Màster Interuniversitari en Investigació Matemàtica

Extensions de grups tipus Gaschütz i el graf de Cayley

(Treball fi de màster)

Estudiant: Neus Fuster i Corral

Tutors: Ramon Esteban i Romero

Enric Cosme i Llópez

Índex

Introducció

En l'article [3], Gaschütz va provar que donat un grup finit A-generat G i un nombre primer p, existeixen una extensió $G^\sharp$ i un epimorfisme de grups $\varphi\colon G^\sharp \longrightarrow G$ de manera que el seu nucli és un grup p-elemental abelià. A més, aquesta extensió és universal sobre tots els grups amb aquestes mateixes característiques. En aquest treball, tractarem de generalitzar aquest resultat de dues formes.

En primer lloc, veurem que per a quasevol grup finit A-generat G i qualsevol nombre natural m, podem trobar una extensió $G^\sharp_m$ i un epimorfisme d'aquesta extensió en G que tinga com a nucli un grup abelià d'exponent m. A més, aquesta extensió també serà universal respecte als grups que tinguen un epimorfisme en G amb nucli abelià d'exponent m.

En segon lloc, com en els casos anteriors haurem vist que l'extensió universal $G^\sharp_m$ es pot construir com el quocient $F/R^\sharp$ on $R^\sharp = R'R^m$, F és el grup lliure sobre A i R és un subgrup de F tal que $F/R \cong G$, veurem que l'extensió natural $G^* = F/R'$, que a diferència de les anteriors, és infinita (excepte si G és trivial), també és universal sobre la resta d'extensions H de G de forma que s'hi pot trobar un epimorfisme $\psi\colon H \longrightarrow G$ amb nucli abelià.

D'altra banda, Ballester-Bolinches, Cosme-Llópez i Esteban-Romero, presenten en [1] la construcció d'un grup G^{Ab_p} basat en el graf de Cayley d'un grup finit A-generat G i demostren que és isomorf a l'extensió universal de Gaschütz $G^\sharp$. En aquesta memòria, exposarem aquestes dues coses amb una mica més de detall. Tot seguit, donat un nombre natural m, construirem de manera similar (també basant-nos en el graf de Cayley) un grup G^{Ab_m} i veurem que és isomorf a l'extensió universal tipus Gaschütz $G^\sharp_m$ de què parlàvem prèviament. Per últim, tractarem de fer una construcció semblant però infinita que siga isomorfa a l'extensió G^*.

Ara bé, abans d'entrar en matèria, parlarem de determinats conceptes que necessitarem més endavant. Per començar, definirem dues extensions del producte directe: els productes semidirecte i el subdirecte, en ambdos casos, seguint el llibre [2]. El producte semidirecte ens serà útil a l'hora de construir grups basant-nos en el graf de Cayley, mentre que el producte subdirecte servirà per veure la relació entre l'extensió tipus Gaschütz per a un natural m i les extensions per a les potències de nombres primers de la descomposició de m.

A continuació, dedicarem una secció a l'estudi dels grups abelians. Concretament, definirem el concepte de grup abelià lliure i utilitzarem les seues propietats per provar el Teorema fonamental dels grups abelians finitament generats, que necessitarem per demostrar que l'extensió G^* és isomorfa al grup que construirem amb el graf de Cayley. Tots els resultats d'aquesta secció es poden trobar en [6] i [4]. El darrer apartat del primer capítol el dedicarem a estudiar grups lliures, que emprarem per provar l'existència de les extensions tipus Gaschütz, i presentacions de grups. En aquest cas, hem extret la informació de nou de [6] i de [5].

Tot seguit, emprarem el següent capítol per estudiar alguns conceptes de teoria de grafs seguint [8] i [7], definir el graf de Cayley d'un grup A-generat G i veure'n alguns exemples.

Finalment, al tercer i últim capítol ens centrarem en provar el que hem exposat inicialment: les diferents generalitzacions del teorema de l'extensió universal de Gaschütz i l'existència d'un isomorfisme entre cadascuna d'aquestes i els diferents grups construïts amb l'ajuda del graf de Cayley.

Capítol 1

Resultats previs

Abans de començar, cal fer un apunt sobre la notació: durant tota la memòria, les aplicacions i la composició l'escriurem per la dreta. Per exemple, $(\psi \circ \varphi)(g)$ es denotarà com $g\varphi\psi$.

1.1 Producte semidirecte

En aquesta secció estudiarem el producte semidirecte, que com veurem, és una generalització del producte directe. Començarem introduïnt el concepte de grup d'operadors per seguidament definir el que s'anomenen productes semidirectes intern i extern. Finalment, veurem la relació entre ells i justificarem perquè podem dir que aquest concepte generalitza el de producte directe.

Definició 1.1. Donats dos grups G i H, suposem que per a cada $g \in G$ i $h \in H$ existeix un element $g^h \in G$ definit de manera que

1. l'aplicació $g \mapsto g^h$ és un automorfisme de G,
2. $g^{hk} = (g^h)^k$, per a tots $g \in G$ i $h, k \in H$.

Aleshores, direm que H és un *grup d'operadors* per a G o simplement que G és un *H-grup*.

Si tenim un homomorfisme $\sigma\colon H \longrightarrow \mathrm{Aut}(G)$ de manera que l'element g^h estiga definit com $g^h := g\sigma_h$,[1] llavors direm que H és un grup d'operadors per a G *via* σ.

Definició 1.2. Siga X un grup amb subgrups G i H de manera que $X = GH$, $G \trianglelefteq X$ i $G \cap H = 1$. Aleshores, es diu que X és el *producte semidirecte (intern)* de

[1] Notem que en aquest context, la notació g^h no representa necessàriament la conjugació. No osbtant això, veurem que la notació es correspon amb la conjugació en el producte semidirecte extern que definirem més endavant.

G amb H. A més, amb l'acció de H sobre G per conjugació, $g^h = h^{-1}gh$, és clar que H és un grup d'operadors per a G.

Definició 1.3. Siga H un grup d'operadors per a G. Si definim una operació binària sobre el producte cartesià $X = G \times H$ com

$$(g, h)(g', h') = (g(g')^{h^{-1}}, hh'),$$

és fàcil comprovar que el conjunt X amb aquesta operació forma un grup amb element identitat $(1_G, 1_H)$ i de manera que l'invers de (g, h) és $((g^{-1})^h, h^{-1})$. A X se l'anomena *producte semidirecte (extern)* de G amb H via σ (on $\sigma\colon H \longrightarrow \mathrm{Aut}(G)$ determina l'acció de H sobre G) i ho denotarem com

$$X = [G]H \quad (\text{via } \sigma).$$

Quan l'acció de H estiga clara pel context, escriurem simplement $X = [G]H$.

Observant les definicions, veiem que el producte semidirecte intern és una manera particular de construir un grup partint de dos subgrups, sent un d'ells normal, mentre que el producte semidirecte extern és un producte cartesià juntament amb una operació concreta que depén de l'homomorfisme σ. Malgrat tot, ambdues definicions estan molt relacionades, com mostra la nota següent.

Nota 1.4. De la definició es dedueix clarament que $X = [G]H$ és el producte semidirecte intern del subgrup $G \times 1 \cong G$ amb $1 \times H \cong H$. A més, el càlcul següent mostra que l'acció de H sobre G es correspon amb la conjugació en X per l'element $(1, h)$:

$$\begin{aligned}(g, 1)^{(1,h)} &= (1, h^{-1})(g, 1)(1, h) \\ &= (1, h^{-1})(g, h) = (g^h, 1).\end{aligned}$$

Per tant, no farem distincions formals entre els productes semidirectes intern i extern: identificarem $G \times 1$ amb G i $1 \times H$ amb H i veurem la versió externa $[G]H$ com el producte semidirecte intern de G amb H.

Nota 1.5. Si l'acció de H sobre G és trivial, és a dir, $H\sigma = 1$, aleshores $[G]H = G \times H$. Així, el producte directe és un cas especial del producte semidirecte.

Exemple: Donats dos grups G i H, el seu producte directe és únic. En canvi, amb el producte semidirecte no ocorre el mateix ja que aquest depén de l'homomorfisme $\sigma\colon H \longrightarrow \mathrm{Aut}(G)$ escollit. Per exemple, si considerem $G = \mathbb{Z}/3\mathbb{Z} = \{1, a, a^2\}$ i $H = \mathbb{Z}/2\mathbb{Z} = \{1, b\}$, tenim dues possibilitats:

(a) Prendre σ_1 l'homomorfisme trivial. En aquest cas, tenim que $[G]H$ (via σ_1) $= G \times H \cong \mathbb{Z}/6\mathbb{Z}$.

(b) Prendre σ_2 de manera que $b\sigma_2$ és l'automorfisme que intercanvia els elements a i a^2. Aleshores, $[G]H$ (via σ_2) $\cong S_3$, on S_3 és el grup simètric d'ordre 3.

1.2 Producte subdirecte

Aquest apartat el dedicarem a definir el producte subdirecte de dos grups. Per fer-ho, començarem veient quan es diu que un subgrup és subdirecte per poder definir tot seguit el producte subdirecte de manera constructiva. Finalment, observarem que el producte directe es pot veure com un cas particular de producte subdirecte.

Definició 1.6. Donat $D = G_1 \times \cdots \times G_r$, es diu que un subgrup U de D és *subdirecte* si $U\pi_i = G_i$ per a cada $i = 1, \ldots, r$, on π_i és la i-èssima projecció.

Lema 1.7. *Donats $N_1, \ldots, N_r$ subgrups normals d'un grup G, l'aplicació*

$$\begin{array}{rccc} \mu\colon & G & \longrightarrow & G/N_1 \times \cdots \times G/N_r \\ & g & \mapsto & (gN_1, \ldots, gN_r) \end{array}$$

és un homomorfisme de grups amb nucli $\bigcap_{i=1}^r N_i$ i a més, $G\mu$ és subdirecte. En particular, $G/(\bigcap_{i=1}^r N_i)$ és isomorf a un subgrup subdirecte de $G/N_1 \times \cdots \times G/N_r$.

