elements d'un grup, diem que x i y són **conjugats** si existeix un $g \in G$ tal que $y = g^{-1}xg$. De manera anàloga, dos subconjunts $X, Y \subseteq G$ s'anomenen conjugats si existeix un $g \in G$ tal que $X = g^{-1}Yg$.

Proposició 1.18. *La conjugació és una relació d'equivalència. A la classe d'equivalència d'un $x \in G$, $Cl_G(x) = \{g^{-1}xg | g \in G\}$, l'anomenem* **classe de conjugació de** *x. Si pel context queda clar escriurem $Cl(x) = Cl_G(x)$.*

1.2 Teorema de Gustafson

Proposició 1.19. *Si $x, y \in G$ són conjugats, aleshores $C_G(x)$ i $C_G(y)$ són conjugats. En particular $\#C_G(x) = \#C_G(y)$.*

Prova. Com que x i y són conjugats, existeix un $g \in G$ tal que $gx = yg$, que es pot reescriure com $xg^{-1} = g^{-1}y$. Aleshores, tenim que

$$h \in C_G(x) \Leftrightarrow hx = xh \Leftrightarrow ghxg^{-1} = gxhg^{-1} \Leftrightarrow ghg^{-1}y = yghg^{-1} \Leftrightarrow ghg^{-1} \in C_G(y).$$

Per tant, concloem que $C_G(x) = gC_G(y)g^{-1}$. És a dir que hi ha una bijecció entre els elements de $C_G(x)$ i els de $C_G(y)$, en particular $\#C_G(x) = \#C_G(y)$. □

Proposició 1.20. *Sigui G un grup i x un element de G, aleshores hi ha una bijecció entre $G/C_G(x)$ i $Cl(x)$. En particular:*

$$\#Cl(x) = [G : C_G(x)].$$

Prova. L'aplicació

$$\begin{aligned} G &\to Cl(x) \\ g &\mapsto g^{-1}xg, \end{aligned}$$

és clarament exhaustiva i satisfà que per cada $y \in Cl(x)$ té exactament $\#C_G(x)$ antiimatges. Efectivament, si tenim $g, g' \in G$ tals que les seves imatges coincideixin, aleshores

$$g^{-1}xg = g'^{-1}xg' \iff g'g^{-1}x = xg'g^{-1} \iff g'g^{-1} \in C_G(x).$$

I per tant se satisfà que $\#G = \#Cl(x)\#C_G(x)$, és a dir que $[G : C_G(x)] = \#Cl(x)$. □

Proposició 1.21. *Donat un element $x \in G$, x és del centre $Z(G)$ si i només si la seva classe de conjugació $Cl_G(x)$ té un sol element que és x.*

Prova. $x \in Z(G) \iff \forall y \in G,\ xy = yx \iff \forall y \in G,\ y^{-1}xy = x \iff Cl_G(x) = \{x\}$. □

Proposició 1.22 (MacHale, 1974 [9]). *Si G no és abelià, aleshores el grup $G/Z(G)$ no pot ser cíclic.*

Prova. Sigui $Z(G)$ el centre de G. Suposem $G/Z(G)$ cíclic amb generador $Z(G)g$, aleshores:

$$G = Z(G) \cup Z(G)g \cup (Z(G)g)^2 \cup \cdots \cup (Z(G)g)^i \cup \dots .$$

Però tenim $(Z(G)g)^i = Z(G)g^i$, perquè els elements del centre commuten amb tots els elements del grup. Per tant:

$$G = Z(G) \cup Z(G)g \cup Z(G)g^2 \cup \cdots \cup Z(G)g^i \cup \dots .$$

D'aquí segueix que tot parell d'elements de G es pot expressar com z_1g^i,z_2g^j amb $z_1, z_2 \in Z(G)$. Per tant, per tot parell d'elements de G tenim $z_1g^iz_2g^j = z_1z_2g^{i+j} = z_2g^jz_1g^i$, que és contradicció amb G no abelià. □

Observació 1.23. Si $\#G/Z(G) = p$, amb p primer, aleshores G és abelià.

Prova. Si $\#G/Z(G) = p$, aleshores com que p és primer, pel teorema de Lagrange, $G/Z(G)$ no té subgrups propis i per tant és cíclic. De la proposició 1.22 se segueix que G és abelià. □

Proposició 1.24. *Si G no és abelià, aleshores $\#Z(G) \le \#G/4$.*

Prova. Veurem que si $\#G/Z(G) = \#G/\#Z(G) \le 3$, aleshores G és abelià. Si $\#G/Z(G) = 1$, aleshores tot element de G és del centre i per tant G és abelià. Si $\#G/Z(G) = 2, 3$, com que són cardinals primers tenim que G és abelià. Per tant si G no és abelià, necessàriament $\#G/Z(G) = \#G/\#Z(G) \ge 4$, que és equivalent a la desigualtat que volíem veure. □

Definició 1.25. La **fracció commutativa** d'un grup finit G és el conjunt de parells ordenats d'elements del grup que commuten, és a dir:

$$C = \{(x, y) \in G \times G \mid xy = yx\}.$$

Observació 1.26. Podem expressar la fracció commutativa en termes dels centralitzadors dels elements del grup de la manera següent:

$$C = \bigsqcup_{x \in G} \{(x, y) \mid y \in C_G(x)\},$$

d'on deduïm $\#C = \sum_{x \in G} \#C_G(x)$.

Prova. Si pels elements de C fixem la primera coordenada $x \in G$, aleshores la segona coordenada ha de ser necessàriament d'un element de $C_G(x)$, és més, hi ha un element de C per cada element del centralitzador de x. Aleshores si fem aquest raonament fixant la primera coordenada per tots els $x \in G$ diferents, obtenim l'expressió de l'observació. I d'aquí se'n dedueix directament la igualtat dels cardinals: $\#C = \#\bigsqcup_{x \in G} \{(x, y) \mid y \in C_G(x)\} = \sum_{x \in G} \#C_G(x)$. □

Definició 1.27. Donat un grup finit, G, el seu **grau de commutativitat**, $dc(G)$, és la probabilitat que dos elements del grup uniformement aleatoris commutin:

$$dc(G) = \frac{\#C}{\#G^2}.$$

Remarca. Per expressar el grau de commutativitat utilitzarem en general la divisió $dc(G) = \#\{(x, y) \in G \times G \mid xy = yx\}/\#G^2$, que en el numerador comptabilitza tots els parells ordenats d'elements de G que commuten, i en el denominador tots els parells ordenats d'elements de G. Observem que, per exemple, donats $x, y \in G$ tals que $xy = yx$, estarem contant tant el parell (x, y) com (y, x). Això no suposa cap problema ja que ho fem tant al numerador com al denominador. Hem utilitzat aquesta expressió de $dc(G)$ en termes de la fracció commutativa perquè en facilita el tractament, però alternativament el grau de commutativitat també es podria expressar en termes de parells no ordenats.

Teorema 1.28 (Gustafson, 1973 [8]). *Per tot grup finit no abelià, G, es té $dc(G) \leq 5/8$.*

Prova. Sigui G un grup finit no abelià i sigui $C = \{(x, y) \in G \times G \mid xy = yx\}$ la fracció commutativa de G, de manera que $dc(G) = \#C/\#G^2$. Podem escriure $\#C$ de la manera següent:

$$\#C = \sum_{x \in G} \#C_G(x) = \sum_{x \in Z(G)} \#C_G(x) + \sum_{x \in G \setminus Z(G)} \#C_G(x).$$

Ara bé, per un element $x \in Z(G)$, aquest commuta amb tot element de G i per tant el seu centralitzador és $C_G(x) = G$. Per altra banda, els elements $x \in G \setminus Z(G)$ segur que no commuten amb tot element de G per no ser del centre, i com que el seu centralitzador és subgrup de G, se satisfà almenys que $\#C_G(x) \leq \#G/2$. Aleshores, a partir de la igualtat anterior:

$$\#C \leq \#Z(G)\#G + (\#G - \#Z(G)) \cdot \frac{1}{2}\#G = \frac{1}{2}\#G(\#Z(G) + \#G) \leq \frac{1}{2}\#G \left(\frac{1}{4}\#G + \#G\right) = \frac{5}{8}\#G^2.$$

On hem utilitzat la desigualtat $\#Z(G) \leq \#G/4$ de 1.24. Finalment, concloem que $dc(G) = \#C/\#G^2 \leq 5/8$. □

Per acabar l'apartat, veurem que la fita que ens dona el teorema anterior és òptima perquè la igualtat se satisfà en el grup dels quaternions.

Observació 1.29. El grup dels quaternions, $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, definit per les igualtats $i^2 = j^2 = k^2 = ijk = -1$ i pel fet que 1 i -1 commuten amb tots els elements del grup, satisfà la igualtat $dc(Q_8) = 5/8$.

Prova. Per veure-ho ens fixarem en totes les desigualtats de la demostració del teorema de Gustafson, i veurem que pel cas dels quaternions, se satisfà la igualtat. Només cal veure que se satisfà $4\#Z(Q_8) = \#Q_8$ i que per tot element $x \in Q_8 \setminus Z(Q_8)$ es té $\#C_G(x) = \#Q_8/2$. Notem que en particular, el que estem veient és que el centre i els centralitzadors són els més grans possibles sense que el grup arribi a ser commutatiu. Per veure-ho, fixem-nos en la taula de multiplicació de Q_8.

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

Tenim que $\#Q_8 = 8$. Per una banda, observem que $\#Z(Q_8) = \#\{\pm 1\} = 2$, i per tant $\#Q_8 = 4\#Z(Q_8)$. Per altra banda $C_{Q_8}(i) = C_{Q_8}(-i) = \{\pm 1, \pm i\}$, $C_{Q_8}(j) = C_{Q_8}(-j) = \{\pm 1, \pm j\}$, $C_{Q_8}(k) = C_{Q_8}(-k) = \{\pm 1, \pm k\}$, és a dir que tot element $x \in Q_8 \backslash Z(Q_8)$ satisfà $C_G(x) = \#(Q_8)/2$. Concloem, doncs, que pel cas dels quaternions tenim $dc(Q_8) = \#C/\#{Q_8}^2 = 5/8$. □

1.3 Teorema de Gallagher

Definició 1.30. Sigui G un grup finit, denotarem per $k(G)$ el **nombre de classes de conjugació de** G.

Proposició 1.31. *Sigui G un grup finit, aleshores el seu grau de commutativitat i el seu nombre de classes de conjugació estan relacionats segons la igualtat:*

$$k(G) = \#G \cdot dc(G).$$

Prova. Tenim que

$$\#G \cdot dc(G) = \frac{\#C}{\#G} = \frac{1}{\#G} \sum_{x \in G} \#C_G(x).$$

Com que la conjugació és una relació d'equivalència, les classes de conjugació són una partició de G. A més, hem vist que dos elements conjugats tenen centralitzadors amb cardinals iguals (proposició 1.19). Llavors, si $x_1, \dots, x_{k(G)} \in G$ són representats de les classes de conjugació, podem reescriure la suma anterior com:

$$\#G \cdot dc(G) = \frac{1}{\#G} \sum_{i=1}^{k(G)} \#Cl(x_i)\#C_G(x_i) = \frac{1}{\#G} \sum_{i=1}^{k(G)} [G : C_G(x_i)]\#C_G(x_i) = \frac{k(G)\#G}{\#G} = k(G).$$

□

Proposició 1.32. *Sigui G un grup finit i $N \trianglelefteq G$ un subgrup normal, per tot $x \in G$ se satisfà:*

$$C_G(x)/C_N(x) \cong C_G(x)N/N \leq C_{G/N}(xN).$$

Prova. Provarem primer la inclusió $C_G(x)N/N \leq C_{G/N}(xN)$. Recordem que $C_G(x)N/N = \{yN \in G/N \mid y \in C_G(x)\}$, i $C_{G/N}(xN) = \{yN \in G/N \mid yNxN = xNyN\}$. Aleshores, donat un $yN \in C_G(x)N/N$, en particular $xy = yx$, a més com que N és normal, es té $yN = Ny$. Aleshores $yNxN = NyxN = NxyN = xNyN$, i per tant $yN \in C_{G/N}(xN)$, tal com volíem veure.