Demostració. Clarament, μ és un homomorfisme:

$$(gg')\mu = (gg'N_1, \ldots, gg'N_r) = (gN_1, \ldots, gN_r)(g'N_1, \ldots, g'N_r) = (g\mu)(g'\mu).$$

A més, $g\mu = (N_1, \ldots, N_r)$ si, i només si, $g \in N_i$ per a tot $i = 1, \ldots, r$, amb la qual cosa, $\ker(\mu) = \bigcap_{i=1}^r N_i$. D'altra banda, la projecció π_i de $G\mu$ és $\{gN_i \mid g \in G\} = G/N_i$, amb la qual cosa, $G\mu$ és subdirecte, i pel teorema d'isomorfia, tenim l'última afirmació de l'enunciat. □

Teorema 1.8. *Siguen G_1, G_2 i H grups i siguen $\varepsilon_i\colon G_i \longrightarrow H$ epimorfismes amb $K_i = \ker(\varepsilon_i)$ per a $i = 1, 2$. Anomenem $D = G_1 \times G_2$, $\overline{G_1} = G_1 \times 1$ i $\overline{G_2} = 1 \times G_2$ i considerem*

$$G = \{(g_1, g_2) \mid g_i \in G_i,\ g_1\varepsilon_1 = g_2\varepsilon_2\}.$$

Aleshores G és subgrup de D i existeixen $\delta_i\colon G \longrightarrow G_i$ epimorfismes tals que

i) $\ker(\delta_1) = G \cap G_2 \cong K_2, \quad \ker(\delta_2) = G \cap G_1 \cong K_1.$

ii) $\ker(\delta_1)\ker(\delta_2) = K_1 \times K_2.$

iii) $G/(K_1 \times K_2) \cong H.$

Demostració. Comencem veient que G és subgrup subdirecte de D, és a dir, donades les projeccions $\pi_i : D \longrightarrow G_i$ per a $i = 1, 2$, vegem que $G\pi_i = G_i$.

Donat $g_1 \in G_1$, $g_1\varepsilon_1 = h \in H$. Ara, com ε_2 és un epimorfisme, existeix $g_2 \in G_2$ de forma que $g_2\varepsilon_2 = h$. Així, $(g_1, g_2) \in G$ i $(g_1, g_2)\pi_1 = g_1$, amb la qual cosa, $G\pi_1 = G_1$ i raonant de manera anàloga, $G\pi_2 = G_2$.

Llavors, si considerem δ_i com la restricció de π_i a G per a $i = 1, 2$, obtenim dos epimorfismes que satisfan:

$$\begin{aligned}\ker(\delta_1) &= G \cap \ker(\pi_1) = G \cap \overline{G_2} = \{(1, g_2) \mid g_2\varepsilon_2 = 1\} \\ &= \{(1, g_2) \mid g_2 \in K_2\} = 1 \times K_2 \cong K_2, \\ \ker(\delta_2) &= G \cap \ker(\pi_2) = G \cap \overline{G_1} = \{(g_1, 1) \mid g_1\varepsilon_1 = 1\} \\ &= \{(g_1, 1) \mid g_1 \in K_1\} = K_1 \times 1 \cong K_1.\end{aligned}$$

A més, com $(K_1 \times 1) \cap (1 \times K_2) = 1$, tenim que $\ker(\delta_1)\ker(\delta_2) = K_1 \times K_2$, amb la qual cosa hem provat *i*) i *ii*).

Per últim, per provar *iii*), considerem l'homomorfisme $\varepsilon\colon G \longrightarrow H \times H$ donat per $g\varepsilon = (g\delta_1\varepsilon_1, g\delta_2\varepsilon_2)$ per a cada $g \in G$. Notem que si $g = (g_1, g_2) \in G$, aleshores $g\delta_1\varepsilon_1 = g_1\varepsilon_1 = g_2\varepsilon_2 = g\delta_2\varepsilon_2$. Per tant, la imatge de ε és $\{(h, h) \mid h \in H\} \cong H$. D'altra banda, el nucli de ε és $K_1 \times K_2$ ja que, si $g = (g_1, g_2) \in \ker(\varepsilon)$, llavors $1 = g\delta_i\varepsilon_i = g_i\varepsilon_i$, amb la qual cosa, $g_i \in K_i$ per a cada $i = 1, 2$. Així, pel teorema d'isomorfia, $G/(K_1 \times K_2) \cong H$. □

Definició 1.9. El subgrup G de $G_1 \times G_2$ del teorema anterior s'anomena *producte subdirecte* de G_1 i G_2 amb grup factor amalgamat H.

Nota 1.10. El producte subdirecte de dos grups G_1 i G_2 amb grup factor amalgamat 1, és el producte directe dels dos grups.

1.3 Estudi dels grups abelians

1.3.1 Grup abelià lliure

Abans de començar, hem de tindre en compte que, com a norma general, quan treballem amb grups abelians emprarem notació additiva.

Definició 1.11. Un grup abelià F es diu *abelià lliure* si és isomorf a una suma directa de grups cíclics infinits. Més concretament, existeix un subconjunt $A \subset F$ format per elements d'ordre infinit, anomenat *base* de F, de manera que $F = \bigoplus_{a\in A}\langle a\rangle$, és a dir, $F \cong \bigoplus_{a\in A}\mathbb{Z}$.

Teorema 1.12. *Siguen F un grup abelià lliure amb base A, G un grup abelià qualsevol i $f\colon A \longrightarrow G$ una funció qualsevol. Aleshores, existeix un únic homomorfisme $\varphi\colon F \longrightarrow G$ que extén f, és a dir, que fa commutatiu el diagrama*

$$\begin{array}{ccc} A & \xrightarrow{\iota} & F \\ & \searrow^{f} & \downarrow{\scriptstyle\varphi} \\ & & G \end{array}$$

on ι és la inclusió. De fet, si $u = \sum m_a a \in F$, aleshores $u\varphi = \sum m_a af$.

Demostració. Si $u \in F$, per la unicitat de l'expressió $u = \sum m_a a$ tenim que la funció $\varphi\colon F \longrightarrow G$ definida com $u \mapsto \sum m_a a f$ està ben definida. A més, φ és clarament un homomorfisme i extén f. Per últim, també tenim la unicitat perquè si ψ fora un altre homomorfisme que extenguera f, $a\psi = a\varphi$ per a tot $a \in A$ i dos homomorfismes que coincideixen en un conjunt de generadors són iguals. □

Teorema 1.13. *Siguen F_1 i F_2 grups abelians lliures amb bases A_1 i A_2, respectivament. Aleshores, $F_1 \cong F_2$ si, i només si, $|A_1| = |A_2|$.*

Demostració. Suposem primer que $|A_1| = |A_2|$. Aleshores, hi ha una bijecció $f\colon A_1 \longrightarrow A_2 \subset F_2$ i pel teorema anterior, existeix $\varphi\colon F_1 \longrightarrow F_2$ amb $a\varphi = af$ per a tot $a \in A_1$. De la mateixa manera, existeix $\psi\colon F_2 \longrightarrow F_1$ amb $b\psi = bf^{-1}$ per a cada $b \in A_2$. Ara bé, $\varphi\psi$ i $\psi\varphi$ són identitats perquè ambdos fixen els elements de la base corresponent. Així, φ és un isomorfisme i $F_1 \cong F_2$.

Suposem ara que $F_1 \cong F_2$. Si p és un nombre primer, aleshores $V = F_1/pF_1$ és un espai vectorial sobre $\mathbb{Z}/p\mathbb{Z}$. Comprovem que $\overline{A_1} = \{a + pF_1 \mid a \in A_1\}$ és una base de V: és clar que $\overline{A_1}$ genera V així que només hem de veure si és linealment independent. Suposem que $\sum \overline{m_a}(a + pF_1) = 0$ per a $\overline{m_a} \in \mathbb{Z}/p\mathbb{Z}$. Si m_a és un representant de $\overline{m_a}$, aleshores $\sum m_a(a + pF_1) = 0$. En F_1, aquesta equació vol dir que $\sum m_a a \in pF_1$, és a dir, que existeixen enters n_a amb $\sum m_a a = \sum p n_a a$. Per la independència de la base, $m_a = pn_a$ i llavors $\overline{m_a} = \overline{0}$ per a tot $a \in A_1$, amb la qual cosa, $\overline{A_1}$ és base de V. Així, tenim que $\dim F_1/pF_1 = |\overline{A_1}| = |A_1|$. De manera anàloga, $\dim F_2/pF_2 = |A_2|$, i com $F_1 \cong F_2$ implica $F_1/pF_1 \cong F_2/pF_2$, obtenim el que volíem: $|A_1| = |A_2|$. □

Definició 1.14. S'anomena *rang* del grup abelià lliure F al cardinal de la seua base.

Teorema 1.15. *Qualsevol grup abelià G és imatge homomorfa d'un grup abelià lliure de rang $|A|$, on A és un conjunt de generadors de G.*

Demostració. Siga $F = \bigoplus_{a\in A}\langle a\rangle$ grup abelià lliure de rang $|A|$. Pel teorema 1.12, donada l'aplicació inclusió $\iota\colon A \longrightarrow G$, existeix un únic homomorfisme $\varphi\colon F \longrightarrow G$ que l'extén a F. Aleshores, $a\varphi = a \in G$ i així $A \subseteq F\varphi$. Llavors, com A genera G, tenim que $F\varphi = G$, com volíem. En particular, $F/\ker\varphi \cong G$. □

Lema 1.16. *Si $\{a_1, \ldots, a_n\}$ és una base d'un grup abelià lliure F i $m \in \mathbb{Z}$, aleshores per a cada $j \neq i$ el conjunt $\{a_1, \ldots, a_{j-1}, a_j + ma_i, a_{j+1}, \ldots, a_n\}$ és també una base de F.*

Demostració. És clar que $F = \langle a_1, \ldots, a_{j-1}, a_j + ma_i, a_{j+1}, \ldots, a_n\rangle$ ja que $a_j = -ma_i + (a_j + ma_i)$. D'altra banda, si $k_1a_1 + \cdots + k_j(a_j + ma_i) + \cdots + k_n a_n = 0$ amb $k_t \in \mathbb{Z}$, aleshores $k_1a_1 + \cdots + (k_i + k_j m)a_i + \cdots + k_j a_j + \cdots + k_n a_n = 0$, amb la qual cosa, cada $k_t = 0$. □

Teorema 1.17. *Si F és un grup abelià lliure de rang finit n i G és un subgrup de F no trivial, aleshores existeixen una base $\{a_1, \ldots, a_n\}$ de F, un enter r amb $1 \leq r \leq n$ i enters positius $d_1, \ldots, d_r$ amb $d_1 \mid d_2 \mid \cdots \mid d_r$ tals que G és abelià lliure amb base $\{d_1a_1, \ldots, d_ra_r\}$.*

Demostració. Ho provarem per inducció sobre n. Si $n = 1$, aleshores $F = \langle a_1 \rangle \cong \mathbb{Z}$ i $G = \langle d_1a_1 \rangle \cong \mathbb{Z}$ per a algun $d_1 \in \mathbb{N}$ i ja ho tenim. Suposem per inducció que el teorema és cert per a tots els grups abelians lliures de rang menor que n.