Provem ara l'isomorfisme $C_G(x)/C_N(x) \cong C_G(x)N/N$. Per fer-ho usarem el Primer Teorema d'Isomorfisme, que en aquest cas ens diu que si $f : C_G(x) \to C_G(x)N/N$ és un homomorfisme de grups, aleshores $C_G(x)/\ker(f) \cong \mathrm{im}(f)$. Sigui, doncs:

$$\begin{aligned} f : C_G(x) &\to C_G(x)N/N \\ y &\mapsto yN, \end{aligned}$$

veiem primer que és un homomorfisme ben definit. Que sigui homomorfisme es dedueix ràpidament de la normalitat de N, ja que $f(x)f(y) = xNyN = xyNN = xyN = f(xy)$. A més, està ben definit perquè f és una projecció natural que envia els elements de $C_G(x)$ a les seves classes. Fixem-nos també que f és exhaustiva ja que per tot $ynN \in C_G(x)N/N$, tenim que $y \in C_G(x)$ i $ynN = yN = f(y)$. I de l'exhaustivitat se segueix que $\mathrm{im}(f) = C_G(x)N/N$. Finalment veiem que $\ker(f) = C_N(x)$, sigui $y \in C_G(x)$:

$$y \in \ker f \iff f(y) = yN = N \iff y \in N \iff y \in C_N(x).$$

Aleshores del Primer Teorema d'Isomorfisme concloem que $C_G(x)/C_N(x) \cong C_G(x)N/N$. □

Proposició 1.33. *Siguin G un grup finit i $N \trianglelefteq G$ un subgrup normal. Donat un $y \in G$ i $n \in N$, es té que $C_{yN}(n) = \emptyset$ o bé hi ha un $yn_0 \in C_{yN}$ tal que $C_{yN}(n) = yn_0 C_N(n)$, és a dir, que $C_{yN}(n)$ és una classe lateral de $C_N(n)$. En particular es té que $\#C_{yN}(n) \leq \#C_N(n)$.*

Prova. Si $C_{yN}(n) = \emptyset$, en particular tenim $0 = \#C_{yN}(n) \leq \#C_N(n)$. Suposem ara que $C_{yN}(n)$ no és buit, i per tant, que existeix algun $yn_0 \in C_{yN}(n)$. Veiem que en aquest cas $C_{yN}(n) = yn_0 C_N(n)$. Veiem primer que $C_{yN}(n) \subseteq yn_0 C_N(n)$. Sigui un $yn' \in C_{yN}(n)$, podem escriure $yn' = yn_0(n_0^{-1}n')$, i com que tant yn' com yn_0 commuten amb n, tenim que $n_0^{-1}n' \in N$ també commuta amb n, és a dir que $n_0^{-1}n' \in C_N(n)$. Veiem ara $C_{yN}(n) \supseteq yn_0 C_N(n)$. Sigui un $n' \in C_N(n)$, llavors com que també yn_0 commuta amb n, tenim que $yn_0 n'$ commuta amb n, i per tant $yn_0 n' = y(n_0 n') \in C_{yN}(n)$.

Aleshores quan $C_{yN}(n) = yn_0 C_N(n)$, tenim que $C_{yN}(n)$ és una classe lateral $C_N(n) \leq G$, i per tant que $\#C_{yN}(n) = \#C_N(n)$. En particular, també es té $\#C_{yN}(n) \leq \#C_N(n)$. □

Teorema 1.34 (Gallagher, 1970 [7])**.** *Sigui G un grup finit i $N \trianglelefteq G$ un subgrup normal, aleshores:*

$$dc(G) \leq dc(G/N)dc(N).$$

Prova. Per la demostració partirem de la inclusió que hem vist a la proposició 1.32,

$$C_G(x)/C_N(x) \cong C_G(x)N/N \leq C_{G/N}(xN),$$

d'on es dedueix:

$$\begin{gathered} \#C_G(x) \leq \#C_{G/N}(xN)\#C_N(x) \\ \sum_{x \in G} \#C_G(x) \leq \sum_{x \in G} \#C_{G/N}(xN)\#C_N(x). \end{gathered}$$

Ara fixem-nos que dos elements de la mateixa classe $yN \in G/N$ han de tenir centralitzadors d'igual cardinal $\#C_{G/N}(yN)$ i per tant podem treure factor comú:

$$\sum_{x \in G} \#C_G(x) \leq \sum_{yN \in G/N} \Big(\#C_{G/N}(yN) \sum_{x \in yN} \#C_N(x) \Big).$$

Observem que per tot $x \in yN$, tenim $n \in C_N(x) \iff n \in N, xn = nx \iff n \in N, x \in C_{yN}(n)$. Llavors podem reescriure la desigualtat com:

$$\sum_{x \in G} \#C_G(x) \leq \sum_{yN \in G/N} \#C_{G/N}(yN) \sum_{n \in N} \#C_{yN}(n).$$

A més tenim que $\#C_{yN}(n) \leq \#C_N(n)$ per la proposició 1.33, i per tant:

$$\sum_{x \in G} \#C_G(x) \leq \sum_{yN \in G/N} \#C_{G/N}(yN) \sum_{n \in N} \#C_N(n)$$

$$\frac{1}{\#G^2} \sum_{x \in G} \#C_G(x) \leq \frac{1}{(\#G/\#N)^2} \sum_{yN \in G/N} \#C_{G/N}(yN) \frac{1}{\#N^2} \sum_{n \in N} \#C_N(n)$$

$$dc(G) \leq dc(G/N) dc(N).$$

□

Com hem vist a 1.31, hi ha una estreta relació entre el grau de commutativitat i el nombre de classes de conjugació d'un grup. Degut a això sovint es pot reescriure un resultat d'un dels dos en termes de l'altre. Un exemple n'és el Teorema de Gallagher que acabem de veure. De fet, en l'article original [7], el resultat donat és el del corol·lari següent, que es dona en termes del nombre de classes de conjugació.

Corol·lari 1.35. *Sigui G un grup finit i $N \trianglelefteq G$ un subgrup normal, aleshores:*

$$k(G) \leq k(G/N) k(N).$$

Prova. El resultat surt directament d'aplicar $k(G) = \#G \cdot dc(G)$ al teorema anterior. □

2. Grup lliure i presentacions

En aquest capítol introduirem els conceptes que ens serviran per poder treballar amb el grau de commutativitat de grups infinits. Els grups infinits en general són més complicats i diversos que els finits, així doncs haurem de fer un treball previ per poder-los expressar d'una manera en què ens sigui prou còmode treballar-hi. En aquest sentit, introduirem els conceptes de grups lliures i la noció de presentació d'un grup. Al llarg del capítol seguirem de manera força propera el desenvolupament que se'n fa a [6].

2.1 Construcció del grup lliure

Començarem el capítol introduint el concepte de grup lliure amb una aproximació algebraica, malgrat que també té altres caracteritzacions, per exemple s'hi pot fer una aproximació més geomètrica com es pot veure a [6]. Per a fer-ho també serà necessari parlar abans de les bases d'un grup.

Observem primer que en un producte d'elements d'un grup G, els elements neutres (o trivials), 1, i les cancel·lacions (productes gg^{-1} per qualsevol $g \in G$) que tingui, són supèrflues. Per exemple, si tenim $a, b \in G$, els productes $a1b = ab$ representen el mateix element de G, i de la mateixa manera $agg^{-1}b = ab$. Aquest fet motiva la propera definició:

Definició 2.1. Un **producte reduït** d'elements d'un grup és el producte d'elements que no té elements neutres ni cancel·lacions. El producte buit, és un producte reduït que correspon a l'element neutre.

Fixem-nos que donat un producte d'elements d'un grup, podríem anar eliminant-ne successivament els factors que siguin elements neutres i cancel·lacions fins a obtenir un producte reduït amb el mateix resultat.

Definició 2.2. Sigui G un grup, diem que $A \subseteq G$ és un **subconjunt lliure** o **independent** si per qualssevol dos productes reduïts diferents d'elements d'$A^{\pm} = A \cup A^{-1}$, aquests representen elements diferents de G. Diem que A **genera** G (o que n'és un **conjunt de generadors**) si per tot element de G existeix un producte d'elements de $A^{\pm}$ (que podem suposar reduït) que el té com a resultat. Direm que A és una **base** de G o que G és **lliure (sobre A)** si A és un conjunt lliure que genera G. Per denotar a un grup lliure usarem la notació $\mathbb{F}$.

Observació 2.3. $A \subseteq G$ és un subconjunt lliure si i només si l'únic producte reduït d'elements d'A que dona l'element trivial és el buit. Aquesta es pot veure com una definició equivalent a A subconjunt lliure.

Prova. Veiem primer la implicació directa. Sigui $A \subseteq G$ lliure i suposem que existeix un producte reduït d'elements d'A diferent del buit que dona l'element trivial. Podem escriure aquest producte com $a_1 a_2 \dots a_m = 1$, però llavors tenim que són dos productes reduïts diferents d'elements d'A amb el mateix resultat en G, l'element trivial, fet que contradiu que A sigui lliure.

Provem ara l'altra implicació. Tenim que l'únic producte reduït d'elements d'A que dona l'element trivial és el buit. Suposem que A no és lliure, i per tant existeixen dos productes reduïts diferents $a = a_1 a_2 \dots a_m$, $b = b_1 b_2 \cdots b_n$ d'elements d'$A^{\pm}$ tals que $a = b$, i per tant $ab^{-1} = 1$. Com que els dos productes reduïts són diferents, tenim que o bé $m \neq n$ o bé existeix algun k amb $a_k \neq b_k$, de manera que $ab^{-1} = 1$ és un producte que reduït és diferent del producte buit, però que tanmateix dona l'element trivial, i això és una contradicció. □

Definició 2.4. Anomenarem **rang** d'un grup G, que escriurem com $\mathrm{rk}(G)$, al cardinal mínim d'un conjunt de generadors de G. Si un grup admet un conjunt de generadors finit direm que és un grup **finitament generat**.

Remarca. D'aquesta definició en sorgeix naturalment el dubte de si hi ha alguna relació entre el rang d'un grup lliure i el cardinal de les seves possibles bases. I tot i que ens portarà una mica de feina, més endavant veurem que aquesta intuïció és certa.

Exemple 2.5. Considerem el grup $(\mathbb{Z}, +)$ amb la notació additiva. Tenim que els subconjunts $\{-1\}$ i $\{1\}$ en són bases. Per una banda $\{-1\}^{\pm} = \{1\}^{\pm} = \{-1, 1\}$ és un conjunt que genera tot element de $\mathbb{Z}$. I per altra banda els únics productes reduïts que admet són de la forma:

$$1 + 1 + \overset{n)}{\cdots} + 1 \text{ o bé } (-1) + (-1) + \overset{n)}{\cdots} + (-1),$$

que són diferents de 0 si $n \neq 0$ i, per tant, el producte buit és l'únic producte reduït que és igual a l'element neutre (i per tant són subconjunts lliures). En particular tenim que $\{1\}$ és un conjunt de generadors de $\mathbb{Z}$ (que té el cardinal mínim perquè el conjunt buit no genera $\mathbb{Z}$) i per tant $\mathrm{rk}(\mathbb{Z}) = 1$.

Exemple 2.6. Considerem ara, per un natural $n \geq 2$, el grup $(\mathbb{Z}/n\mathbb{Z}, +)$, i veurem que no és lliure. Fixem-nos que en aquest cas $\{\overline{1}\} = \{1 + n\mathbb{Z}\}$ no és una base de $\mathbb{Z}/n\mathbb{Z}$, perquè malgrat ser-ne generador, no és lliure degut a què $\overline{1} + \overline{1} + \overset{n)}{\cdots} + \overline{1} = \overline{0}$, i per tant hi ha dues expressions reduïdes per a l'element trivial. De fet, cap subconjunt $A \subseteq \mathbb{Z}/n\mathbb{Z}$ en pot ser una base, ja que el subconjunt buit no genera i per qualsevol element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ se satisfà $\overline{a} + \overline{a} + \overset{n)}{\cdots} + \overline{a} = \overline{0}$ i per tant A no podria ser un subconjunt lliure. Concloem, doncs, que el grup $\mathbb{Z}/n\mathbb{Z}$ no és lliure.

Observació 2.7. Si $\mathbb{F}$ és un grup lliure amb base $A \subseteq \mathbb{F}$, aleshores A és un conjunt de generadors minimal. És a dir que $\langle A \rangle = \mathbb{F}$, però per qualsevol $\emptyset \neq S \subseteq A$ es té $\langle A \setminus S \rangle \neq \mathbb{F}$.

Prova. Suposem que existeix un $S \neq \emptyset$ tal que $\langle A \setminus S \rangle = \mathbb{F}$. Sigui $s \in S \subseteq A$ tenim que es pot expressar com un element de A, però en particular $s \in \mathbb{F}$ i per tant també es pot expressar com un producte d'elements de $A \setminus S$ (que hem suposat generador de $\mathbb{F}$). Això és una contradicció amb A subconjunt lliure. $\square$

A continuació farem la construcció de grups lliures amb bases de cardinal arbitrari.

Definició 2.8. Donat A un conjunt (finit o infinit), que anomenarem alfabet o conjunt de lletres elementals, una **paraula** sobre A és una seqüència ordenada i finita de lletres, $a_1 a_2 \ldots a_n$, on $n \geq 0$, i $a_i \in A$, amb possibles repeticions. El nombre total de lletres d'una paraula s'anomena longitud, que escrivim com $|a_1 a_2 \ldots a_n| = n$. Com a conveni, designarem per 1 l'única paraula de longitud zero, o paraula buida. El conjunt de totes les paraules sobre A el designem per A^*.

Remarca. Farem servir la notació exponencial habitual en el producte successiu d'un mateix element per abreujar les paraules, és a dir que escriurem

$$a^n = a \cdot a \overset{n)}{\cdots} a \quad \text{i} \quad a^{-n} = (a^{-1})^n$$

per $n \geq 0$. Per exemple, si tinguéssim la paraula $aabbbacd^{-1}d^{-1}$ la podríem escriure com $a^2 b^3 acd^{-2}$.

Observació 2.9. Donat un alfabet A, el conjunt A^* és un monoide amb la concatenació com a operació: $u \cdot v = uv$, per $u, v \in A^*$. A més, tenim que $|u \cdot v| = |u| + |v|$ i per tant l'únic element invertible és el neutre, 1.

Prova. Efectivament, la concatenació és una operació interna, i a més es comprova ràpidament l'associativitat, $(u \cdot v) \cdot w = uv \cdot w = uvw = u \cdot vw = u \cdot (v \cdot w)$, i que la paraula buida és l'element neutre, $1 \cdot u = u = u \cdot 1$. $\square$

Exemple 2.10. Veiem un parell d'exemples d'alfabets que ens ajudaran a veure el que estem construint. El monoide que genera l'alfabet d'una lletra $A = \{a\}$ és isomorf al dels números naturals, ja que $A^* = \{1, a, a^2, a^3, \dots\}$ i $a^n \cdot a^m = a^{n+m}$ per $n, m \in \mathbb{N}$. Per altra banda, el monoide que genera l'alfabet de dues lletres $A = \{a, b\}$ no és un commutatiu degut a que $ab \neq ba$.

Així doncs, per ara tenim que A és lliure i generador de A^*, però no és pas un grup sinó un monoide, ja que ens falta que els seus elements tinguin inversos. Llavors afegirem inversos formals al conjunt, definint $A^{\pm} = A \sqcup A^{-1} = \{a, a^{-1} | a \in A\}$. Fixem-nos però, que així només hem afegit elements nous, però hem de forçar que realment a i a^{-1} siguin inversos, és a dir que $a^{-1}a = 1 = aa^{-1}$. Ho aconseguirem fent una relació d'equivalència apropiada.

Definició 2.11. Anomenem **reducció elemental**, que designem per $\rightsquigarrow$, a la transformació consistent a eliminar una cancel·lació dins d'una paraula. És a dir, que per $a \in A$ i $u, v \in (A^{\pm})^*$,

$$uaa^{-1}v \rightsquigarrow uv \quad \text{i} \quad ua^{-1}av \rightsquigarrow uv.$$

Anomenem **inserció elemental** a la transformació inversa, que consisteix en inserir una cancel·lació dins d'una paraula, i **transformació elemental** a la seva clausura simètrica, que designarem per $\leftrightsquigarrow$. És a dir, que per dues paraules $w, w' \in (A^{\pm})^*$,

$$w \leftrightsquigarrow w' \iff w \rightsquigarrow w' \quad \text{ó} \quad w' \rightsquigarrow w.$$

Observem a més que si $w \leftrightsquigarrow w'$, aleshores $|w| = |w'| \pm 2$. Finalment, definim $\sim$ com la clausura reflexotransitiva de la transformació elemental. És a dir, que per tot $w, w' \in (A^{\pm})^*$, se satisfà:

1. $w \sim w$
2. $w \sim w' \iff \exists w_0 = w, w_1, \dots, w_n = w'$ tals que $w_0 \leftrightsquigarrow w_1 \leftrightsquigarrow \cdots \leftrightsquigarrow w_n$.

És a dir, que $w \sim w'$ si pots passar de w a w' amb una quantitat finita de transformacions elementals, entenem que això inclou el cas amb $n = 0$ transformacions.

Observem que a partir d'aquesta definició constructiva que hem donat, és clar que $\sim$ és una relació d'equivalència i per tant podem fer el conjunt quocient $\mathbb{F}_A = (A^{\pm})^* / \sim$, que és el conjunt de classes de paraules equivalents segons $\sim$. Així, la classe $[w] \in \mathbb{F}_A$ conté totes les paraules que són iguals a w mòdul les equivalències elementals $a^{-1}a = 1 = aa^{-1}$ $\forall a \in A$, tal com volíem. Finalment, definim a $\mathbb{F}_A = (A^{\pm})^* / \sim$ una operació binària adaptant de manera natural la concatenació de $(A^{\pm})^*$,

$$[u] \cdot [v] = [uv].$$

Observem que aquesta operació està ben definida, ja que si $u \sim u'$ i $v \sim v'$, aleshores $uv \sim u'v \sim u'v'$ i per tant $[u] \cdot [v] = [uv] = [u'v'] = [u'] \cdot [v']$. On hem usat el fet clar que si $u \leftrightsquigarrow u'$, podem fer la mateixa transformació elemental sobre uv deixant v igual i per tant $uv \leftrightsquigarrow u'v$.

Proposició 2.12. *El conjunt* $\mathbb{F}_A = (A^{\pm})^* / \sim$ *és un grup.*

Prova. L'associativitat s'hereta de la concatenació sobre $(A^{\pm})^*$ i l'element neutre és $[1]$, ja que que si $[u] \in \mathbb{F}_A$, es té $[u] \cdot [1] = [u] = [1] \cdot [u]$. L'invers d'una classe $[a_{i_1}^{\epsilon_1} \dots a_{i_n}^{\epsilon_n}] \in \mathbb{F}_A$ amb $\epsilon_j = \pm 1$, és $[a_{i_n}^{-\epsilon_n} \dots a_{i_1}^{-\epsilon_1}]$. $\square$

Un cop hem construït el grup $\mathbb{F}_A$, ara ens falta veure que efectivament és lliure. De manera natural podríem injectar el conjunt A en $\mathbb{F}_A$ amb $\iota_A : A \to \mathbb{F}_A$, $a \mapsto [a]$, interpretant A com el conjunt de classes de paraules de longitud 1. Però hauríem de veure prèviament que dues lletres diferents pertanyen a dues classes d'equivalència diferents, es a dir, que per dues lletres positives diferents $a, b \in A$, no es té $[a] = [b]$. Intentar demostrar rigorosament aquesta idea, que a priori sembla tant intuïtiva, ens motiva la següent definició.

Definició 2.13. Una paraula $w \in (A^{\pm})^*$ és **reduïda** si no conté cap parell de lletres consecutives mútuament inverses formals. És a dir, una paraula $w = a_{i_1}^{\epsilon_1} \dots a_{i_n}^{\epsilon_n}$ serà reduïda si quan dues lletres consecutives coincideixin, $a_{i_j} = a_{i_{j+1}}$, aleshores també coincideixen els seus signes $\epsilon_j = \epsilon_{j+1}$. Designarem el conjunt de paraules reduïdes en A per $R(A) \subseteq (A^{\pm})^*$.

Proposició 2.14. *Tota classe d'equivalència $[w] \in \mathbb{F}_A$ conté una i només una paraula reduïda que designarem per $\overline{w}$.*

Prova. Veiem primer l'existència, és a dir que cada classe $[w] \in \mathbb{F}_A$ conté una paraula reduïda. Prenem un representant w de la classe, i si aquest no és ja una paraula reduïda hi podem aplicar reduccions elementals successivament fins a obtenir-la. És segur que en un nombre finit de passos s'obtindrà una paraula reduïda ja que la longitud d'una paraula, $|w|$, és finita (i no pot ser menor que 0) i per cada reducció elemental disminueix en dues unitats.

Veiem ara la unicitat. Suposem que una classe $[w] \in \mathbb{F}_A$ conté dues paraules reduïdes diferents $\overline{w}, \overline{w}' \in R(A)$, Com que són de la mateixa classe podem construir una successió de transformacions elementals entre ambdues, sigui doncs $\overline{w} = w_0 \leftrightsquigarrow w_1 \leftrightsquigarrow \cdots \leftrightsquigarrow w_n = \overline{w}'$ la que minimitza $N = \sum_{i=0}^{n} |w_i|$. Com que $\overline{w} \neq \overline{w}'$, tenim que n no pot ser 0 ni 1 ni 2, per tant ha de ser $n \geq 3$. A més, com que són reduïdes tenim $|w_0| \leq |w_1|$ i $|w_{n-1}| \geq |w_n|$ i, per tant, existeix un $j \in [1, n-1]$ tal que $|w_{j-1}| \leq |w_j| \geq |w_{j+1}|$. Fixem-nos ara en les reduccions elementals $w_{j-1} \leftsquigarrow w_j \rightsquigarrow w_{j+1}$ i en les dues lletres de w_j afectades en cadascuna d'aquestes reduccions. Si n'hi ha una o dues en comú, aleshores $w_{j-1} = w_{j+1}$, i això contradiu la minimalitat de N. Si les dues reduccions afecten a parells de lletres disjunts, és té que $w_j = xa^{\epsilon}a^{-\epsilon}yb^{\delta}b^{-\delta}z$ per certes paraules x, y, z i lletres $a, b \in A$ i certs signes $\epsilon, \delta = \pm 1$. Però canviant $w_{j-1} \leftsquigarrow w_j \rightsquigarrow w_{j+1}$ per $xa^{\epsilon}a^{-\epsilon}yz \rightsquigarrow xyz \leftsquigarrow xyb^{\delta}b^{-\delta}z$ o $xyb^{\delta}b^{-\delta}z \rightsquigarrow xyz \leftsquigarrow xa^{\epsilon}a^{-\epsilon}yz$ segons convingui, es pot reduir el valor de N, fet que contradiu la seva minimalitat, i d'aquesta manera queda provada la unicitat de la paraula reduïda. $\square$

Observació 2.15. Com que cada classe d'equivalència $[w] \in \mathbb{F}_A$ conté una i només una paraula reduïda, podem pensar el grup $\mathbb{F}_A$ com el conjunt de paraules reduïdes, $R(A)$, amb l'operació $u \cdot v = \overline{uv}$. Sovint farem aquesta interpretació i farem un abús de notació escrivint $w \in \mathbb{F}_A$ per referir-nos a l'element $[w] = [\overline{w}] \in \mathbb{F}_A$.

Corol·lari 2.16. *La funció $\iota_A : A \hookrightarrow \mathbb{F}_A, a \mapsto [a]$ és injectiva.*

Prova. Observem que les lletres $a \in A$ són reduïdes ja que no poden contenir cap parell d'inverses formals clarament. Aleshores per $a, b \in A$, $[a] = [b]$ implica que $a = b$, ja que sinó tindríem dues paraules reduïdes diferents en una mateixa classe. $\square$

Corol·lari 2.17. *Per tot A, el conjunt $\mathbb{F}_A$ és lliure amb base A.* $\square$

2.2 Presentacions de grups

Ara que hem construït el grup lliure de base A arbitrària, ens interessarà veure per quins conjunts obtindrem grups lliures isomorfs. És a dir, què han de satisfer dos conjunts A i A' per tal que $\mathbb{F}_A \cong \mathbb{F}_{A'}$. Intuïtivament podríem pensar que això se satisfà quan A i A' tenen el mateix cardinal, i veurem que efectivament és així. Per fer-ho, però, primer haurem d'introduir una altra caracterització dels grups lliures, que en realitat, n'és la definició estàndard en termes categòrics.

Proposició 2.18. *Siguin F un grup i $A \subseteq F$. Designem per $\iota_A : A \hookrightarrow F$ la inclusió natural. Aleshores, F és lliure amb base A si i només si, per a tot grup G, i tota aplicació (de conjunts) $\varphi : A \to G$, existeix un únic morfisme de grups $\tilde{\varphi} : F \to G$ tal que $\tilde{\varphi}\iota_A = \varphi$.*

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, hook, "\iota_A"'] & G \\
F \arrow[ur, dashed, "\exists!\tilde{\varphi}"'] &
\end{tikzcd}$$

Prova. Comencem amb la implicació cap a la dreta. Veurem primer la unicitat. Suposem que F és lliure amb base A. Donats G i $\varphi : A \to G$, busquem un morfisme $\tilde{\varphi} : A \to G$ que satisfaci $\tilde{\varphi}(a) = \varphi(a)$ per tot element $a \in A$. Per tant, per a qualsevol producte reduït d'elements de A, $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, tenim que $\tilde{\varphi}(a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}) = \tilde{\varphi}(a_{i_1})^{\epsilon_1} \cdots \tilde{\varphi}(a_{i_n})^{\epsilon_n} = \varphi(a_{i_1})^{\epsilon_1} \cdots \varphi(a_{i_n})^{\epsilon_n}$. Com que A genera F, el possible morfisme $\tilde{\varphi}$ queda completament determinat per φ, i això implica la seva unicitat. Pel que fa a l'existència, fixem-nos que com que A és un subconjunt lliure de F (i, per tant, cap element de F no té dues expressions diferents com a producte reduït d'elements de A), és clar que la igualtat anterior per a $\tilde{\varphi}$ ens proporciona una aplicació ben definida de $F \to G$. Finalment, veiem que $\tilde{\varphi}$ és un morfisme de grups: prenem $x, y \in F$ i considerem les seves expressions reduïdes úniques,

$$x = a_{i_n}^{\epsilon_n} \cdots a_{i_2}^{\epsilon_2} a_{i_1}^{\epsilon_1} \quad \text{i} \quad y = b_{j_1}^{\delta_1} b_{j_2}^{\delta_2} \cdots b_{j_m}^{\delta_m},$$

amb $a_{i_1}, \ldots, a_{i_n}, b_{j_1}, \ldots, b_{j_m} \in A$ i $\epsilon_1, \ldots, \epsilon_n, \delta_1, \ldots, \delta_m = \pm 1$. Aleshores, pel producte xy tindrem un número de cancel·laions $0 \leq r \leq \min\{n, m\}$. En aquest cas se satisfarà $a_{i_1}^{\epsilon_1} = b_{j_1}^{-\delta_1}, \ldots, a_{i_r}^{\epsilon_r} = b_{j_r}^{-\delta_r}, a_{i_{r+1}}^{\epsilon_{r+1}} \neq b_{j_{r+1}}^{-\delta_{r+1}}$ i, per tant, l'única expressió reduïda de xy com a producte d'elements de A és $xy = a_{i_n}^{\epsilon_n} \cdots a_{i_{r+1}}^{\epsilon_{r+1}} b_{j_{r+1}}^{\delta_{r+1}} \cdots b_{i_m}^{\delta_m}$. Així doncs, tenim

$$\begin{aligned}
\tilde{\varphi}(xy) &= \tilde{\varphi}(a_{i_n}^{\epsilon_n} \cdots a_{i_{r+1}}^{\epsilon_{r+1}} b_{j_{r+1}}^{\delta_{r+1}} \cdots b_{i_m}^{\delta_m}) \\
&= \varphi(a_{i_n})^{\epsilon_n} \cdots \varphi(a_{i_{r+1}})^{\epsilon_{r+1}} \varphi(b_{j_{r+1}})^{\delta_{r+1}} \cdots \varphi(b_{i_m})^{\delta_m} \\
&= [\varphi(a_{i_n})^{\epsilon_n} \cdots \varphi(a_{i_{r+1}})^{\epsilon_{r+1}}] \cdot [\varphi(a_{i_r})^{\epsilon_r} \cdots \varphi(a_{i_1})^{\epsilon_1}] \cdot [\varphi(b_{j_1})^{\delta_1} \cdots \varphi(b_{i_r})^{\delta_r}] \cdot [\varphi(b_{j_{r+1}})^{\delta_{r+1}} \cdots \varphi(b_{i_m})^{\delta_m}] \\
&= \tilde{\varphi}(a_{i_n}^{\epsilon_n} \cdots a_{i_{r+1}}^{\epsilon_{r+1}} a_{i_r}^{\epsilon_r} \cdots a_{i_1}^{\epsilon_1}) \cdot \tilde{\varphi}(b_{j_1}^{\delta_1} \cdots b_{i_r}^{\delta_r} b_{j_{r+1}}^{\delta_{r+1}} \cdots b_{i_m}^{\delta_m}) \\
&= \tilde{\varphi}(x) \cdot \tilde{\varphi}(y).
\end{aligned}$$