Definim S com el conjunt dels enters s tals que existeix una base $\{b_1, \ldots, b_n\}$ de F i un element de G de la forma $sb_1 + k_2b_2 + \cdots + k_nb_n$ amb $k_i \in \mathbb{Z}$ per a $i = 2, \ldots, n$. Notem que, en aquest cas, $\{b_2, b_1, b_3, \ldots, b_n\}$ també és una base de F i, per tant, $k_2 \in S$ (i de manera similar, la resta dels k_i).

Com $G \neq 0$, tenim que $S \neq \varnothing$ i podem prendre d_1 com el mínim enter positiu de S. A més, per a alguna base $\{b_1, \ldots, b_n\}$ de F existeix $v \in G$ amb $v = d_1b_1 + k_2b_2 + \cdots + k_nb_n$ $(k_2, \ldots, k_n \in \mathbb{Z})$. Per l'algorisme de la divisió, per a cada $i = 2, \ldots, n$, $k_i = d_1q_i + r_i$ amb $0 \leq r_i < d_1$ i llavors $v = d_1(b_1 + q_2b_2 + \cdots + q_nb_n) + r_2b_2 + \cdots + r_nb_n$. Si anomenem $a_1 = b_1 + q_2b_2 + \cdots + q_nb_n$, pel lema 1.16, $W = \{a_1, b_2, \ldots, b_n\}$ és una base de F. Com $v \in G$, $r_i < d_1$ i qualsevol reordenació de W és una base de F, cada $r_i \in S$ i aleshores la minimalitat de d_1 implica que $r_2 = \cdots = r_n = 0$. Així, $v = d_1a_1 \in G$.

Siga $H = \langle b_2, b_3, \ldots, b_n \rangle$. Aleshores H és un grup abelià lliure de rang $n - 1$ tal que $F = \langle a_1 \rangle \oplus H$. Vegem que $G = \langle v \rangle \oplus (G \cap H) = \langle d_1a_1 \rangle \oplus (G \cap H)$. Si $u = t_1a_1 + t_2b_2 + \cdots + t_nb_n \in G$ $(t_i \in \mathbb{Z})$, per l'algorisme de la divisió $t_1 = d_1q_1 + r_1$ amb $0 \leq r_1 < d_1$. Llavors, G conté l'element $u - q_1v = r_1a_1 + t_2b_2 + \cdots + t_nb_n$ i per la minimalitat de d_1 en S, $r_1 = 0$ i així $u = q_1v + (t_2b_2 + \cdots + t_nb_n) \in \langle v \rangle + (G \cap H)$. D'altra banda, com $\{a_1, b_2, \ldots, b_n\}$ és una base de F, $\langle v \rangle \cap (G \cap H) = 0$, amb la qual cosa, $G = \langle v \rangle \oplus (G \cap H)$.

Si $G \cap H = 0$, aleshores $G = \langle d_1a_1 \rangle$ i el teorema és cert; suposem que $G \cap H \neq 0$. Per la hipòtesi d'inducció, existeixen una base $\{a_2, \ldots, a_n\}$ de H i enters positius $r, d_2, \ldots, d_r$ amb $d_2 \mid d_3 \mid \cdots \mid d_r$ tals que $G \cap H$ és abelià lliure amb base $\{d_2a_2, \ldots, d_ra_r\}$.

Com $F = \langle a_1 \rangle \oplus H$ i $G = \langle d_1x_1 \rangle \oplus (G \cap H)$, tenim que $\{a_1, \ldots, a_n\}$ és una base de F i $\{d_1a_1, \ldots, d_ra_r\}$ ho és de G. Per tant, només falta comprovar que d_1 divideix a d_2. Per l'algorisme de la divisió, $d_2 = qd_1 + r_0$ amb $0 \leq r_0 < d_1$. Pel lema 1.16, $\{a_2, a_1 + qa_2, a_3, \ldots, a_n\}$ és una base de F i com $r_0a_2 + d_1(a_1 + qa_2) = d_1a_1 + d_2a_2 \in G$, la minimalitat de d_1 en S implica que $r_0 = 0$, amb la qual cosa, $d_1 \mid d_2$. □

1.3.2 Grups abelians finitament generats

Definició 1.18. Un grup G és *finitament generat* si existeix un subconjunt finit A de G tal que $\langle A\rangle = G$.

Corol·lari 1.19. *Si G és un grup abelià finitament generat per n elements, aleshores qualsevol subgrup H de G és generat per m elements amb $m \leq n$.*

Demostració. Pel teorema 1.15, existeixen un grup abelià lliure F de rang n i un epimorfisme $\pi\colon F \longrightarrow G$. $H\pi^{-1}$ és un subgrup de F i per tant és abelià lliure de rang $m \leq n$ pel teorema 1.17. Aleshores, la imatge mitjançant π d'una base de $H\pi^{-1}$ és un conjunt de m elements com a màxim que genera $H\pi^{-1}\pi = H$. □

Nota 1.20. El corol·lari és fals si ometem la paraula abelià.

Teorema 1.21 (Teorema fonamental dels grups abelians finitament generats)**.** *Tot grup G abelià finitament generat és isomorf a una suma directa finita de grups cíclics en la qual els sumands cíclis finits (si hi ha algun) són d'ordre $m_1, \ldots, m_t$ amb $m_1 > 1$ i $m_1 \mid m_2 \mid \cdots \mid m_t$.*

Demostració. Si $G \neq 0$ i G és generat per n elements, aleshores pel teorema 1.15, existeixen un grup abelià lliure F de rang n i un epimorfisme $\pi\colon F \longrightarrow G$. Si π és un isomorfisme, aleshores $G \cong F \cong \mathbb{Z} \oplus \overset{(n)}{\cdots} \oplus \mathbb{Z}$ i ja ho tenim. Si no, pel teorema 1.17, existeixen una base $\{a_1, \ldots, a_n\}$ de F i enters positius $r, d_1, \ldots, d_r$ amb $1 \leq r \leq n$ i $d_1 \mid \cdots \mid d_r$ tals que $\{d_1a_1, \ldots, d_ra_r\}$ és base de $K = \ker\pi$.

Ara, $F = \sum_{i=1}^{n}\langle a_i\rangle$ i $K = \sum_{i=1}^{r}\langle d_ia_i\rangle$, on $\langle a_i\rangle \cong \mathbb{Z}$ i $\langle d_ia_i\rangle \cong d_i\mathbb{Z}$ sota el mateix isomorfisme. Anomenant $d_i = 0$ per a $i = r+1, \ldots, n$, podem reescriure K com $K = \sum_{i=1}^{n}\langle d_ia_i\rangle$. Aleshores tenim que

$$G \cong \frac{F}{K} = \frac{\sum_{i=1}^{n}\langle a_i\rangle}{\sum_{i=1}^{n}\langle d_ia_i\rangle} \cong \sum_{i=1}^{n}\frac{\langle a_i\rangle}{\langle d_ia_i\rangle} \cong \sum_{i=1}^{n}\frac{\mathbb{Z}}{d_i\mathbb{Z}}.$$

Notem que si $d_i = 1$, aleshores $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0$ i si $d_i = 0$, aleshores $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/0 = \mathbb{Z}$.

Siguen $m_1, \ldots, m_t$ els d_i (en ordre) tals que $d_i > 1$ i siga s el nombre de d_i tals que $d_i = 0$. Aleshores,

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus (\mathbb{Z} \oplus \overset{(s)}{\cdots} \oplus \mathbb{Z}),$$

amb $m_1 > 1$ i $m_1 \mid m_2 \mid \cdots \mid m_t$. □

Teorema 1.22. *Tot grup G abelià finitament generat és isomorf a una suma directa finita de grups cíclics on cada sumand és infinit o d'ordre potència d'un primer.*

Demostració. És suficient aplicar el teorema anterior i tindre en compte que si m és un enter positiu de manera que la seua descomposició en nombres primers és $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, aleshores $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$. □

Definició 1.23. Donats un grup abelià G, un enter m i un primer p, definim els següents subgrups de G:

$$\begin{aligned} mG &= \{mg \mid g \in G\}; \\ G[m] &= \{g \in G \mid mg = 0\}; \\ G(p) &= \{g \in G \mid o(g) = p^n \text{ per a algun } n \geq 0\}; \\ G\tau &= \{g \in G \mid o(g) \text{ és finit}\}. \end{aligned}$$

El subgrup $G\tau$ s'anomena *subgrup de torsió* de G. A més, si $G = G\tau$ es diu que G és un grup *de torsió* i si $G\tau = 0$, es diu que G és *lliure de torsió.*

Lema 1.24. *Per a qualssevol enters $n > 1$ i $m < n$ es compleix que:*

(i) $(\mathbb{Z}/p^n\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z}$.

(ii) $p^m(\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^{n-m}\mathbb{Z}$.

Demostració. Com l'element $p^{n-1} \in \mathbb{Z}/p^n\mathbb{Z}$ té ordre p, tenim que $\langle p^{n-1} \rangle \cong \mathbb{Z}/p\mathbb{Z}$ i $\langle p^{n-1} \rangle \leq (\mathbb{Z}/p^n\mathbb{Z})[p]$. D'altra banda, si $u \in (\mathbb{Z}/p^n\mathbb{Z})[p]$, aleshores $pu = 0$ en $\mathbb{Z}/p^n\mathbb{Z}$, amb la qual cosa, $pu \equiv 0 \mod p^n$ en $\mathbb{Z}$. Però que p^n dividisca a pu, implica que $p^{n-1} \mid u$. Per tant, en $\mathbb{Z}/p^n\mathbb{Z}$, $u \in \langle p^{n-1} \rangle$ i llavors $(\mathbb{Z}/p^n\mathbb{Z})[p] \leq \langle p^{n-1} \rangle$. Així, tenim (i).