Per veure l'altra implicació, suposem que la propietat universal per a F és certa. Considerem $H = \langle A \rangle \leq F$, el subgrup de F generat per A, i designem per $i : H \hookrightarrow F$ la inclusió. Aplicant la propietat universal a la inclusió $\varphi : A \hookrightarrow H$, obtenim un morfisme $\tilde{\varphi} : F \to H$ que compleix $\tilde{\varphi}\iota_A = \varphi$. Ara, apliquem novament la propietat universal a la composició $\iota_A = i\varphi : A \hookrightarrow H \hookrightarrow F$. El morfisme $i\tilde{\varphi}$ compleix $(i\tilde{\varphi})\iota_A = i(\tilde{\varphi}\iota_A) = i\varphi$, i la identitat $\mathrm{id}_F : F \to F$ també ho compleix, $\mathrm{id}_F\, \iota_A = \iota_A = i\varphi$. Però aleshores de la unicitat se segueix que $\mathrm{id}_F = i\tilde{\varphi}$, d'on deduïm que $F = \mathrm{im}(\mathrm{id}_F) = \mathrm{im}(i\tilde{\varphi}) = \mathrm{im}(\tilde{\varphi}) \leq H = \langle A \rangle$ i, per tant, que A genera F.

$$\begin{tikzcd} A \arrow[r, hook, "\varphi"] \arrow[d, hook, "\iota_A"'] & H \arrow[r, hook, "i"] & F \\ F \arrow[ur, dashed, "\tilde{\varphi}"] \arrow[urr, dashed, "i\tilde{\varphi}=\mathrm{id}_F"'] & & \end{tikzcd}$$

Només ens falta veure que A és un subconjunt lliure de F. Podem considerar el conjunt A com un alfabet formal i $G = \mathbb{F}_A$. Aplicant la propietat universal a la inclusió $\varphi : A \hookrightarrow \mathbb{F}_A, a \mapsto [a]$, existeix un morfisme $\tilde{\varphi} : F \to \mathbb{F}_A$ que compleix $\tilde{\varphi}\iota_A = \varphi$. Això significa que $\tilde{\varphi}(a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}) = \varphi(a_{i_1})^{\epsilon_1} \cdots \varphi(a_{i_n})^{\epsilon_n} = [a_{i_1}]^{\epsilon_1} \cdots [a_{i_n}]^{\epsilon_n} = [a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}]$, per a cada producte reduït $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ d'elements d'A. Per tant, si dos productes reduïts d'elements de A, $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ i $b_{j_1}^{\delta_1} \cdots b_{j_m}^{\delta_m}$, donen el mateix resultat a F, $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n} =_F b_{j_1}^{\delta_1} \cdots b_{j_m}^{\delta_m}$, llavors $[a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}] =_{\mathbb{F}_A} [b_{j_1}^{\delta_1} \cdots b_{j_m}^{\delta_m}]$, i de la unicitat de les paraules reduïdes d'una mateixa classe de $\mathbb{F}_A$ que hem vist a la proposició 2.14, se segueix que: $n = m, a_{i_1} = b_{j_1}, \dots, a_{i_n} = b_{j_n}$ i $\epsilon_1 = \delta_1, \dots, \epsilon_n = \delta_n$. Per tant, A és un subconjunt lliure de F. $\square$

Proposició 2.19. *Siguin $\mathbb{F}$ un grup lliure amb base $A \subseteq \mathbb{F}$ i $\mathbb{F}'$ un grup lliure amb base $A' \subseteq \mathbb{F}'$ i siguin ι_A i $\iota_{A'}$ les respectives inclusions. Llavors, $\mathbb{F}$ i $\mathbb{F}'$ són grups isomorfs si i només si A i A' tenen el mateix cardinal: $\mathbb{F} \cong \mathbb{F}' \iff \#A = \#A'$.*

Prova. Comencem veient la implicació com a l'esquerra, suposem $\#A = \#A'$. Podem prendre una aplicació bijectiva $\eta : A \to A'$. Podem aplicar la propietat universal de $\mathbb{F}$ a $\iota_{A'}\eta$ per obtenir un morfisme $\alpha : \mathbb{F} \to \mathbb{F}'$ que compleix $\alpha\iota_A = \iota_{A'}\eta$. Anàlogament podem aplicar la propietat universal de $\mathbb{F}'$ a $\iota_A\eta^{-1}$ per obtenir un morfisme $\beta : \mathbb{F}' \to \mathbb{F}$ que compleix $\beta\iota_{A'} = \iota_A\eta^{-1}$.

$$\begin{tikzcd} A \arrow[r, hook, "\eta"] \arrow[d, hook, "\iota_A"'] & A' \arrow[r, hook, "\iota_{A'}"] & \mathbb{F}' \\ \mathbb{F} \arrow[urr, dashed, "\alpha"'] & & \end{tikzcd} \qquad \begin{tikzcd} A' \arrow[r, hook, "\eta^{-1}"] \arrow[d, hook, "\iota_{A'}"'] & A \arrow[r, hook, "\iota_A"] & \mathbb{F} \\ \mathbb{F}' \arrow[urr, dashed, "\beta"'] & & \end{tikzcd}$$

Ara apliquem la propietat universal de $\mathbb{F}$ a la inclusió ι_A, clarament la identitat compleix $\iota_A \,\mathrm{id}_{\mathbb{F}} = \iota_A$, però resulta que el morfisme $\beta\alpha : \mathbb{F} \to \mathbb{F}' \to \mathbb{F}$ també, ja que $\beta\alpha\iota_A = \beta\iota_{A'}\eta = \iota_A\eta^{-1}\eta = \iota_A$. Aleshores de la unicitat se segueix que $\beta\alpha = \mathrm{id}_{\mathbb{F}}$. Podem fer l'argument simètric per deduir que $\alpha\beta = \mathrm{id}_{\mathbb{F}'}$. Per tant, $\mathbb{F} \cong \mathbb{F}'$.

$$\begin{tikzcd} A \arrow[r, hook, "\iota_A"] \arrow[d, hook, "\iota_A"'] & \mathbb{F} \\ \mathbb{F} \arrow[ur, dashed, "\beta\alpha=\mathrm{id}_{\mathbb{F}}"'] & \end{tikzcd} \qquad \begin{tikzcd} A' \arrow[r, hook, "\iota_{A'}"] \arrow[d, hook, "\iota_{A'}"'] & \mathbb{F}' \\ \mathbb{F}' \arrow[ur, dashed, "\alpha\beta=\mathrm{id}_{\mathbb{F}'}"'] & \end{tikzcd}$$

Veiem ara la implicació com a la dreta, suposem doncs, que $\mathbb{F} \cong \mathbb{F}'$. És fàcil veure que, si $\#A \geq \aleph_0$, llavors $\#\mathbb{F} = \#A$, usant el fet que la unió numerable de conjunts numerables és també numerable. Per tant, si $\#A, \#A' \geq \aleph_0$ el resultat és clar: $\#A = \#\mathbb{F} = \#\mathbb{F}' = \#A'$. Per tant, ens podem restringir al cas $\#A \leq \infty$.

Observem que, per cada grup G, la propietat universal de $\mathbb{F}$ ens dona una bijecció $\mathrm{Map}(A, G) \to \mathrm{Hom}(\mathbb{F}, \mathrm{G}), \varphi \mapsto \tilde{\varphi}$, entre el conjunt d'aplicacions d'A a G, i el conjunt de morfismes de grups de $\mathbb{F}$ a G, que té com a inversa la restricció $\phi_{|A} \leftarrow\!\!\dashv \phi$. Per tant aquests dos conjunts tenen el mateix cardinal, $\#\,\mathrm{Map}(A, G) = \#\,\mathrm{Hom}(\mathbb{F}, \mathrm{G})$. Aleshores com que per hipòtesi tenim $\mathbb{F} \cong \mathbb{F}'$, podem mirar les aplicacions i morfismes a $\mathbb{Z}/2\mathbb{Z}$ i en resulta:

$$2^{\#A} = \#\,\mathrm{Map}(A, \mathbb{Z}/2\mathbb{Z}) = \#\,\mathrm{Hom}(\mathbb{F}, \mathbb{Z}/2\mathbb{Z}) =$$
$$= \#\,\mathrm{Hom}(\mathbb{F}', \mathbb{Z}/2\mathbb{Z}) = \#\,\mathrm{Map}(A', \mathbb{Z}/2\mathbb{Z}) = 2^{\#A'},$$

d'on se segueix que $\#A = \#A'$. $\square$

Observació 2.20. Un grup lliure $\mathbb{F}$ pot ser-ho sobre diversos subconjunts seus $A, A' \subseteq \mathbb{F}$, però aleshores tots hauran de tenir el mateix cardinal $\#A = \#A'$. A més, donat que les bases de $\mathbb{F}$ són sistemes de generadors minimals, ara veiem que, de fet, són sistemes de generadors de cardinal mínim possible. En altres paraules, si A és base de $\mathbb{F}$, aleshores $\mathrm{rk}(\mathbb{F}) = \#A$. És per això que, llevat d'isomorfisme, tenim un sol grup lliure per a cada rang. Aleshores ens podem referir al grup lliure de rang p per $\mathbb{F}_p$, si no volem fer referència a cap base concreta.

Fixem-nos que aquesta situació és similar a la de l'àlgebra lineal: un espai vectorial E sobre un cos K pot tenir diverses bases, però en tot cas hauran de tenir sempre el mateix cardinal que és la dimensió de E sobre K. Com ja hem vist, hi ha grups lliures de qualsevol rang, de la mateixa manera que hi ha espais vectorials de qualsevol dimensió. No obstant això hi ha una diferència important: en àlgebra lineal tot espai vectorial té bases i, per tant, té una dimensió ben definida. En canvi, en el context dels grups, hi ha molts grups que no tenen cap base, és a dir, no són lliures sobre cap subconjunt. Un exemple d'això són els grups finits no trivials. Malgrat aquesta mancança dels grups lliures, igualment d'alguna manera contenen tota la informació possible sobre tots els grups possibles a través del concepte de presentació, tal com veurem a continuació.

Teorema 2.21. *Tot grup G és quocient d'un grup lliure. És a dir, que per a tot grup G existeixen un cardinal p i un subgrup $N \trianglelefteq \mathbb{F}_p$ tals que $G \cong \mathbb{F}_p/N$.*

Prova. Primer observem que donat un grup G sempre hi podem prendre algun conjunt de generadors A, ja que almenys $A = G$ clarament genera G. Aleshores sigui $A \subseteq G$ un conjunt de generadors de G i sigui $p = \#A$ el seu cardinal. Prenem A com un conjunt abstracte, i considerem el grup lliure $\mathbb{F}_A$. Per la propietat universal aplicada a la inclusió $\varphi : A \to G$, existeix un únic morfisme de grups $\tilde{\varphi} : \mathbb{F}_A \to G$ tal que $\tilde{\varphi}\iota_A = \varphi$, és a dir, que $\tilde{\varphi}([a]) = a$, per a tot $a \in A$.

$$\begin{tikzcd} A \arrow[r, hook, "\varphi"] \arrow[d, hook, "\iota_A"'] & G \\ \mathbb{F}_A \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

Com que A és un conjunt de generadors de G, $\tilde{\varphi}$ és exhaustiu i, pel primer teorema d'isomorfia, $N = \ker\tilde{\varphi}$ és un subgrup normal de $\mathbb{F}_A$ que satisfà $\mathbb{F}_A/N \cong \mathrm{Im}(\tilde{\varphi}) = G$. $\square$

Definició 2.22. Sigui G un grup, donat un subconjunt $R \subseteq G$, la seva **la clausura normal**, $\langle\langle R\rangle\rangle$, és el subgrup generat per tots els conjugats d'elements de R. Aleshores, per aquesta definició, clarament $\langle\langle R\rangle\rangle$ és un subgrup normal de G.

Definició 2.23. Sigui G un grup, una **presentació** per a G és un parell (A, R) on A és un conjunt de símbols, R és un subconjunt de $\mathbb{F}_A$, i $G \cong \mathbb{F}_A/\langle\langle R\rangle\rangle$. Fent un abús de llenguatge, se sol escriure $G = \langle A|R\rangle$, i es diu que els elements de A (resp., R) són els generadors (resp., relators) de G donats per la presentació $\langle A|R\rangle$, i que $w \in (A^{\pm})^*$ és una paraula en els generadors de G.

Diem que una presentació $\langle A|R\rangle$ és una **presentació finita** si A i R són conjunts finits. Diem que un grup és **finitament presentat** si admet una presentació finita.

Corol·lari 2.24. *El grup lliure amb base A admet la presentació* $\mathbb{F}_A = \langle A|-\rangle$. $\square$

Observació 2.25. A partir del teorema anterior 2.21, si fixem una base per $\mathbb{F}_p$ i una família de generadors de N com a subgrup normal de $\mathbb{F}_p$, hem obtingut el concepte de presentació. De fet, el teorema ens diu que tot grup admet una presentació (de fet, infinites presentacions). Podem interpretar aquest teorema de dues maneres diferents. Tenim que tota la informació algebraica d'un grup qualsevol està continguda en els reticles de subgrups normals dels grups lliures. Si bé això els fa molt útils a l'hora de buscar informació sobre qualsevol grup, també ens indica que contenen tota la complexitat del grup i que sovint serà difícil tractar-hi.

2.3 Mida de les boles del grup lliure

Acabarem aquest capítol estudiant algunes característiques més concretes del grup lliure. Ja hem vist abans que llevat d'isomorfisme tenim un grup lliure per a cada rang $p \geq 0$. Fixem-nos que els casos $p = 0$ i $p = 1$ són força especials, ja que són els únics rangs pels quals el grup lliure és abelià, en particular $\mathbb{F}_0 = \{1\}$ i $\mathbb{F}_1 = \langle\{a\}\rangle = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\} \cong \mathbb{Z}$. Per contra, per tot $p \geq 2$ podem fer un argument semblant al vist a l'exemple 2.10 per veure que $\mathbb{F}_p$ no és abelià. Acabem l'apartat amb una proposició en què veiem quina és la mida de les boles dels grups lliures per aquest darrer cas.

Proposició 2.26. *Donat el grup lliure de rang* $p \geq 2$, $\mathbb{F}_p$. *Anomenem* $S(n) = \{w \in \mathbb{F}_p \mid |w|_X = n\}$ *a l'esfera de radi* n *de* $\mathbb{F}_p$, *és a dir, el subconjunt de paraules reduïdes de, exactament,* n *lletres. Anomenem* $\mathbb{B}(n) = \{w \in \mathbb{F}_p \mid |w|_X \leq n\}$ *a la bola de radi* n *de* $\mathbb{F}_p$. *Aleshores, per* $n \geq 1$, *es té que*

$$\#S(n) = 2p(2p-1)^{n-1} \quad \text{i que} \quad \#B(n) = \frac{p(2p-1)^n - 1}{p-1}.$$

Per altra banda, sigui el conjunt de paraules de longitud parella fitada per un n, $\mathbb{B}^{par}(n) = \{w \in \mathbb{F}_p \mid 2 | |w|_X \leq n\}$, *i l'anàleg per les paraules de longitud senar,* $\mathbb{B}^{sen}(n) = \{w \in \mathbb{F}_p \mid 2 \nmid |w|_X \leq n\}$, *aleshores les seves mides són, si* n *és parell (i el cas* n *senar també queda definit per les mateixes igualtats):*

$$\#\mathbb{B}^{par}(n) = \#\mathbb{B}^{par}(n+1) = \frac{(2p-1)^{n+1} - 1}{2(p-1)} \quad i \quad \#\mathbb{B}^{sen}(n) = \#\mathbb{B}^{sen}(n-1) = \frac{(2p-1)^n - 1}{2(p-1)}.$$

Prova. Observem primer que qualsevol base lliure de $\mathbb{F}_p$ tindrà exactament $2p$ elements. Per trobar quantes paraules tenim a cada subconjunt, tindrem en compte només les paraules reduïdes per no repetir elements del grup lliure. Aleshores una paraula $s_1 s_2 \cdots s_n = s \in S(n)$ només té la restricció de què no pot tenir dos elements consecutius inversos, ja que sinó no seria reduïda. Així doncs, la primera lletra, s_1, pot ser qualsevol lletra de les $2p$ lletres de la base, i per les posicions posteriors, s_k amb $k \geq 2$, no es podrà prendre l'invers de la lletra anterior i per tant podrà prendre $2p - 1$ valors diferents. Així doncs, $\#S(n) = 2p(2p-1)^{n-1}$ per tot $n \geq 1$. Fixem-nos que $\#S(0) = 1$ ja que en aquest cas només conté la paraula buida.

Aleshores podem calcular quantes paraules hi ha de longitud fitada per n, és a dir, la mida de la bola $B(n)$. Observem que:

$$\#B(n) = \sum_{k=0}^{n} \#S(k) = 1 + \sum_{k=1}^{n} 2p(2p-1)^{k-1} = 1 + \sum_{k=0}^{n-1} 2p(2p-1)^k =$$

$$= 1 + 2p\frac{(2p-1)^n - 1}{(2p-1) - 1} = \frac{p(2p-1)^n - 1}{p-1}.$$

Calculem ara de manera similar les mides de $\mathbb{B}^{par}(n)$ i $\mathbb{B}^{sen}(n)$. Fixem-nos que per $n \geq 2$ parell, $\mathbb{B}^{par}(n) = \mathbb{B}^{par}(n+1)$ ja que $n+1$ és senar i per tant aquest augment de radi no ha afegit cap paraula parella. Igualment es dedueix $\mathbb{B}^{sen}(n) = \mathbb{B}^{sen}(n-1)$ ja que com que n és parell, reduint el radi a $n-1$ no hem tret cap de les paraules senars de la bola. Així doncs, en tenim prou amb fer els càlculs per n parell:

$$\mathbb{B}^{par}(n) = \sum_{k=0}^{n/2} \#S(2k) = 1 + \sum_{k=1}^{n/2} 2p(2p-1)^{2k-1} = 1 + 2p \sum_{k=0}^{(n/2)-1} (2p-1)^{2k+1} =$$

$$= 1 + 2p(2p-1) \sum_{k=0}^{(n/2)-1} ((2p-1)^2)^k = 1 + 2p(2p-1)\frac{((2p-1)^2)^{\frac{n}{2}} - 1}{(2p-1)^2 - 1} = \frac{(2p-1)^{n+1} - 1}{2(p-1)},$$

$$\mathbb{B}^{sen}(n) = \sum_{k=0}^{(n/2)-1} \#S(2k+1) = \sum_{k=0}^{(n/2)-1} 2p(2p-1)^{2k} = 2p \sum_{k=0}^{(n/2)-1} ((2p-1)^2)^k =$$

$$= 2p\frac{((2p-1)^2)^{\frac{n}{2}} - 1}{(2p-1)^2 - 1} = \frac{(2p-1)^n - 1}{2(p-1)}.$$

Observem, a més, que $\#\mathbb{B}(n) = \#\mathbb{B}^{par}(n) + \#\mathbb{B}^{sen}(n)$, com ha de ser, ja que $\mathbb{B}(n) = \mathbb{B}^{par}(n) \sqcup \mathbb{B}^{sen}(n)$.

□

Observació 2.27. Fixem-nos que la demostració anterior no ens servia en els casos $p = 0, 1$, però també podem calcular la mida de les boles del grup lliure per aquests rangs amb altres mètodes. Per $p = 0$ el grup lliure només té la paraula buida i per tant $\#\mathbb{F}_0 = 1$. Per $p = 1$ ja hem vist que $\mathbb{F}_p \cong \mathbb{Z}$, i per tant és senzill trobar la mida de les boles, ja que són les mateixes que pels enters: $\#S(0) = 1$ i per $n \geq 1$, $\#S(n) = 2$ i $\#\mathbb{B}(n) = 2n + 1$.

3. Grau de commutativitat de grups finitament generats

Aquest és el capítol central del treball, on revisarem el teorema principal de [1], d'Antolín, Martino i Ventura. Aquest teorema conté, en primer lloc, una generalització del teorema de Gustafson per a certs grups infinits de la manera que podríem esperar de manera natural, establint que si el seu grau de commutativitat és major a $5/8$, aleshores és que el grup és abelià. En segon lloc, també demostrarem que el grau de commutativitat d'un grup és positiu si i només si és virtualment abelià (és a dir, que conté un subgrup abelià d'índex finit). Fixem-nos que aquest és un resultat especialment interessant, ja que relaciona el grau de commutativitat, una propietat essencialment combinatòria, amb la virtualitat abeliana, una propietat essencialment algebraica i lligada a l'estructura intrínseca del grup. Com veurem, no podrem provar aquest resultat per a qualsevol grup, sinó que ens haurem de restringir a certs tipus de grups (concretament els grups finitament generats de creixement subexponencial i residualment finits), que igualment són molt més generals que els grups finits.

3.1 Generalització de la definició de grau de commutativitat

Per a treballar amb el grau de commutativitat de grups infinits, primerament hem de traslladar la noció de grau de commutativitat a grups infinits d'alguna manera coherent, però no ho podem fer directament a partir de la definició que hem donat per a grups finits perquè si $\#G = \infty$, llavors el grau de commutativitat tal com l'hem definit a la primera secció no estaria ben definit. Així doncs veurem primer com podem estendre el concepte de grau de commutativitat als grups infinits. Això sí, tot això no serà possible per qualsevol grup infinit, sinó que ens caldrà restringir-nos una mica més.

El que farem, doncs, és utilitzar les boles centrades en l'element neutre d'un grup. Per a grups finitament generats aquestes boles tenen un nombre finit d'elements i per tant hi podem calcular el grau de commutativitat tal com l'hem definit per a grups finits. Aleshores farem tendir el radi de les boles a infinit per tal de tenir boles cada cop més grans que acabin contenint tot el grup en el límit.

Definició 3.1. Sigui $G = \langle X \rangle$ un grup finitament generat i X un conjunt finit. El **grau de commutativitat de G respecte X**, denotat per $dc_X(G)$, és

$$dc_X(G) = \limsup_{n\to\infty} \frac{\#\{(u,v) \in \mathbb{B}_X(n) \times \mathbb{B}_X(n) \mid uv = vu\}}{\#\mathbb{B}_X(n)^2} \in [0,1],$$

on $\mathbb{B}_X(n) = \{g \in G \mid |g|_X \leq n\}$ és el conjunt dels elements de G que es poden expressar com paraules en X de longitud fitada per n.

Remarca. Aquesta és una definició de grau de commutativitat més general que la donada al primer capítol per a grups finits, ja que permet tots els grups finitament generats, que són molts més que només els finits. Pel que fa a la notació, com que aquesta definició es construeix a partir d'un conjunt X, denotarem el grau de commutativitat per $dc_X(G)$, mentre que seguirem denotant amb $dc(G)$ el cas per a grups finits donat a la definició 1.27. Fixem-nos però, que efectivament les dues definicions coincideixen en el cas dels grups finits, com és natural que sigui.

Prova. Efectivament, per tot grup finit G per tot conjunt de generadors X, per la finitud de G existirà un $N > 0$ tal que per tot $n > N$ es tindrà $G \subseteq \mathbb{B}_X(n)$, i aleshores $dc_X(G) = dc(G)$. $\square$

Remarca. Fixem-nos que un bon motiu per pensar que aquesta és una generalització raonable de la noció de grau de commutativitat a grups finitament generats és que hi ha un teorema anàleg al de Gustafson usant aquesta definició, tal com veurem més endavant al teorema 3.20, i s'obté exactament la mateixa fita per al grau de commutativitat de grups no abelians: 5/8.

De la definició de grau de commutativitat per a grups finitament generats que acabem de donar a 3.1 en sorgeixen naturalment un parell de qüestions a discutir. En primer lloc, hem escrit un $\limsup$ en lloc d'un $\lim$ perquè a priori no sabem si el límit hauria d'existir per qualsevol grup G i conjunt de generadors X, però és necessari realment? Doncs resulta que la qüestió és prou complicada: per una banda no s'ha trobat cap exemple on el límit no existeixi i sigui necessari fer el límit superior, però per altra banda, per ara tampoc s'ha trobat cap prova que demostri que el límit sempre existeixi. Així doncs, haurem de treballar amb el límit superior.

Fixem-nos també que la definició que hem donat de grau de commutativitat aparentment depèn del conjunt de generadors del grup, X. Això és així en general, però veurem en aquest capítol que hi ha certs tipus de grups en què per a qualsevol conjunt de generadors d'un grup s'obté el mateix grau de commutativitat. Això serà molt important perquè voldrà dir que el grau de commutativitat és una propietat inherent del grup. Aquesta qüestió, està estretament relacionada amb el creixement del grup.

Definició 3.2. Un grup finitament generat G és de **creixement subexponencial** si existeix algun conjunt de generadors $\langle X\rangle = G$ tal que $\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n+1)}{\#\mathbb{B}_X(n)} = 1$; i és de **creixement polinomial de grau** d, on d és un enter, si $0 < Cn^d \leq \#\mathbb{B}_X(n) \leq Dn^d$ per a certes constants C, D i d. Si $\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n+1)}{\#\mathbb{B}_X(n)} = \lambda > 1$ direm que el grup és de **creixement exponencial**.