Per veure (ii), notem que $p^m \in \mathbb{Z}/p^n\mathbb{Z}$ té ordre p^{n-m}. Per tant, $p^m(\mathbb{Z}/p^n\mathbb{Z}) = \langle p^m \rangle \cong \mathbb{Z}/p^{n-m}\mathbb{Z}$. □

Teorema 1.25. *Siga G un grup abelià finitament generat. Aleshores:*

(i) Existeix un únic enter no negatiu s de manera que el nombre de sumands cíclics infinits de qualsevol descomposició de G com a suma directa de grups cíclics és precisament s.

(ii) O bé G és abelià lliure o bé existeix una única llista d'enters positius (no necessàriament distints) $m_1, \ldots, m_t$ amb $m_1 > 1$ i $m_1 \mid \cdots \mid m_t$ tals que

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus F,$$

amb F abelià lliure.

(iii) O bé G és abelià lliure o bé existeix una llista d'enters positius $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ que és única excepte per l'ordre dels seus membres, de manera que $p_1, \ldots, p_k$ són primers (no necessàriament distints) i $\alpha_1, \ldots, \alpha_k$ són enters positius (no necessàriament distints) i es té que

$$G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z} \oplus F,$$

amb F abelià lliure.

Demostració. (i) Qualsevol descomposició de G com a suma directa de grups cíclics (almenys n'hi ha una pel teorema 1.21) es pot veure com $G \cong H \oplus F$, on H és suma directa de grups cíclics finits (potser 0) i F és abelià lliure amb rang s, el nombre de sumands cíclics infinits de la descomposició. Si $\iota\colon H \longrightarrow H \oplus F$ és la injecció canònica $h \mapsto (h, 0)$, aleshores $H\iota$ és el subgrup de torsió de $H \oplus F$, i així, $H\iota \cong G\tau$. Aleshores,

$$\frac{G}{G\tau} \cong \frac{H \oplus F}{H\iota} \cong F.$$

Per tant, qualsevol descomposició de G ens porta a la conclusió que $G/G\tau$ és un grup abelià lliure amb rang el nombre s de sumands cíclics infinits de la descomposició. Com que $G/G\tau$ no depén de la descomposició concreta, tenim que s està únicament determinat.

(iii) Suposem que G té dues descomposicions, diguem-ne

$$G \cong \sum_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \oplus F \quad \text{i} \quad G \cong \sum_{j=1}^{d} \mathbb{Z}/k_j\mathbb{Z} \oplus F,$$

amb cada n_i, k_j una potència de primer i F abelià lliure. Hem de veure que $r = d$ i que (després de reordenar-los) $n_i = k_i$ per a cada i. Notem que $\sum_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \cong G\tau \cong \sum_{j=1}^{d} \mathbb{Z}/k_j\mathbb{Z}$. Per a cada primer p, $\sum \mathbb{Z}/n_i\mathbb{Z}(p)$ és clarament isomorf a la suma directa dels $\mathbb{Z}/n_i\mathbb{Z}$ tals que n_i és potència de p. Llavors, com $\sum \mathbb{Z}/n_i\mathbb{Z}(p) \cong \sum \mathbb{Z}/k_j\mathbb{Z}(p)$ per a cada p, podem suposar sense perdre generalitat que cada n_i i k_j és potència d'un primer p fix. A més, per simplificar la notació, a partir d'ara anomenarem a $G\tau$ com G. Així, tenim

$$\sum_{i=1}^{r} \mathbb{Z}/p^{a_i}\mathbb{Z} \cong G \cong \sum_{i=1}^{d} \mathbb{Z}/p^{c_j}\mathbb{Z},$$

amb $1 \leq a_1 \leq \cdots \leq a_r$ i $1 \leq c_1 \leq \cdots \leq c_d$.

Vegem primer que qualssevol dos descomposicions d'aquest tipus han de tindre

el mateix nombre de sumands. Pel lema 1.24, tenim que

$$G[p] \cong \sum_{i=1}^{r} (\mathbb{Z}/p^{a_i}\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \overset{(r)}{\cdots} \oplus \mathbb{Z}/p\mathbb{Z}$$
$$G[p] \cong \sum_{j=1}^{d} (\mathbb{Z}/p^{c_j}\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \overset{(d)}{\cdots} \oplus \mathbb{Z}/p\mathbb{Z}$$

i per tant, $r = d$.

Siga υ el primer enter tal que $a_i = c_i$ per a tot $i < \upsilon$ però $a_\upsilon \neq c_\upsilon$. Podem suposar que $a_\upsilon < c_\upsilon$. Com $p^{a_\upsilon}(\mathbb{Z}/p^{a_i}\mathbb{Z}) = 0$ per a cada $a_i \leq a_\upsilon$, el lema 1.24 implica que

$$p^{a_\upsilon} G \cong \sum_{i=1}^{r} p^{a_\upsilon}(\mathbb{Z}/p^{a_i}\mathbb{Z}) \cong \sum_{i=\upsilon+1}^{r} \mathbb{Z}/p^{a_i - a_\upsilon}\mathbb{Z},$$

amb $a_{\upsilon+1} - a_\upsilon \leq \cdots \leq a_r - a_\upsilon$. És clar que hi ha com a molt $r - (\upsilon+1) + 1 = r - \upsilon$ sumands no nuls. De manera similar, com $a_i = c_i$ per a $i < \upsilon$ i $a_\upsilon < c_\upsilon$, de la segona descomposició obtenim que

$$p^{a_\upsilon} G \cong \sum_{i=\upsilon}^{r} \mathbb{Z}/p^{c_i - a_\upsilon}\mathbb{Z},$$

amb $1 \leq c_\upsilon - a_\upsilon \leq \cdots \leq c_r - a_\upsilon$. Òbviament, hi ha almenys $r - \upsilon + 1$ sumands no nuls. Però aleshores tenim dues descomposicions del grup $p^{a_\upsilon}G$ com a suma directa de grups cíclics d'ordre potència d'un primer amb un nombre de sumands diferent, el que contradiu el que hem provat al paràgraf anterior. Per tant, $a_i = c_i$ per a tot i, com volíem.

(*ii*) Suposem que G té dues descomposicions

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus F \quad \text{i} \quad G \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_d\mathbb{Z} \oplus F,$$

amb $1 < m_1 \mid \cdots \mid m_t$, $1 < k_1 \mid \cdots \mid k_d$ i F abelià lliure. Cada n_i i k_j té una factorització en nombres primers de manera que, afegint termes de la forma p^0 quan calga, totes tenen els mateixos nombres primers $p_1, \ldots, p_r$. Així,

$$\begin{aligned} m_1 &= p_1^{a_{1,1}} p_2^{a_{1,2}} \cdots p_r^{a_{1,r}} & k_1 &= p_1^{c_{1,1}} p_2^{c_{1,2}} \cdots p_r^{c_{1,r}} \\ m_2 &= p_1^{a_{2,1}} p_2^{a_{2,2}} \cdots p_r^{a_{2,r}} & k_2 &= p_1^{c_{2,1}} p_2^{c_{2,2}} \cdots p_r^{c_{2,r}} \\ &\vdots & &\vdots \\ m_t &= p_1^{a_{t,1}} p_2^{a_{t,2}} \cdots p_r^{a_{t,r}} & k_d &= p_1^{c_{d,1}} p_2^{c_{d,2}} \cdots p_r^{c_{d,r}} \end{aligned}$$

Com $m_1 \mid m_2 \mid \cdots \mid m_t$, per a cada j tenim que $0 \leq a_{1,j} \leq a_{2,j} \leq \cdots \leq a_{t,j}$. De la mateixa manera, $0 \leq c_{1,j} \leq c_{2,j} \leq \cdots \leq c_{d,j}$ per a cada j. A més,

$$\sum_{i,j} \mathbb{Z}/p_j^{a_{i,j}}\mathbb{Z} \cong \sum_{i=1}^{t} \mathbb{Z}/m_i\mathbb{Z} \cong G\tau \cong \sum_{i=1}^{d} \mathbb{Z}/k_i\mathbb{Z} \cong \sum_{i,j} \mathbb{Z}/p_j^{c_{i,j}}\mathbb{Z},$$

on alguns sumands poden ser 0. Llavors, per a cada $j = 1, \dots, r$

$$\sum_{i=1}^{t} \mathbb{Z}/p_j^{a_{i,j}}\mathbb{Z} \cong G(p_j) \cong \sum_{i=1}^{d} \mathbb{Z}/p_j^{c_{i,j}}\mathbb{Z}.$$

Donat que $m_1 > 1$, ha d'haver-hi algun primer p_j de forma que $1 \leq a_{1,j} \leq \cdots \leq a_{t,j}$, amb la qual cosa, $\sum_{i=1}^{t} \mathbb{Z}/p_j^{a_{i,j}}\mathbb{Z}$ té t sumands. Aleshores (iii) implica que $\sum_{i=1}^{d} \mathbb{Z}/p_j^{c_{i,j}}\mathbb{Z}$ ha de tindre t sumands no nuls, i així, $t \leq d$. De manera anàloga, $k_1 > 1$ implica que $d \leq t$ i per tant $t = d$. D'aquesta manera, per (iii), hem de tindre que $a_{i,j} = c_{i,j}$ per a tot i, j, i aleshores $m_i = k_i$ per a tot $i = 1, \dots, t$, com volíem. □

Definició 1.26. Si G és un grup abelià finitament generat, aleshores els enters $m_1, \dots, m_t$ únicament determinats de l'apartat (ii) del teorema anterior, s'anomenen *factors invariants* de G i les potències de nombres primers de l'apartat (iii) s'anomenen *divisors elementals* de G.

Corol·lari 1.27. *Dos grups abelians finitament generats G i H són isomorfs si, i només si, tenen els mateixos factors invariants (respectivament, divisors elementals) i les seues parts lliures $G/G\tau$ i $H/H\tau$ tenen el mateix rang.*

1.4 Grups lliures i presentacions

1.4.1 Grup lliure

Hem vist que, per a grups abelians, existeix la noció de grup abelià lliure. A continuació, veurem un concepte anàleg per a grups no abelians: el concepte de grup lliure. En aquest cas, prendrem com a definició una generalització de la propietat presentada al teorema 1.12.