Definició 3.3. Sigui $G = \langle X\rangle$ un grup finitament generat. Una aplicació $f_G : G \to \mathbb{N}$ és una **estimació de la X-mètrica** si $\exists K > 0$ tal que $\forall w \in G$ es té que

$$\frac{1}{K} f(w) \leq |w|_X \leq K f(w).$$

Proposició 3.4. *Si tenim X i Y dos conjunts finits generadors d'un grup $G = \langle Y\rangle = \langle X\rangle$, aleshores $|\cdot|_Y$ és una estimació de la X-mètrica i $|\cdot|_X$ és una estimació de la Y-mètrica.*

Prova. Com que $G = \langle Y\rangle$, aleshores tot $x \in X \subseteq G$ és igual a algun producte finit d'elements de Y, $x = y_{j_1} \cdots y_{j_{|x|_Y}}$, on la llargada d'aquest producte, $|x|_Y$, depèn, és clar, de x. Podem prendre un $k_1 \geq \max_{x\in X}\{|x|_Y\}$ que sigui no nul (hem pogut fer el màxim perquè X és un conjunt finit). Si prenem ara un $w \in G$ qualsevol, el podem expressar com a producte de $|w|_X$ elements de X, $w = x_{i_1} \cdots x_{i_{|w|_X}}$. Utilitzant però l'expressió dels $x \in X$ com a producte d'elements de Y tenim:

$$|w|_Y = |x_{i_1} \cdots x_{i_{|w|_X}}|_Y \leq |x_{i_1}|_Y + \cdots + |x_{i_{|w|_X}}|_Y \leq k_1 |w|_X \Rightarrow \frac{1}{k_1}|w|_Y \leq |w|_X.$$

Fent un argument simètric intercanviant el paper de X i Y podem obtenir un $k_2 > 0$ tal que $|w|_X \leq k_2|w|_Y$. Llavors, per a $K = \max\{k_1, k_2\} > 0$, se satisfà

$$\frac{1}{K}|w|_Y \leq \frac{1}{k_1}|w|_Y \leq |w|_X \leq k_2|w|_Y \leq K|w|_Y,$$

i per tant $|\cdot|_Y$ és una estimació de la X-mètrica. Fixem-nos que es té $\frac{1}{K}|w|_Y \leq |w|_X \Rightarrow |w|_Y \leq K|w|_X$ i que $|w|_X \leq K|w|_Y \Rightarrow \frac{1}{K}|w|_X \leq |w|_Y$, i per tant també $|\cdot|_X$ és una estimació de la Y-mètrica, i ja satisfà les desigualtats per la mateixa $K > 0$. $\square$

Observació 3.5. Si un grup G és de creixement polinomial per un sistema de generadors X, aleshores per qualsevol altre conjunt de generadors Y, també ho serà. Per tant, el creixement polinomial d'un grup és independent del conjunt de generadors triat.

Prova. De la proposició anterior tenim que existeix una constant K tal que $\mathbb{B}_Y(n) \subseteq \mathbb{B}_X(Kn)$. Per ser G de creixement polinomial respecte X existeixen constants D i d tals que $\#\mathbb{B}_X(n) \leq Dn^d$. Aleshores:

$$\#\mathbb{B}_Y(n) \leq \#\mathbb{B}_X(Kn) \leq D(Kn)^d = (DK^d)n^d.$$

Anàlogament es pot trobar una fita inferior, i per tant G també és de creixement polinomial de grau d respecte el conjunt de generadors Y. □

Definició 3.6. Sigui G un grup i sigui $f : G \to \mathbb{N}$ una aplicació. Definim la f-**bola** i el f-**grau de commutativitat** com:

$$\mathbb{B}_f(n) = \{w \in G \mid f(w) \leq n\},$$

$$dc_f(G) = \limsup_{n\to\infty} \frac{\#\{(u,v) \in \mathbb{B}_f(n) \times \mathbb{B}_f(n) \mid uv = vu\}}{\#\mathbb{B}_f(n)^2}.$$

Proposició 3.7. *Sigui $G = \langle X \rangle$ un grup de creixement polinomial, i sigui $f : G \to \mathbb{N}$ una estimació de la X-mètrica. Aleshores*

$$dc_X(G) > 0 \iff dc_f(G) > 0.$$

Prova. De f estimació de la X-mètrica tenim que $\exists K > 0$ tal que $f(w) \leq K|w|_X \leq K^2 f(w)$, d'on deduïm que $\mathbb{B}_f(n) \subseteq \mathbb{B}_X(Kn) \subseteq \mathbb{B}_f(K^2 n)$. És a dir, que podem posar una f-bola dins d'una bola respecte un conjunt de generadors X i viceversa modificant el radi per una certa constant. A partir de la primera inclusió de boles $\mathbb{B}_f(n) \subseteq \mathbb{B}_X(Kn)$, obtenim

$$\#\{(u,v) \in (\mathbb{B}_f(n))^2 \mid uv = vu\} \leq \#\{(u,v) \in (\mathbb{B}_X(Kn))^2 \mid uv = vu\}$$

$$\frac{\#\{(u,v) \in (\mathbb{B}_f(n))^2 \mid uv = vu\}}{\#\mathbb{B}_X(Kn)^2} \leq \frac{\#\{(u,v) \in (\mathbb{B}_X(Kn))^2 \mid uv = vu\}}{\#\mathbb{B}_X(Kn)^2}$$

$$\left(\frac{\#\{(u,v) \in (\mathbb{B}_f(n))^2 \mid uv = vu\}}{\#\mathbb{B}_f(n)^2}\right)\left(\frac{\#\mathbb{B}_f(n)}{\#\mathbb{B}_X(Kn)}\right)^2 \leq \frac{\#\{(u,v) \in (\mathbb{B}_X(Kn))^2 \mid uv = vu\}}{\#\mathbb{B}_X(Kn)^2},$$

i si prenem el límit superior a ambdós costats, obtenim que

$$dc_f(G) \limsup_{n\to\infty} \left(\frac{\#\mathbb{B}_f(n)}{\#\mathbb{B}_X(Kn)}\right)^2 \leq dc_X(G).$$

Fixem-nos que a més $\limsup_{n\to\infty} \left(\frac{\#\mathbb{B}_f(n)}{\#\mathbb{B}_X(Kn)}\right)^2 > 0$, perquè

$$\frac{\#\mathbb{B}_f(n)}{\#\mathbb{B}_X(Kn)} \geq \frac{\#\mathbb{B}_X(n/K)}{\#\mathbb{B}_X(Kn)} \geq \frac{C(n/K)^d}{D(Kn)^d} = \frac{C}{DK^{2d}} > 0,$$

on hem usat que $\mathbb{B}_f(n) \subseteq \mathbb{B}_X(n/K)$ i també que $G = \langle X \rangle$ és de creixement polinomial. I per tant, per la desigualtat anterior entre els graus de commutativitat tenim que $dc_X(G) = 0 \Rightarrow dc_f(G) = 0$. L'altra implicació es prova fent un procés anàleg però partint de la inclusió de boles $\mathbb{B}_X(Kn) \subseteq \mathbb{B}_f(K^2 n)$. □

Remarca. Observem que com que el grau de commutativitat no pot prendre valors negatius per la seva definició, el resultat de la proposició anterior sota les mateixes hipòtesis, és equivalent a

$$dc_X(G) = 0 \iff dc_f(G) = 0.$$

Corol·lari 3.8. *Per dos conjunts de generadors finits d'un grup de creixement polinomial $\langle X \rangle = \langle Y \rangle = G$, es té que*

$$dc_X(G) = 0 \iff dc_Y(G) = 0.$$

Prova. Es dedueix directament del resultat anterior i del fet que si un grup té dos conjunts de generadors finits $\langle X \rangle = \langle Y \rangle = G$, aleshores $|\cdot|_Y$ és una estimació de la X-mètrica, tal com hem vist a la proposició 3.4. □

Definició 3.9. Siguin $\langle Y \rangle = H \leq G = \langle X \rangle$. El subgrup H és **no distorsionat** si $\exists K > 0$ tal que $\forall h \in H$, $\frac{1}{K}|h|_Y \leq |h|_X \leq K|h|_Y$.

Remarca. Observem que si $\langle Y \rangle = H \leq G = \langle X \rangle$ és un subgrup no distorsionat, $|\cdot|_X$ restringit a H és una estimació de la Y-mètrica per H.

Corol·lari 3.10. *Sigui $G = \langle X \rangle$ un grup de creixement polinomial i $\langle Y \rangle = H \leq G$ un subgrup no distorsionat. Aleshores,*

$$dc_X(H) = 0 \iff dc_Y(H) = 0.$$

Prova. Com que si H és un subgrup no distorsionat de G, aleshores $|\cdot|_X$ restringit a H és una estimació de la Y-mètrica per H, llavors el resultat se segueix directament de la proposició 3.7. □

3.2 Subgrups d'índex finit

Per tal de poder demostrar el teorema principal del capítol, haurem de fer servir alguns resultats per a grups d'índex finit, que veurem en aquesta secció. A continuació introduirem dues definicions que ens serviran per a demostrar el lema de Burillo-Ventura [2], el primer d'aquests resultats. Es tracten del grafs de Cayley i de Schreier, que constitueixen una manera natural de descriure l'estructura dels grups i d'una manera geomètrica i no tan combinatòria com havíem anat veient fins ara.

Definició 3.11. Siguin G un grup i $X \subseteq G$ un conjunt de generadors de G. Aleshores, el **graf de Cayley respecte** X, que anomenarem $\mathrm{Cay}(G, X)$, és el graf dirigit (o digraf) amb conjunt de vèrtexs X, i un arc $g \xrightarrow{x} gx$ per a cada element $g \in G$ i cada generador $x \in X^{\pm}$.

Definició 3.12. Donat un grup, G, un conjunt de generadors del grup, X, i un subgrup $H \leq G$, el **graf de Schreier (per l'esquerra) de** H **respecte a** X, que designarem per $\mathrm{Sch}_G(H, X)$, és el graf que té per conjunt de vèrtexs el conjunt de classes laterals per l'esquerra de G mòdul H, G/H, i un arc $gH \xrightarrow{x} xgH$ per cada classe lateral $gH \in G/H$ i per cada element $x \in X^{\pm}$, i la classe lateral H com a vèrtex base.

Remarca. Independentment del conjunt de generadors triat, X, qualsevol element del grup G pot ser expressat com un producte d'elements de X, per tant de la definició del graf de Cayley de G respecte X, se segueix que $\mathrm{Cay}(G, X)$ és un graf connex. Aquesta connexió també l'hereta, per a qualsevol subgrup $H \leq G$, el graf de Schreier de H respecte a X, $\mathrm{Sch}_G(H, X)$.

Observació 3.13. Donat un grup, G, i un conjunt de generadors del grup, X, si prenem el subgrup $H = \{1\} \leq G$, fixem-nos que aleshores $\mathrm{Sch}_G(H, X) = \mathrm{Cay}(G, X)$.

Prova. Es dedueix directament de la definició del graf de Schreier i de que $G/\{1\} = G$. $\square$

Lema 3.14 (Burillo-Ventura, 2002 [2])**.** *Sigui G un grup de creixement subexponencial i $H \leq_{f.i.} G$ un subgrup d'índex finit, aleshores per tot $g \in G$ existeix*

$$\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n) \cap gH}{\#\mathbb{B}_X(n)} = \lim_{n\to\infty} \frac{\#\mathbb{B}_X(n) \cap Hg}{\#\mathbb{B}_X(n)} = \frac{1}{[G:H]}.$$

Prova. Sigui $X = \{g_1, g_2, \dots, g_p\}$ un conjunt finit de generadors de G de creixement subexponencial, sigui $\Gamma = \mathrm{Cay}(G, X)$ el graf de Cayley de G respecte de X, i sigui $\Gamma' = \mathrm{Sch}_G(H, X)$ el graf de Schreier de H en G respecte de X. Observem primer que els dos són grafs clarament connexos, i a més hi ha una aplicació natural de $\pi : \Gamma \to \Gamma', g \mapsto gH$, que envia cada element a la seva classe lateral per l'esquerra. Veurem ara que Γ és un espai recobridor de Γ' per l'aplicació π, és a dir, que existeix un espai discret D tal que per tot $gH \in \Gamma'$ existeix un entorn $U \subseteq \Gamma'$ tal que $\pi^{-1}(U) = \bigsqcup_{d\in D} V_d$ i $\pi_{|V_d} : V_d \to U$ és un homeomorfisme per tot $d \in D$. Siguin $H = y_0H, y_1H, y_2H, \dots, y_pH$ les classes de G/H (vèrtexs de Γ') amb $p = [G : H] - 1 < \infty$ i on prenem $y_0 = 1$ i representants $\{y_0, \dots, y_p\}$ tals que que formin un subgraf connex en Γ, i fixem-nos que els podem prendre així ja que Γ' és connex. Tenim, llavors, que tots els y_i han de ser diferents perquè sinó dues classes serien iguals, i també que els $y_i \notin H$, ja que sinó tindríem que y_iH seria la mateixa classe que H. Com que H és finitament generat podem ordenar els seus elements $H = \{1, h_1, h_2, \dots\}$, i prendre $D = H$ i $V_d = V_{h_d} = \{y_ih_d \mid i = 0, \dots, p\}$. Fixem-nos que per aquests V_d, π és un recobriment, ja que si prenem $U = \Gamma'$, tot element $g \in G$ és de la forma $g = y_ih_d$ per a certs i i d, ja que pertany a una classe d'equivalència, i a més els conjunts V_d són tots clarament disjunts entre ells i tots isomorfs a Γ'. I per tant Γ és un espai recobridor de Γ'.

Ara com que el graf Γ' té $[G : H] < \infty$ vèrtexs i és connex, podem triar $T \subseteq \Gamma'$ un subgraf que sigui un arbre maximal en Γ', anomenem C al diàmetre de T (és a dir, la màxima distància entre dos vèrtexs qualssevol de T). Aleshores com que Γ és un espai recobridor de Γ' podem aixecar el subgraf $T \subseteq \Gamma'$ en Γ, i per cada $h_d \in H$ hi ha un únic subarbre de $V_d \subseteq \Gamma$, que anomenarem T_h, i que és isomorf a T. Fixem-nos que dos d'aquests subarbres són disjunts ja que són subconjunts de conjunts disjunts. A més la unió de tots els T_h cobreix tot el grup G, ja que per tot $g \in G$ $\exists y_i \in Y$ tal que $g \in y_iH$, i per tant $\exists h_d \in H$ tal que $g = y_ih_d \in T_{h_d}$. Tenim, doncs, que cada vèrtex de Γ pertany a un i només un T_h.

Fent servir els arbres T_h, el seu diàmetre C, i la desigualtat triangular, podem deduir que un element (vèrtex) qualsevol $x \in T_h$ té longitud $|x|_X \leq |h|_X + |x-h|_X \leq n+C$ i també $|x|_X \geq ||h|_X + |x-h|_X| \geq n-C$, on $n = |x|_X$. Aleshores se satisfan les inclusions:

$$\mathbb{B}_X(n-C) \subseteq \bigsqcup_{h\in H\cap B_X(n)} V(T_h) \subseteq B_X(n+C),$$

on $V(T_h)$ és el conjunt de vèrtexs de T_h. Prenent cardinals,

$$\#\mathbb{B}_X(n-C) \leq \#H \cap B_X(n) \cdot [G:H] \leq \#B_X(n+C).$$

Dividint per $\#\mathbb{B}_X(n)$ obtenim:

$$\frac{\#\mathbb{B}_X(n-C)}{\#\mathbb{B}_X(n)} \leq \frac{\#H \cap B_X(n) \cdot [G:H]}{\#\mathbb{B}_X(n)} \leq \frac{\#B_X(n+C)}{\#\mathbb{B}_X(n)}.$$

Fem ara a tots els termes el límit quan n tendeix a infinit. Fixem-nos que a causa del creixement subexponencial de X tenim que

$$\lim_{n\to\infty} \frac{\#B_X(n+C)}{\#\mathbb{B}_X(n)} = \prod_{i=0}^{C-1} \lim_{n\to\infty} \frac{\#B_X(n+i+1)}{\#\mathbb{B}_X(n+i)} = \prod_{i=0}^{C-1} 1 = 1 \quad \text{i que} \quad \lim_{n\to\infty} \frac{\#B_X(n-C)}{\#\mathbb{B}_X(n)} = 1,$$

on el segon límit es dedueix de manera anàloga. Així doncs, com que el primer i el tercer terme de la desigualtat tendeixen a 1 (i que l'argument donat es pot fer anàlogament per totes les classes laterals de H), obtenim que per tot $g \in G$, es té:

$$\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n) \cap gH}{\#\mathbb{B}_X(n)} = \lim_{n\to\infty} \frac{\#\mathbb{B}_X(n) \cap Hg}{\#\mathbb{B}_X(n)} = \frac{1}{[G:H]}.$$

□

Remarca. Una hipòtesi de 3.14 és que el grup G té creixement subexponencial. Veurem a continuació que això no és a causa d'una restricció tècnica a l'hora de fer la demostració en un cas més general, sinó que, efectivament, existeixen grups amb creixement exponencial pels quals no existeix el límit de l'enunciat.

Prova. Farem servir l'exemple dels grups lliures de rang $p \geq 2$, $\mathbb{F}_p$, aprofitant que ja els hem estudiat força. Usarem en particular la proposició 2.26, que ens dona els cardinals de les boles dels grups lliures de rang $p \geq 2$, i dels subconjunts fitats de paraules parelles i senars. Fixem-nos en primer lloc que per aquests grups tenim

$$\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n+1)}{\#\mathbb{B}_X(n)} = \lim_{n\to\infty} \frac{(p(2p-1)^{n+1}-1)/(p-1)}{(p(2p-1)^n-1)/(p-1)} = 2p-1 \geq 3,$$

i per tant $\mathbb{F}_p$ és un grup de creixement exponencial. Ara, sigui X una base lliure de $\mathbb{F}_p$, agafem el subgrup de les paraules de longitud parell, $H = \{w \in \mathbb{F}_p \mid 2 | |w|_X\} \leq_2 \mathbb{F}_p$. Fixem-nos que l'index de H és clarament 2, doncs només té dues classes laterals en $\mathbb{F}_p$, que corresponen a les paraules de longituds parelles i imparelles respectivament. A continuació però, veurem que

$$\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n) \cap H}{\#\mathbb{B}_X(n)} \neq \frac{1}{[G:H]} = \frac{1}{2}.$$

Ho farem veient que hi ha dues successions parcials que no convergeixen al mateix límit. Agafem la successió parcial dels n parells i la dels n senars. Pel cas de n senar, recordem que teníem $\#\mathbb{B}_X^{par}(n) = \#\mathbb{B}_X^{par}(n-1)$:

$$\lim_{\substack{n \text{ senar} \\ n\to\infty}} \frac{\#\mathbb{B}_X(n) \cap H}{\#\mathbb{B}_X(n)} = \lim_{\substack{n \text{ senar} \\ n\to\infty}} \frac{\#\mathbb{B}_X^{par}(n-1)}{\#\mathbb{B}_X(n)} = \lim_{\substack{n \text{ senar} \\ n\to\infty}} \frac{((2p-1)^n - 1/(2(p-1))}{(p(2p-1)^n-1)/(p-1)} = \frac{1}{2p} \overset{p\geq 2}{\leq} \frac{1}{4}.$$

Pel cas de n parell, aleshores:

$$\lim_{\substack{n \text{ parell} \\ n\to\infty}} \frac{\#\mathbb{B}_X(n) \cap H}{\#\mathbb{B}_X(n)} = \lim_{\substack{n \text{ parell} \\ n\to\infty}} \frac{\#\mathbb{B}_X^{par}(n)}{\#\mathbb{B}_X(n)} = \lim_{\substack{n \text{ parell} \\ n\to\infty}} \frac{((2p-1)^{n+1} - 1/(2(p-1))}{(p(2p-1)^n-1)/(p-1)} = \frac{2p-1}{2p} \overset{p\geq 2}{\geq} \frac{3}{4}.$$

Per tant, hem vist que aquestes dues parcials no convergeixen al mateix límit, i per tant el límit de la successió no pot existir. És més, de fet les dues successions parcials estan uniformement allunyades de $\frac{1}{2}$. □

Proposició 3.15. *Siguin* $\langle Y\rangle = H \leq_{f.i.} G = \langle X\rangle$ *amb* G *de creixement subexponencial. Aleshores,*

$$dc_X(G) \geq \frac{1}{[G:H]^2} dc_X(H).$$

Si a més el creixement és polinomial, aleshores també se satisfà $dc_Y(H) > 0 \Rightarrow dc_X(H) > 0 \Rightarrow dc_X(G) > 0$.

Prova. Com que $H \cap \mathbb{B}_X(n) \subseteq \mathbb{B}_X(n)$, tenim que $\#\{(u,v) \in (\mathbb{B}_X(n))^2 \mid uv = vu\} \geq \#\{(u,v) \in (H \cap \mathbb{B}_X(n))^2 \mid uv = vu\}$. Aleshores per tot $\epsilon > 0$ existeix un $n > 0$ prou gran tal que

$$\frac{\#\{(u,v) \in (\mathbb{B}_X(n))^2 \mid uv = vu\}}{\#\mathbb{B}_X(n)^2} = \frac{\#\{(u,v) \in (H \cap \mathbb{B}_X(n))^2 \mid uv = vu\}}{\#(H \cap \mathbb{B}_x(n))^2} \cdot \frac{\#(H \cap \mathbb{B}_x(n))^2}{\#\mathbb{B}_X(n)^2} \geq$$

$$\frac{\#\{(u,v) \in (H \cap \mathbb{B}_X(n))^2 \mid uv = vu\}}{\#(H \cap \mathbb{B}_x(n))^2} \cdot \left(\frac{1}{[G:H]} - \epsilon\right)^2,$$

on hem usat el Lema de Burillo-Ventura (3.14). Si prenem límits superiors a ambdós costats obtenim $dc_X(G) \geq dc_X(H)\left(\frac{1}{[G:H]} - \epsilon\right)^2$. I com que això és cert per tot ϵ, fent tendir $\epsilon \to 0$ obtenim que $dc_X(G) \geq \frac{1}{[G:H]^2} dc_X(H)$, tal com volíem veure. En particular, obtenim com a conseqüència, utilitzant també 3.10, que $dc_Y(H) > 0 \Rightarrow dc_X(H) > 0 \Rightarrow dc_X(G) > 0$. □

Remarca. La hipòtesi del creixement polinomial és necessària perquè és una hipòtesi de la proposició 3.10 esmentada.

A continuació veurem un altre resultat, que és semblant a la desigualtat del teorema de Gallagher que hem vist al primer capítol per a grups finits 1.34, però per a grups infinits. Tot i així, fixem-nos també que no és un resultat totalment anàleg, sinó que en aquesta versió de per a grups infinits, la desigualtat és una mica més laxa.

Lema 3.16. *Sigui* $G = \langle X\rangle$ *un grup de creixement subexponencial. Aleshores per tot quocient finit* G/N, *tenim que* $dc_X(G) \leq dc(G/N)$.

Prova. Sigui $N \trianglelefteq G$ un subgrup normal de G amb índex finit $[G:N] = d$. Pel Lema de Burillo-Ventura 3.14 tenim que $\forall g \in G$ se satisfà, independentment de X i g, que

$$\lim_{n\to\infty} \frac{\#\mathbb{B}_X(n) \cap gN}{\#\mathbb{B}_X(n)} = \frac{1}{d}.$$

Però a més, com que $\#G/N < \infty$, hi ha un número finit de classes laterals del quocient G/N, i per tant el límit és uniforme sobre g. És a dir, que $\forall \epsilon > 0\ \exists n_0\ \forall n \geq n_0$ i $\forall g \in G$ es té que

$$\left(\frac{1}{d} - \epsilon\right) \#\mathbb{B}_X(n) \leq \#gN \cap \mathbb{B}_X(n) \leq \left(\frac{1}{d} + \epsilon\right) \#\mathbb{B}_X(n). \tag{1}$$

Suposem ara que $dc_X(G) > dc(G/N)$ i arribarem a una contradicció. Per definició, això vol dir que $\exists \delta > 0$ tal que

$$dc(G/N) + \delta < \frac{\#\{(u,v) \in (\mathbb{B}_X(n))^2 \mid uv = vu\}}{\#\mathbb{B}_X(n)^2},$$

per infinits n. Sigui ara $\epsilon > 0$ prou petit tal que $2\epsilon d + \epsilon^2 d^2 \leq \delta$. Aleshores existirà un $n > 0$ prou gran tal que a més també se satisfarà 1, i usant tot això tenim

$$dc(G/N) + \delta < \frac{\#\{(u,v) \in (\mathbb{B}_X(n))^2 \mid uv = vu\}}{\#\mathbb{B}_X(n)^2} \leq$$

$$\leq \frac{1}{\#\mathbb{B}_X(n)^2} \#\{(\overline{u},\overline{v}) \in (G/N)^2 \mid \overline{uv} = \overline{vu}\} \left(\frac{1}{d} + \epsilon\right)^2 \#\mathbb{B}_X(n)^2,$$

on a la darrera desigualtat hem usat que si mirem els elements que commuten en el quocient G/N i els multipliquem per una fita superior del nombre d'elements de qualsevol classe de G/N (que obtenim de la segona desigualtat de l'equació 1), aleshores tenim un nombre d'elements superior al de la bola $\mathbb{B}_X(n)$. Aleshores, si seguim amb la cadena de desigualtats, simplificant la darrera expressió, obtenim que

$$dc(G/N) + \delta < \#\{(\overline{u},\overline{v}) \in (G/N)^2 \mid \overline{uv} = \overline{vu}\} \frac{1}{d^2} (1 + \epsilon d)^2$$

$$\leq \#\{(\overline{u},\overline{v}) \in (G/N)^2 \mid \overline{uv} = \overline{vu}\} \frac{1}{d^2} + 2\epsilon d + \epsilon^2 d^2$$

$$\leq dc(G/N) + \delta,$$

que és una contradicció.

□

Definició 3.17. Un grup G és **residualment finit** si, per tot element no trivial $1 \neq g \in G$, existeix un quocient finit de G tal que la imatge de g hi és no trivial.

Observació 3.18. Donat $G = \langle X \rangle$ un grup finitament generat i un natural n, hi ha un nombre finit de subgrups de G d'índex n.

Prova. Veiem primer que donat un grup qualsevol G (finitament generat o no), un subgrup $H \leq G$ d'índex finit n et dóna un homomorfisme de G a S_n, el grup simètric d'ordre n.

Per veure-ho, considerem l'acció per multiplicació esquerra de G en les classes laterals de H. Al ser H d'índex n, podem enumerar les classes laterals de H per $1, 2, \ldots, n$ d'alguna manera, utilitzant 1 per a la classe $1H = H$. Aleshores observem que qualsevol $g \in G$ permuta les classes laterals portant xH a gxH. A més, l'aplicació $f : G \to S_n$ que construïm d'aquesta manera, és un homomorfisme. Efectivament, considerem $g_1, g_2 \in G$ amb $f(g_1), f(g_2)$ les seves respectives permutacions associades, donada una classe xH tenim que f preserva l'operació ja que $f(g_1) \circ f(g_2)(xH) = f(g_1)(g_2 xH) = g_1 g_2 xH = f(g_1 g_2)(xH)$; i a més la identitat es preserva ja que $f(1)(xH) = 1xH = xH$.

A més, diferents subgrups d'índex n et donen homomorfismes diferents. Això és perquè pots recuperar H d'aquesta representació permutacional: és exactament l'estabilitzador de 1, $H = \mathrm{Stab}(1) = \{g \in G \mid gH = H\}$. Un element de G deixa H inalterat precisament quan està en H. Per tant, el nombre de subgrups d'índex n en G no és més gran que el nombre d'homomorfismes $G \to S_n$.