Definició 1.28. Donats un grup F i un conjunt no buit A, es diu que F és un *grup lliure* sobre A quan existeix una funció $\iota\colon A \longrightarrow F$ tal que, donats un grup G i una aplicació $f\colon A \longrightarrow G$, existeix un únic homomorfisme de grups $\varphi\colon F \longrightarrow G$ tal que $\iota\varphi = f$.

$$\begin{array}{ccc} A & \xrightarrow{\iota} & F \\ & \searrow^{f} & \downarrow{\scriptstyle \varphi} \\ & & G \end{array}$$

Nota 1.29. De la definició de grup lliure podem extraure les següents conclusions.

(a) La funció $\iota\colon A \longrightarrow F$ és injectiva: suposem que $a_1\iota = a_2\iota$ però $a_1 \neq a_2$. Prenem un grup G que tinga almenys dos elements distints g_1 i g_2 i escollim una funció $f\colon A \longrightarrow G$ tal que $a_1 f = g_1$ i $a_2 f = g_2$. Però llavors tenim una contradicció perquè, si φ és l'únic homomorfisme tal que $\iota\varphi = f$, aleshores

$$g_1 = a_1 f = a_1\iota\varphi = a_2\iota\varphi = a_2 f = g_2$$

i sabíem que $g_1 \neq g_2$.

(b) Clarament, F també és lliure sobre la imatge de ι: tan sols cal prendre l'aplicació inclusió de $A\iota \longrightarrow F$. Per tant, un grup lliure sempre és lliure en un subconjunt. En aquest cas, es diu que F és lliure amb *base* $A\iota$, i dir que el diagrama és commutatiu equival a dir que φ és l'única extensió de f a F.

El següent que volem provar és que donat un conjunt no buit, sempre existeix un grup lliure sobre aquest, però per fer-ho, abans hem de definir el conceptes de paraula i paraula reduïda sobre un conjunt i dotar-los d'una operació.

Donat un conjunt A, considerem $A^{-1} = \{a^{-1} \mid a \in A\}$ i anomenem $\tilde{A} = A \cup A^{-1}$. Direm que una successió finita d'elements de $\tilde{A}$ és una *paraula* en $\tilde{A}$ i denotarem el conjunt de totes aquestes com $\tilde{A}^*$. En aquest conjunt també inclourem la paraula buida, que representarem com 1.

Podem considerar una operació sobre el conjunt de paraules com segueix: si $w = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ i $v = b_1^{\delta_1} \dots b_m^{\delta_m}$ amb $a_i, b_j \in A$ i $\varepsilon_i, \delta_j \in \{-1, 1\}$ són dues paraules sobre el conjunt $\tilde{A}$, el seu producte serà la paraula $wv = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} b_1^{\delta_1} \dots b_m^{\delta_m}$.

Donada una paraula $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}$ amb $a_i \in A$ i $\varepsilon_i \in \{-1, 1\}$, direm que la seua paraula *inversa* és $w^{-1} = a_n^{-\varepsilon_n} \dots a_2^{-\varepsilon_2} a_1^{-\varepsilon_1}$.

Una paraula $w = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ és *reduïda* si no té dues lletres adjacents de la forma aa^{-1} o $a^{-1}a$. Notem que la paraula inversa d'una paraula reduïda és també reduïda. A més, per conveni, la paraula buida és reduïda.

Una *subparaula* d'una paraula $w = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ és una paraula de la forma $v = a_i^{\varepsilon_i} \dots a_j^{\varepsilon_j}$ amb $1 \leq i \leq j \leq n$ o bé la paraula buida. Aleshores, v és una subparaula de w si existeixen dues subparaules (potser buides) w' i w'' amb $w = w'vw''$.

Ara bé, el producte de paraules no està ben definit sobre el conjunt de paraules reduïdes en $\tilde{A}$ perquè el fet que w i v siguen reduïdes no implica necessàriament que wv ho siga. Malgrat això, podem definir una nova multiplicació de paraules reduïdes: si w i v són reduïdes, considerarem el seu producte com la paraula reduïda obtinguda del producte wv anterior després de fer les cancel·lacions pertinents. Per ser més precisos, donades les paraules reduïdes w i v, existeix una subparaula (potser buida) u de w amb $w = w'u$ de manera que u^{-1} és una subparaula de v amb $v = u^{-1}v'$ i que verifica que $w'v'$ és una paraula reduïda. Aleshores, definim

el producte de paraules reduïdes com $wv = w'v'$. Aquest producte l'anomenarem *juxtaposició*.

Teorema 1.30. *Donat un conjunt A, existeix un grup lliure F amb base A.*

Demostració. Considerem F com el conjunt de totes les paraules reduïdes sobre $\tilde{A}$. Podríem demostrar que F és un grup amb l'operació de juxtaposició que acabem de definir, però per verificar l'associativitat hauríem d'analitzar molts casos. Enlloc d'això, emprarem el truc de Van der Waerden.

Per a cada $a \in A$ i $\varepsilon \in \{-1, 1\}$, considerem la funció $|a^\varepsilon| \colon F \longrightarrow F$ definida com

$$(a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n})|a^\varepsilon| = \begin{cases} a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} a^\varepsilon & \text{si } a^\varepsilon \neq a_n^{-\varepsilon_n}, \\ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_{n-1}^{\varepsilon_{n-1}} & \text{si } a^\varepsilon = a_n^{-\varepsilon_n}. \end{cases}$$

Com $|a^\varepsilon||a^{-\varepsilon}| = |a^{-\varepsilon}||a^\varepsilon| = 1_F$, tenim que $|a^\varepsilon|$ és una permutació de F amb inversa $|a^{-\varepsilon}|$. Siga S_F el grup simétric sobre F i considerem $\mathcal{F}$ el subgrup de S_F generat per $\mathcal{A} = \{|a| \mid a \in A\}$. Vegem que $\mathcal{F}$ és un grup lliure amb base $\mathcal{A}$. Notem que hi ha una bijecció $\xi : \mathcal{A} \longrightarrow A$, $|a| \mapsto a$.

Donat un element arbitrari $1 \neq g \in \mathcal{F}$, podem trobar una factorització

$$g = |a_1^{\varepsilon_1}| \cdots |a_n^{\varepsilon_n}| \tag{1.1}$$

amb $\varepsilon_i = \pm 1$ per a cada $i = 1, \dots, n$ i de forma que $|a^\varepsilon|$ i $|a^{-\varepsilon}|$ no siguen adjacents (en cas contrari, els cancel·lem). Observem que a més aquesta factorització és única ja que $1g = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ és el lletreig d'una paraula reduïda, que és clarament únic.

Per veure que $\mathcal{F}$ és lliure amb base $\mathcal{A}$, suposem que G és un grup i prenem una funció $f \colon \mathcal{A} \longrightarrow G$. Com que la factorització (1.1) és única, l'aplicació $\varphi \colon \mathcal{F} \longrightarrow G$ donada per $g\varphi = (|a_1^{\varepsilon_1}|f) \cdots (|a_n^{\varepsilon_n}|f)$ està ben definida i extén f. Per tant, només ens falta veure que φ és un homomorfisme; la unicitat de φ la tindrem perquè $\mathcal{A}$ genera $\mathcal{F}$ i dos homomorfismes que coincideixen en un sistema generador han de ser iguals.

Siguen w i v paraules reduïdes sobre $\mathcal{A}$. En cas que la paraula wv també siga reduïda, és clar que $(wv)\varphi = (w\varphi)(v\varphi)$. En cas contrari, escribim $w = w'u$ i $v = u^{-1}v'$ com en la definició de juxtaposició. Aleshores, tenim que

$$\begin{aligned} w\varphi &= (w'\varphi)(u\varphi) \\ v\varphi &= (u^{-1}\varphi)(v'\varphi) = (u\varphi)^{-1}(v'\varphi) \end{aligned}$$

amb la qual cosa,

$$(w\varphi)(v\varphi) = (w'\varphi)(u\varphi)(u\varphi)^{-1}(v'\varphi) = (w'\varphi)(v'\varphi)$$

i d'altra banda, com $w'v'$ és reduïda,

$$(wv)\varphi = (w'v')\varphi = (w'\varphi)(v'\varphi)$$

i així, φ és un homomorfisme.

Amb açò, hem vist que $\mathcal{F}$ és un grup lliure amb base $\mathcal{A}$. Ara bé, com l'aplicació $\tilde{\xi}\colon \mathcal{F} \longrightarrow F$ definida com $|a_1^{\varepsilon_1}| \cdots |a_n^{\varepsilon_n}| \mapsto a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ és una bijecció, si considerem en F l'operació induïda[2] per $\tilde{\xi}$ (és a dir, donats $\omega_1, \omega_2 \in F$, prenem com a producte $\omega_1 \cdot \omega_2 = (g_1 g_2)\tilde{\xi}$, on $g_1, g_2 \in \mathcal{F}$ amb $g_1\tilde{\xi} = \omega_1$ i $g_2\tilde{\xi} = \omega_2$), aleshores F és un grup i $\tilde{\xi}$ és un isomorfisme. A més, com $\mathcal{A}\tilde{\xi} = \mathcal{A}\xi = A$, tenim que F és un grup lliure amb base A, i A genera F ja que $\mathcal{A}$ genera $\mathcal{F}$. □

Corol·lari 1.31. *Qualsevol grup G és un quocient d'un grup lliure.*

Demostració. Construïm el conjunt $A = \{a_g \mid g \in G\}$ de manera que $f\colon A \longrightarrow G$, $a_g \mapsto g$ és una bijecció. Si F és un grup lliure amb base A, aleshores existeix un homomorfisme $\varphi\colon F \longrightarrow G$ que extén f. A més, φ ha de ser sobrejectiu perquè f ho és. Per tant, $F/\ker\varphi \cong F\varphi = G$. □

Lema 1.32. *Si F és un grup lliure amb base A, aleshores F/F' és un grup abelià lliure amb base $A_\sharp = \{aF' \mid a \in A\}$.*

Demostració. Suposem que G és un grup abelià i que $f\colon A_\sharp \longrightarrow G$ és una funció. Definim $f_\sharp\colon A \longrightarrow G$ tal que $af_\sharp = (aF')f$ per a cada $a \in A$. Com F és lliure amb base A, existeix un homomorfisme $\varphi\colon F \longrightarrow G$ que extén $f_\sharp$.

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & F \\ & \searrow^{f_\sharp} & \downarrow{\scriptstyle \varphi} \\ & & G \end{array}$$

Si prenem $\omega \in F'$, aleshores existeixen $\omega_1, \omega_2 \in F$ de manera que $\omega = [\omega_1, \omega_2]$. Llavors, $\omega\varphi = ([\omega_1, \omega_2])\varphi = (\omega_1\varphi)^{-1}(\omega_2\varphi)^{-1}(\omega_1\varphi)(\omega_2\varphi) = 1$ perquè G és abelià. Per tant, $F' \leq \ker\varphi$ i podem considerar l'homomorfisme $\tilde{\varphi}\colon F/F' \longrightarrow G$ definit com $\omega F' \mapsto \omega\varphi$ que extén f: donat $aF' \in A_\sharp$, $(aF')i\tilde{\varphi} = (aF')\tilde{\varphi} = a\varphi = ai\varphi = af_\sharp = (aF')f$, amb la qual cosa, $i\tilde{\varphi} = f$.

$$\begin{array}{ccc} A_\sharp & \xrightarrow{\ i\ } & F/F' \\ & \searrow^{f} & \downarrow{\scriptstyle \tilde{\varphi}} \\ & & G \end{array}$$

Vegem que $\tilde{\varphi}$ és única i haurem acabat: suposem que $\theta\colon F/F' \longrightarrow G$ és tal que $(aF')\theta = (aF')f$. Si $\nu\colon F \longrightarrow F/F'$ és l'homomorfisme natural, aleshores $\nu\theta\colon F \longrightarrow G$ és un homomorfisme amb $a\nu\theta = (aF')\theta = (aF')f = a\varphi$ per a tot $a \in A$. Ara, com A és una base de F, $\nu\theta = \varphi = \nu\tilde{\varphi}$ i com ν és sobrejectiu, $\theta = \tilde{\varphi}$. Així, F/F' és abelià lliure amb base A. □

[2]De fet, aquesta operació que s'indueix és la juxtaposició que hem definit prèviament.

Teorema 1.33. *Siguen F_1 i F_2 grups lliures amb bases A_1 i A_2, respectivament. Aleshores $F_1 \cong F_2$ si, i només si, $|A_1| = |A_2|$.*

Demostració. Comencem suposant que $|A_1| = |A_2|$. Prenem les aplicacions injectives $\iota_1 \colon A_1 \longrightarrow F_1$ i $\iota_2 \colon A_2 \longrightarrow F_2$ de la definició de grup lliure i considerem una bijecció $\alpha \colon A_1 \longrightarrow A_2$. Aleshores, existeixen β_1 i β_2 homomorfismes que fan commutatius els següents diagrames:

$$\begin{array}{ccc} A_1 & \xrightarrow{\iota_1} & F_1 \\ & \searrow^{\alpha\iota_2} & \downarrow{\scriptstyle \beta_1} \\ & & F_2 \end{array} \qquad\qquad \begin{array}{ccc} A_2 & \xrightarrow{\iota_2} & F_2 \\ & \searrow^{\alpha^{-1}\iota_1} & \downarrow{\scriptstyle \beta_2} \\ & & F_1 \end{array}$$

Notem que $\underbrace{\iota_1\beta_1}_{\alpha\iota_2}\beta_2 = \alpha\,\underbrace{\iota_2\beta_2}_{\alpha^{-1}\iota_1} = \alpha\alpha^{-1}\iota_1 = \iota_1$, amb la qual cosa, el diagrama

$$\begin{array}{ccc} A_1 & \xrightarrow{\iota_1} & F_1 \\ & \searrow^{\iota_1} & \downarrow{\scriptstyle \beta_1\beta_2} \\ & & F_1 \end{array}$$

és commutatiu. Ara bé, l'aplicació identitat sobre F_1 també fa aquest diagrama commutatiu. Llavors, per unicitat, $\beta_1\beta_2 = 1_{F_1}$. Amb un argument similar, $\beta_2\beta_1 = 1_{F_2}$ i per tant, β_1 és un isomorfisme i $F_1 \cong F_2$.

Suposem ara que $F_1 \cong F_2$, amb la qual cosa, $F_1/F_1' \cong F_2/F_2'$. Pel lema 1.32, F_1/F_1' és abelià lliure amb base $A_{\sharp,1} = \{aF_1' \mid a \in A_1\}$ i per tant, el seu rang és $|A_{\sharp,1}| = |A_1|$. Anàlogament, el rang de F_2/F_2' és $|A_2|$. Aleshores, pel teorema 1.13, tenim que $|A_1| = |A_2|$. □

Definició 1.34. El *rang* d'un grup lliure és el nombre d'elements de qualsevol de les seues bases.

Exemple: El grup cíclic infinit, $\mathbb{Z}$, és lliure amb base $A = \{1\}$. En canvi, $G = \mathbb{Z}\times\mathbb{Z}$ no és lliure: suposem que G fora lliure sobre un conjunt A. Clarament, $|A| \geq 2$ ja que en cas contrari $\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}$ i per tant, podem agafar $a, b \in A$ distints. Ara bé, $ab = ba$ com a elements de G (denotant la operació com a producte) però com a paraules reduïdes sobre A són distintes, amb la qual cosa, $G \ncong F$, on F és el grup lliure amb base A. Així, G no és lliure. De fet, l'únic grup que és alhora lliure i abelià lliure és $\mathbb{Z}$.

Nota 1.35. Després d'haver vist les propietats dels grups lliures i els grups abelians lliures, veiem que hi ha un clar paral·lelisme entre ambdues nocions. Açò es deu a que es poden veure com a objectes lliures en les categories de grups i de grups abelians, respectivament.

1.4.2 Presentacions de grups

Definició 1.36. Siguen A un conjunt i Δ una família de paraules sobre A. Es diu que un grup G té com a *generadors* A i com a *relacions* Δ si $G \cong F/R$, on F és el grup lliure amb base A i R és el subgrup normal de F generat per Δ. A més, el parell ordenat $\langle A \mid \Delta \rangle$ s'anomena *presentació* de G.

Nota 1.37. Segons hem vist al corol·lari 1.31, qualsevol grup G es pot veure com un quocient F/R d'un grup lliure F. En particular, qualsevol grup G té una presentació $\langle A \mid \Delta \rangle$: tan sols cal prendre una base A del grup lliure F i un conjunt Δ que genere el subgrup normal R.

Exemple: Un grup lliure té com a presentació $F = \langle A \mid \varnothing \rangle$, on $|A|$ és el rang de F. El grup abelià lliure G de rang $|A|$ té com a presentació

$$G = \langle A \mid aba^{-1}b^{-1}, \text{ per a tot } a, b \in A \rangle.$$

Exemple: Els grups cíclics admeten la presentació $\mathbb{Z}/n\mathbb{Z} = \langle a \mid a^n \rangle$, i un grup $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ té com a presentació $\langle a, b \mid a^n, b^m, aba^{-1}b^{-1} \rangle$.

Exemple: Un grup pot admetre distintes presentacions: per exemple, el grup simètric d'ordre 4 es pot veure com $S_4 = \langle a, b \mid a^4, b^2, (ab)^3 \rangle$, però també com $S_4 = \langle a, b \mid a^3, b^2, (ab)^4 \rangle$.

Exemple: Una possible presentació del grup dièdric d'ordre $2n$ és $D_n = \langle a, b \mid a^n, b^2, (ab)^2 \rangle$, mentre que la presentació $Q_8 = \langle i, j, k \mid i^2, j^2, k^2, ijk \rangle$ representa el grup quaterni.

Teorema 1.38 (Von Dyck)**.** *Siga A un conjunt i siga R el conjunt de paraules reduïdes sobre A. Suposem que el grup G té una presentació $\langle A \mid R \rangle$. Si H és un grup generat per A que satisfà les relacions de G, és a dir, per a tot $\omega \in R$, $\omega = 1$ en H, aleshores existeix un epimorfisme de grups de G en H.*

Definició 1.39. Direm que un grup G és *generat* per un conjunt A, o *A-generat*, si existeix una aplicació $f\colon A \longrightarrow G$ tal que la imatge de f és un sistema generador de G, açò és, si existeix un epimorfisme φ_G del grup lliure F sobre A a G.

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & F \\ & \searrow^{f} & \downarrow{\scriptstyle \varphi_G} \\ & & G \end{array}$$

En aquest cas, per simplificar la notació, podem identificar els elements de A amb les seues imatges en G i considerarem que φ_G és fix una vegada donats A i G.

Definició 1.40. Si G i H són dos grups A-generats amb epimorfismes associats φ_G i φ_H, direm que un homomorfisme $\varphi\colon G \longrightarrow H$ *manté generadors* si $\varphi_G\varphi = \varphi_H$. Clarament, aquest homomorfisme ha de ser un epimorfisme.

Capítol 2

Introducció a la teoria de grafs

Definició 2.1. Un *graf* Γ consisteix en un conjunt $V(\Gamma)$ de vèrtexs i un conjunt $E(\Gamma)$ d'arestes juntament amb dues funcions

$$\alpha\colon E(\Gamma) \longrightarrow V(\Gamma) \quad \text{i} \quad {}^{-}\colon E(\Gamma) \longrightarrow E(\Gamma)$$

de manera que per a qualsevol $e \in E(\Gamma)$, $\bar{\bar{e}} = e$ i $\bar{e} \neq e$. A més, podem definir $\omega\colon E(\Gamma) \longrightarrow V(\Gamma)$ com $e\omega = \bar{e}\alpha$. Quan Γ estiga clar, escriurem simplement $V = V(\Gamma)$ i $E = E(\Gamma)$.

Anomenarem *vèrtex inicial* de l'aresta e a $e\alpha$; $e\omega$ serà el *vèrtex final* i $\bar{e}$ l'aresta *inversa* de e. A més, direm que un graf Γ és *finit* si ho són $V(\Gamma)$ i $E(\Gamma)$.

Notem que $\mathbb{Z}_2$ actua lliurement sobre E via la involució $e \mapsto \bar{e}$, fet que motiva la definició següent.