Ara, finalment, utilitzem la suposició que G és finitament generat per observar que només pot haver-hi un nombre finit d'aquests homomorfismes, ja que qualsevol homomorfisme està determinat pels seus valors en els generadors i només hi ha un nombre finit de llocs on pots portar cada generador.

Així doncs, un grup finitament generat admet només un nombre finit d'homomorfismes a S_n i, en conseqüència, un nombre finit de subgrups d'índex n. □

Proposició 3.19. *Un grup G que sigui finitament generat i residualment finit satisfà que per tot element no trivial $1 \neq g \in G$, hi ha un subgrup característic en G (és a dir, que és invariant sota qualsevol automorfisme de G) d'índex finit que no conté g.*

Prova. Sigui G un grup residualment finit, aleshores sabem que per tot element no trivial $1 \neq g \in G$, existeix un quocient finit de G tal que la imatge de g hi és no trivial. Fixem-nos que això és equivalent a dir que per tot $g \neq 1$, existeix un subgrup normal d'índex finit tal que $g \notin N$. Fixem-nos ara, que si a més usem la hipòtesi de que G és finitament generat, podem prendre un subgrup que sigui característic. Efectivament, prenem $K = \bigcap_{i=1}^{k} H_i$, la intersecció de tots els subgrups d'índex igual a N, que hem anomenat H_i, per $i = 1, \dots, k$, que n'hi ha finits per l'observació anterior, i que per tant K és d'índex finit. Veiem ara que K també ha de ser característic. Si $f : G \to G$ és un automorfisme, fixem-nos que aleshores la imatge d'un subgrup d'índex finit concret $H \leq_{f.i.} G$, ha de ser també un subgrup amb el mateix índex, $f(H) \leq_{f.i.} G$. I tenint en compte que un automorfisme és bijectiu, les imatges de tots els subgrups d'un índex finit concret, han de ser els mateixos subgrups permutats. Aleshores, per tot f automorfisme, es té que

$$f(K) = f\left(\bigcap_{i=1}^{k} H_i\right) = \bigcap_{i=1}^{k} f(H_i) = \bigcap_{i=1}^{k} H_i = K,$$

i per tant K és característic. A més, $g \notin K$ ja que teníem que $g \notin N$.

□

3.3 Teorema d'Antolín-Martino-Ventura

Amb tots els resultats previs que ja hem vist en aquest capítol i al llarg del treball, ja estem a punt per demostrar el teorema principal del treball.

Teorema 3.20 (Antolín, Martino i Ventura, 2017 [1]). *Sigui $G = \langle X \rangle$ un grup de creixement subexponencial i residualment finit. Aleshores*

(i) $dc_X(G) > 5/8 \Rightarrow G$ *és abelià;*

(ii) $dc_X(G) > 0 \iff G$ *és virtualment abelià, és a dir que existeix un subgrup d'índex finit $H \leq_{f.i.} G$ tal que H és abelià.*

En particular, (i) i (ii) son certs per grups de creixement polinomial.

Prova. Demostrem primer *(i)*. Sigui G un grup amb $dc_X(G) > 5/8$. Aleshores del lema 3.16 se segueix que tots els quocients finits Q de G tenen grau de commutativitat major a $5/8$ i com que són finits, del teorema de Gustaffson 1.28 en resulta que són abelians. Aleshores suposem que existeixen $g_1, g_2 \in G$ tals que no commuten, és a dir que $g_1 g_2 g_1^{-1} g_2^{-1} \neq 1$ és un element no trivial. Com que G és residualment finit, això voldria dir que $g_1 g_2 g_1^{-1} g_2^{-1} \neq 1$ és un element no trivial d'un quocient finit $Q = G/N$, fet que és contradicció amb Q abelià. Concloem doncs que G és abelià.

Per demostrar *(ii)*, veiem primer la implicació cap a l'esquerra. Així doncs, suposem que G té un subgrup abelià d'índex finit $H \leq_{f.i.} G$. Aleshores, per la proposició 3.15, tenim que

$$dc_X(G) \geq \frac{1}{[G:H]^2} dc_X(H) = \frac{1}{[G:H]^2} > 0.$$

Per veure la implicació cap a la dreta, demostrarem el contrarecíproc. Suposem, doncs, que G no és virtualment abelià, i veurem que aleshores $dc_X(G) = 0$. Sabem que G és finitament generat, residualment finit i que no és virtualment abelià. Per tant, podem triar dos elements que no commutin $g_1, g_2 \in G$ i un subgrup característic d'índex finit $K_1 \trianglelefteq G$, per la proposició 3.19, tal que $g_1 g_2 g_1^{-1} g_2^{-1} \notin K_1$, i aleshores com que G/K_1 és finit i no abelià, es té que $dc(G/K_1) < 5/8$ per Gustaffson. Però clarament aquestes tres propietats (ser finitament generat, residualment finit i no ser virtualment abelià) són heretades per subgrups d'índex finit. Aleshores podem repetir successivament aquesta construcció i obtenir la seqüència descendent

$$G = K_0 \trianglerighteq K_1 \trianglerighteq K_2 \trianglerighteq \cdots \trianglerighteq K_{i-1} \trianglerighteq K_i \trianglerighteq \cdots,$$

on cadascun és subgrup característic d'índex finit respecte l'anterior i per tant $dc(K_i/K_{i+1}) \leq 5/8$. Ara, com que tots els K_i són característics respecte l'anterior, i ser subgrup característic és transitiu, en particular també són característics a G, i això implica que també són subgrups normals a G. Llavors podem fer els quocients G/K_i, i com que pel tercer teorema d'isomorfisme tenim que $(G/K_i)/(K_{i-1}/K_i) = G/K_{i-1}$, el teorema de Gallagher 1.34 ens diu que

$$dc(G/K_i) \leq dc(K_{i-1}/K_i) dc(G/K_{i-1}) \leq \frac{5}{8} dc(G/K_{i-1}),$$

per tot $i \geq 1$. Per inducció tenim que $dc(G/K_i) \leq (5/8)^i$, i aleshores, pel lema 3.16 que ja hem mencionat, tenim que

$$dc_X(G) \leq dc(G/K_i) \leq (5/8)^i.$$

Com que això és cert per tot $i \geq 1$, concloem que $dc_X(G) = 0$.

□

Remarca. Fixem-nos que el teorema de Gustafson 1.28 és un cas particular del resultat que acabem de demostrar.

Recordem que quan hem definit el grau de commutativitat per a grups finitament generats hem fet una petita discussió sobre si era necessari fer servir el límit superior o si podíem assegurar que el límit existia. Doncs en el següent corol·lari veiem un dels casos en què sí que existeix el límit.

Corol·lari 3.21. *Sigui G un grup finitament generat, de creixement subexponencial i residualment finit, i sigui X un conjunt finit de generadors de G. Aleshores el límit*

$$dc_X(G) = \lim_{n\to\infty} \frac{\#\{(u,v) \in \mathbb{B}_X(n) \times \mathbb{B}_X(n) \mid uv = vu\}}{\#\mathbb{B}_X(n)^2}$$

existeix i no depèn del conjunt de generadors X.

Prova. Fixem-nos que el grup G satisfà les hipòtesis del teorema d'Antolín-Martino-Ventura, i aleshores tenim que el seu grau de commutativitat per un conjunt de generadors X és positiu si i només si el grup és virtualment abelià.

Aleshores si G no és virtualment abelià, el seu grau de commutativitat serà zero i tindrem que

$$0 \leq \lim_{n\to\infty} \frac{\#\{(u,v) \in \mathbb{B}_X(n) \times \mathbb{B}_X(n) \mid uv = vu\}}{\#\mathbb{B}_X(n)^2} \leq \limsup_{n\to\infty} \frac{\#\{(u,v) \in \mathbb{B}_X(n) \times \mathbb{B}_X(n) \mid uv = vu\}}{\#\mathbb{B}_X(n)^2} = 0,$$

i per tant el límit existirà, i a més serà 0, per a qualsevol conjunt de generadors. En el cas que G sigui virtualment abelià, aleshores existeix un $H \leq_{f.i.} G$ abelià tal que $G = H \sqcup Hg_1 \sqcup \cdots \sqcup Hg_r$. Aleshores fent servir tècniques de grups virtualment abelians que no detallarem, es pot trobar explícitament el límit, i llavors es veu que no depèn del sistema de generadors. □

Corol·lari 3.22. *Sigui $G = \langle X \rangle = \langle Y \rangle$ un grup finitament generat de creixement subexponencial i residualment finit. Aleshores,*

$$dc_X(G) = 0 \iff dc_Y(G) = 0.$$

Prova. Donades les hipòtesis de l'enunciat, se satisfà el teorema anterior. Aleshores en particular, tenim que

$$dc_X(G) > 0 \iff G \text{ és virtualment abelià} \iff dc_Y(G) > 0.$$

I per tant concloem $dc_X(G) = 0 \iff dc_Y(G) = 0$. Fixem-nos que podem fer aquest raonament perquè ser virtualment abelià és una propietat intrínseca del grup que no depèn del sistema de generadors triat. $\square$

Conclusions

En aquest treball hem vist el teorema d'Antolín-Martino-Ventura, una versió més general del teorema de Gustafson per a grups finitament generats, fent la pertinent generalització de la definició del grau de commutativitat. A més, també s'ha demostrat en el mateix teorema que si un grup té una part considerable que commuta, aleshores estarà organitzada en forma de subgrup abelià d'índex finit.

Per tal de provar aquest resultat però, hem hagut d'afegir certes hipòtesis, el creixement subexponencial i la residualitat finita, però fins on conec, tampoc no hi ha contraexemples de grups més generals que no satisfacin el resultat del teorema. Així doncs, és raonable conjecturar que el teorema podria ser cert en casos més generals. En aquest sentit, per a la futura recerca seria interessant provar de demostrar aquest resultat podent renunciar a alguna d'aquestes hipòtesis.

Per altra banda, hem vist que, efectivament, la fita per al grau de commutativitat de grups no abelians finitament generats és la mateixa que per als grups finits: $5/8$. La recerca d'aquest treball també es podria seguir en un altre sentit, i és estudiar aquestes fites superiors per a certs tipus de grups més concrets o bé per altres tipus d'estructures algebraiques. En aquest sentit, es pot seguir la línia d'articles com [5], en què es generalitza el concepte de grau de commutativitat a un anell de grup $F[G]$, on G és un grup finit i F un cos finit, i es dona una fita superior per al grau de commutativitat en aquesta estructura. Seguint la línia d'aquest treball de fi de grau es podria intentar fer la generalització per $F[G]$ en el cas que G no sigui finit.

Finalment, fixem-nos que en estudiar el grau de commutativitat, hem mirat en quin grau un grup satisfà una certa equació concreta, que és que donats dos elements del grup u, v commutin, és a dir, l'equació $uvu^{-1}v^{-1} = 1$. Aquesta equació és particularment interessant per tractar-se de la commutativitat, però també es podria seguir la recerca d'aquest treball intentant obtenir resultats anàlegs però per a altres equacions, és a dir, per a alguna equació del tipus $f(u_1, \dots, u_k) = 1$, on $u_1, \dots, u_k$ són elements d'un grup.

Així doncs, tot i que en aquest treball no haguem pogut tractar alguna d'aquestes qüestions, el camp estudiat té potencial d'estudi en moltes línies diferents.

Referències

[1] Yago Antolín, Armando Martino i Enric Ventura. "Degree of Commutativity of infinite groups". A: *Proceedings of the American Mathematical Society* 145.2 (2017), pp. 479-485. ISSN: 00029939, 10886826. URL: https://www.jstor.org/stable/procamermathsoci.145.2.479 (cons. 10-06-2023).

[2] J. Burillo i E. Ventura. "Counting Primitive Elements in Free Groups". A: *Electronic Notes in Discrete Mathematics* 10 (2001). Comb01, Euroconference on Combinatorics, Graph Theory and Applications, pàg. 50-53. ISSN: 1571-0653. DOI: https://doi.org/10.1016/S1571-0653(04)00357-9. URL: https://www.sciencedirect.com/science/article/pii/S1571065304003579.

[3] Pep Burillo. *Estructures algebraiques*. Apunts del curs 2012-2013.

[4] Timothy Burness et al. "On the commuting probability of p-elements in a finite group". A: *Algebra Number Theory* 17 (maig de 2023), pàg. 1209-1229. DOI: 10.2140/ant.2023.17.1209.

[5] Abdollah Chashiani i Rashid Rezaei. "On the commutativity degree of a group algebra". A: *Afrika Matematika* 32 (febr. de 2021). DOI: 10.1007/s13370-021-00887-5.

[6] Jordi Delgado i Enric Ventura i Gatell. "Autòmats de Stallings, un camí d'anada i tornada". A: *Butlletí de la Societat Catalana de Matemàtiques* 37.1 (gen. de 2023), pàg. 5-59. URL: https://revistes.iec.cat/index.php/BSCM/article/view/115308.003.

[7] Patrick X. Gallagher. "The Number of Conjugacy Classes in a Finite Group." A: *Mathematische Zeitschrift* 118 (1970), pàg. 175-179. URL: http://eudml.org/doc/171450.

[8] W. H. Gustafson. "What is the Probability that Two Group Elements Commute?" A: *The American Mathematical Monthly* 80.9 (1973), pàg. 1031-1034. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2318778 (cons. 08-06-2023).

[9] Desmond MacHale. "How Commutative Can a Non-Commutative Group Be?" A: *The Mathematical Gazette* 58.405 (1974), pàg. 199-202. ISSN: 00255572. URL: http://www.jstor.org/stable/3615961 (cons. 15-05-2023).

[10] D. Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 1996. ISBN: 9780387944616. URL: https://books.google.es/books?id=lqyCjUFY6WAC.