Definició 2.2. Una *orientació* de Γ consisteix en l'elecció d'un representant de cada $\mathbb{Z}_2$-òrbita, és a dir, de cada parell d'arestes $\{e, \bar{e}\}$ s'escolleix exactament una. Els representants escollits s'anomenen *arestes positivament orientades*.

Un graf Γ junt a una orientació donada, s'anomena *graf orientat* o *dirigit*.

Si Γ és un graf orientat, denotarem per $E^+(\Gamma)$ al conjunt d'arestes positivament orientades. Aleshores, $E(\Gamma) = E^+(\Gamma) \cup \overline{E^+(\Gamma)}$ i la unió és disjunta. A més, un graf orientat està completament determinat per $E^+(\Gamma)$ i les funcions α i ω.

Normalment, per dibuixar grafs orientats només representem les arestes positivament orientades emprant una fletxa per marcar l'orientació. S'entén que l'aresta inversa és la mateixa però recorreguda en el sentit contrari al que marca la fletxa.

Definició 2.3. Un *camí* p de longitud $|p| = n$ en un graf Γ és una successió d'arestes $e_1 \dots e_n$ tal que $e_j\omega = e_{j+1}\alpha$ per a $j = 1, \dots, n-1$. Es diu que el camí p comença en $p\alpha = e_1\alpha$ i acaba en $p\omega = e_n\omega$.

En cas que $p\alpha = p\omega$, el camí p s'anomena *circuit* o *cicle*. En cada vèrtex v, considerarem el cicle buit (de longitud zero) i el denotarem per 1_v.

Si Γ és orientat i tots els e_j que formen el camí pertanyen a $E^+(\Gamma)$, p s'anomena *camí dirigit*. Per conveni, el cicle buit es considera dirigit.

El camí invers d'un camí p és $\bar{p} = \bar{e_n} \dots \bar{e_1}$. Notem que $\bar{p}\alpha = p\omega$, $\bar{p}\omega = p\alpha$ i $\bar{\bar{p}} = p$. Per conveni, $\bar{1_v} = 1_v$.

Quan tenim dos camins p_1 i p_2 de manera que $p_1\omega = p_2\alpha$, podem composar-los per obtindre'n un de nou, l'anomenat camí producte p_1p_2, juxtaposant les successions d'arestes. Clarament, si p_1 i p_2 són dirigits, p_1p_2 també ho serà. A més, el producte de dos cicles en un vèrtex també és un cicle.

La composició de camins és associativa i els camins buits actuen com identitats locals, per tant, tenim que els camins en Γ, $\Pi(\Gamma)$, formen una categoria menuda: els objectes són els vèrtexs $V(\Gamma)$ i donats dos vèrtexs $v_1, v_2 \in V(\Gamma)$, els morfismes són els camins de v_1 a v_2, denotats per $\Pi(\Gamma)(v_1, v_2)$. Notem que aquesta categoria té una operació involutiva: $p \mapsto \bar{p}$.

Quan Γ siga orientat, denotarem per Γ^* la subcategoria de $\Pi(\Gamma)$ consistent en tots els camins dirigits. Aquesta se sol anomenar categoria lliure generada pel graf dirigit Γ.

Definició 2.4. Direm que Γ és *feblement connex* si qualssevol dos vèrtexs es poden unir mitjançant un camí. Un graf orientat es diu que és *fortament connex* si podem fer el mateix amb camins dirigits.

Una component connexa d'un graf és un subgraf connex maximal i qualsevol graf és unió disjunta de les seues components connexes. Un subgraf maximal fortament connex en un graf orientat s'anomena component fortament connexa.

En un graf orientat, direm que el vèrtex w és *accessible* des del vèrtex v, i ho denotarem per $w \leq v$, si hi ha un camí dirigit que va de v a w. Notem que aquesta relació és un preordre i que, si considerem la relació d'equivalència associada a aquest, aleshores $v \equiv w$ si, i només si, estan en la mateixa component fortament connexa de Γ.

2.1 Grup fonamental d'un graf

Donats $p_1, p_2 \in \Pi(\Gamma)(v_1, v_2)$, direm que p_1 és *homotòpic* a p_2, i ho denotarem per $p_1 \sim p_2$, si p_1 es pot obtindre afegint o esborrant de p_2 camins de la forma $e\bar{e}$.

Com que clarament si $p_1 \sim p_2$ i $p_3 \sim p_4$, aleshores $p_1p_3 \sim p_2p_4$, tenim que aquesta relació d'equivalència és una congruència. Anomenarem $\pi(\Gamma)$ al quocient resultant. Notem que, donada $[p]$ la classe d'homotopia del camí p, el seu invers és $[p]^{-1} = [\bar{p}]$, i per tant, $\pi(\Gamma)$ és un grupoide al qual anomenarem *grupoide fonamental* de Γ.

Si $v \in V(\Gamma)$, aleshores definim $\pi_1(\Gamma, v)$ com $\pi(\Gamma)(v, v)$, és a dir, com el conjunt d'elements de $\pi(\Gamma)$ que comencen i acaben en el vèrtex v. Cadascun d'aquests conjunts és un grup que anomenarem *grup fonamental* de Γ en v.

Definició 2.5. Un camí $p \in \Pi(\Gamma)$ es diu *reduït* si no té cap subcamí de la forma $e\bar{e}$. De fet, qualsevol camí dirigit en un graf orientat és reduït.

Es pot provar que cada classe d'homotopia de $\pi(\Gamma)$ conté un únic camí reduït.

Definició 2.6. Un graf és un *bosc* si els seus cicles reduïts tenen longitud zero. Un *arbre* és un bosc connex.

Açò és, si Γ és connex, Γ és un arbre si $\pi_1(\Gamma, v) = 1_v$ per a cada $v \in V(\Gamma)$. A més, pel lema de Zorn, tot graf connex té un subarbre maximal que conté tot els vèrtexs.

Teorema 2.7. *Siguen Γ un graf connex orientat, $T \subseteq \Gamma$ un subarbre maximal i $v_0 \in V(\Gamma)$. Per a cada $v \in V(\Gamma)$, considerem p_v com l'únic camí reduït en T de v_0 a v, i per a cada $e \in E^+(\Gamma)$, definim $\tilde{e} = p_{e\alpha} e \overline{p_{e\omega}}$. Aleshores, $\pi_1(\Gamma, v_0)$ és un grup lliure generat per $\{[\tilde{e}] \mid e \notin E(T)\}$.*

Gràcies a aquest teorema, si Γ és finit, podem trobar algorísmicament una base per al grup fonamental de Γ en cada vèrtex: primer construïm l'arbre maximal T i després calculem els $\tilde{e}$ apropiats.

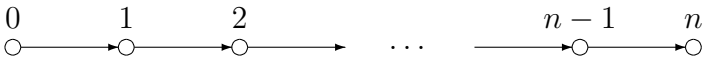
2.2 Morfismes de grafs i immersions

Definició 2.8. Un *morfisme de grafs* $\phi\colon \Gamma \longrightarrow \Delta$ consisteix en un parell de funcions $\phi_V\colon V(\Gamma) \longrightarrow V(\Delta)$ i $\phi_E\colon E(\Gamma) \longrightarrow E(\Delta)$, que per facilitar la notació denotarem indistintament com ϕ, que compleixen:

1. $e\phi\alpha = e\alpha\phi$, és a dir, el vèrtex origen de la imatge de e en Δ coincideix amb la imatge del vèrtex origen de e en Γ.
2. $\bar{e}\phi = \overline{e\phi}$, és a dir, la imatge de l'aresta inversa de e en Γ coincideix amb l'aresta inversa en Δ de la imatge de e.

Direm que un morfisme de grafs és *fidel* si $e_1\alpha = e_2\alpha, e_1\omega = e_2\omega$ i $e_1\phi = e_2\phi$ impliquen que $e_1 = e_2$.

Exemple: Podem descriure l'arc estàndard de longitud n, A_n, com l'interval $[0, n]$ subdividit pels enters i amb una aresta positivament orientada de j a $j + 1$ per a $j = 0, \ldots, n - 1$:



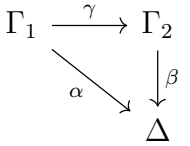
Aleshores, un camí p de longitud n de v_1 a v_2 es correspon a un morfisme de grafs $p\colon A_n \longrightarrow \Gamma$ amb $p(0) = v_1$ i $p(n) = v_2$.

Notem que els grafs formen una categoria on els objectes són els mateixos grafs i els morfismes són els morfismes de grafs. Aquesta categoria s'anomena *categoria dels grafs*.

Donats Γ i Δ grafs orientats, es diu que el morfisme ϕ *manté l'orientació* si envia arestes positivament orientades en Γ a arestes positivament orientades en Δ. Notem que un camí dirigit p de longitud n és un morfisme de grafs que manté l'orientació $p\colon A_n \longrightarrow \Gamma$.

Si $\phi\colon \Gamma \longrightarrow \Delta$ és un morfisme de grafs i Δ és orientat, aleshores hi ha una única orientació de Γ de manera que ϕ mantinga l'orientació i s'anomena *orientació de* Γ *induïda per* ϕ.

Lema 2.9. *Siguen* Γ_1, Γ_2 *i* Δ *grafs orientats i considerem el diagrama commutatiu de morfismes de grafs següent:*



Si γ *i* β *mantenen l'orientació, aleshores* α *també ho fa, i si* α *i* β *mantenen l'orientació, aleshores* γ *també.*

Aleshores, si tenim un graf orientat fix Δ i considerem tots els grafs amb morfismes a Δ i els orientem de forma que els morfismes que van a Δ mantinguen l'orientació, tots els morfismes entre els distints grafs mantindran l'orientació.

Definició 2.10. Donats un graf Γ i un vèrtex $v \in V(\Gamma)$, definim

$$\mathrm{Star}(v) = v\alpha^{-1} = \{e \in E(\Gamma) \mid e\alpha = v\}.$$

Si $\phi\colon \Gamma \longrightarrow \Delta$ és un morfisme de grafs, per a cada $v \in V(\Gamma)$ tenim l'aplicació induïda $\phi_v\colon \mathrm{Star}(v) \longrightarrow \mathrm{Star}(v\phi)$. Llavors, ϕ s'anomena:

1. *Immersió*, si ϕ_v és injectiva per a cada $v \in V(\Gamma)$.
2. *Localment sobrejectiu*, si ϕ_v és sobrejectiva per a cada $v \in V(\Gamma)$.
3. *Cobriment*, si ϕ_v és bijectiva per a cada $v \in V(\Gamma)$.

Clarament, la composició d'immersions és una immersió, la composició de morfismes localment sobrejectius és localment sobrejectiu i la composició de cobriments és un cobriment.
Exemple: Si el morfisme $p\colon A_n \longrightarrow \Gamma$ representa un camí reduït de longitud n en un graf Γ, aleshores p és una immersió.

2.3 Grafs etiquetats

Definició 2.11. Donat un conjunt A, definim el *ram* B_A com el graf amb un únic vèrtex, $V(B_A) = \{1\}$, i $|A|$ arestes (totes cicles) $E(B_A) = \tilde{A} = A \cup A^{-1}$. Orientarem B_A escollint $E^+(B_A) = A$ i farem que $a^{-1} = \bar{a}$.

Es pot veure fàcilment que $\Pi(B_A) = \tilde{A}^*$, $\pi(B_A) = FG(A)$, el grup lliure generat per A, i $B_A^* = A^*$.

Definició 2.12. Un *etiquetatge* d'un graf Γ sobre A consisteix en un morfisme de grafs fidel $l\colon \Gamma \longrightarrow B_A$, orientant Γ amb l'orientació induïda per l. Si e és una aresta de Γ, anomenarem *etiqueta de* e a el.

Podem generalitzar açò a camins: si considerem l'aplicació induïda

$$l\colon \Pi(\Gamma) \longrightarrow \tilde{A}^*,$$

donat un camí p, anomenarem *etiqueta de* p a pl. Notem que si p és un camí dirigit, aleshores $pl \in A^*$. A més, si pl és una paraula reduïda, aleshores p serà un camí reduït.

Podem pensar en un graf etiquetat com una col·lecció de vèrtexs i arestes orientades de manera que cadascuna d'aquestes últimes estiga etiquetada amb un element de A de forma que dues arestes amb els mateixos extrems no tinguen la mateixa etiqueta. Quan tinguem un graf Γ etiquetat amb A l'anomenarem *A-graf.*

2.4 El graf de Cayley

Definició 2.13. Donat un grup G A-generat, el *graf de Cayley* $\Gamma_A(G)$ de G amb respecte a A és un A-graf que té com a vèrtexs els elements de G, $V(\Gamma_A(G)) = G$, i com arestes el conjunt $E(\Gamma_A(G)) = G \times A$ de manera que donada una aresta $(g, a) \in E$, $(g, a)\alpha = g$ i $(g, a)\omega = ga$. Podem veure les arestes de manera més senzilla: són aquelles de la forma $g \xrightarrow{a} ga$, on $g \in G$ i $a \in A$, etiquetades amb a.

Notem que el graf de Cayley d'un grup A-generat G sempre és feblement connex.

Nota 2.14. A l'hora de representar els grafs de Cayley identificarem cada generador $a \in A$ amb un color diferent per tal de poder estalviar-nos escriure l'etiqueta en cada aresta. Així, la representació gràfica és més visual.

Exemple: El graf de Cayley d'un grup lliure sempre és un arbre. Per exemple, la figura 2.1 mostra el graf de Cayley del grup lliure $F = \langle a, b \mid \varnothing \rangle$ de rang 2.

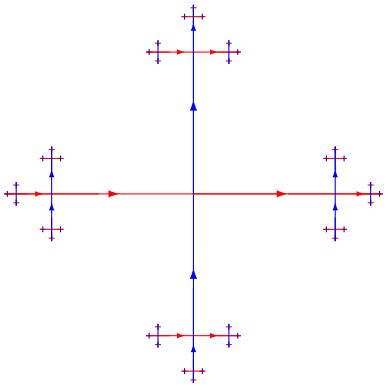


Figura 2.1: Graf de Cayley de F

El graf de Cayley del grup lliure de rang 1, $\mathbb{Z} = \langle a \mid \varnothing \rangle$, és simplement el que mostra la figura 2.2.

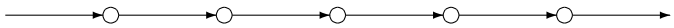


Figura 2.2: Graf de Cayley de $\mathbb{Z}$

Exemple: Un exemple senzill és el que proporcionen els grups cíclics: el graf de Cayley del grup $\mathbb{Z}/n\mathbb{Z} = \langle a \mid a^n \rangle$ és simplement un cicle de longitud n. La figura 2.3 representa aquest graf per a $n = 7$.

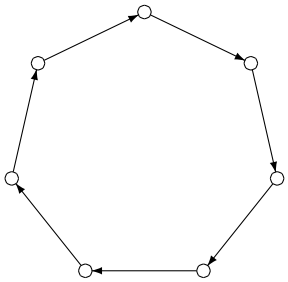
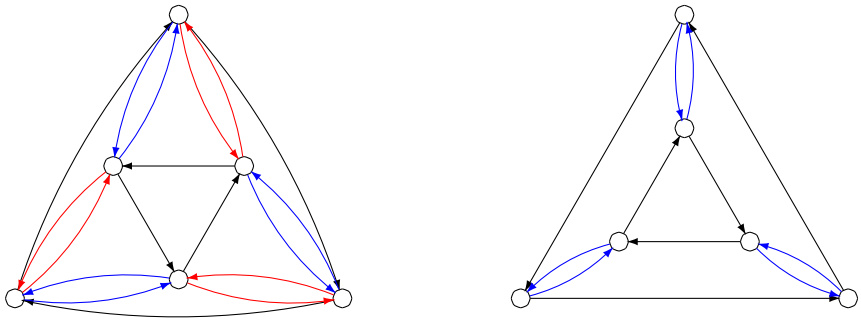


Figura 2.3: Graf de Cayley de $\mathbb{Z}/7\mathbb{Z}$

Exemple: El graf de Cayley d'un grup no és únic ja que depén del conjunt generador A escollit. La figura 2.4 mostra els grafs de Cayley del grup simètric d'ordre 3 associats a les presentacions $S_3 = \langle a, b, c \mid a^3, b^2, c^2, abc, (bc)^3 \rangle$ i $S_3 = \langle a, b \mid a^3, b^2, (ab)^2 \rangle$.



(a) Amb 3 generadors (b) Amb 2 generadors

Figura 2.4: Graf de Cayley per a S_3

Exemple: La figura 2.5 representa el graf de Cayley associat al grup alternat d'ordre 4 amb la presentació $A_4 = \langle a, b \mid a^3, b^2, (ab)^3 \rangle$.

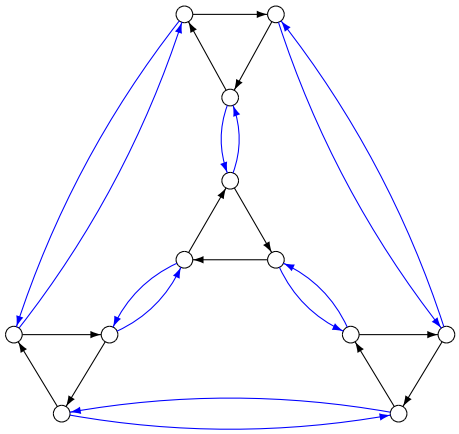


Figura 2.5: Graf de Cayley de A_4

Exemple: La figura 2.6 és el graf de Cayley de $D_4 = \langle a, b \mid a^4, b^2, (ab)^2 \rangle$.

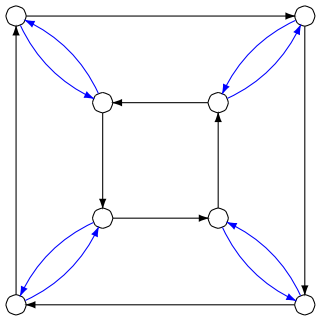


Figura 2.6: Graf de Cayley de D_4

Capítol 3

Extensions de grups tipus Gaschütz

Hi ha un resultat de Gaschütz que afirma que donat un grup finit A-generat G i un nombre primer p, existeix una extensió $G^\sharp$ de G i un epimorfisme $\varphi\colon G^\sharp \longrightarrow G$ el nucli del qual és un grup p-elemental abelià. De fet, aquesta extensió és universal sobre tots els grups amb aquesta propietat.

En aquest capítol, estudiarem aquesta extensió universal de Gaschütz i tractarem d'extendre el resultat per a qualsevol nombre natural m no necessàriament primer. A més, utilitzarem el graf de Cayley del grup G per construir un grup G^{Ab_m} que serà isomorf a l'extensió de Gaschütz $G^\sharp_m$. Per últim, intentarem fer una extensió tipus Gaschütz però infinita i de nou tractarem de construir-la amb l'ajuda del graf de Cayley.

Ara bé, el primer que farem serà provar el teorema de Nielsen–Schreier sobre subgrups de grups lliures ja que en la demostració d'aquest resultat emprarem una construcció que ens serà molt útil a l'hora de provar que G^{Ab_p} és isomorf a $G^\sharp$.

3.1 El teorema de Nielsen–Schreier

Notació 3.1. Suposem que tenim un conjunt A i un grup A-generat G. Siguen $A^{-1} = \{a^{-1} \mid a \in A\}$, $\tilde{A} = A \cup A^{-1}$ i $\tilde{A}^*$ el conjunt de totes les paraules amb lletres en $\tilde{A}$. Aleshores, donada una paraula $\omega \in \tilde{A}^*$, denotarem per $[\omega]_G$ a la imatge de ω mitjançant l'homomorfisme natural de $\tilde{A}^*$ a G, és a dir, si $\omega = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} \in \tilde{A}^*$ amb $a_i \in A$, $\varepsilon_i \in \{1, -1\}$ i $f\colon A \longrightarrow G$ és l'aplicació tal que la imatge de f és un sistema generador de G, aleshores

$$[\omega]_G = (a_1 f)^{\varepsilon_1} (a_2 f)^{\varepsilon_2} \cdots (a_n f)^{\varepsilon_n} \in G.$$

Ara bé, com hem dit en la definició 1.39 de grup A-generat, per simplificar la notació, podem identificar els elements de $a \in A$ amb les seues imatges en G, af. Per tant, podem dir simplement que $[\omega]_G = a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$.

Teorema 3.2 (Nielsen–Schreier)**.** *Siguen F un grup lliure i H un subgrup de F. Aleshores, H és lliure.*

Si, a més a més, F té rang n i H té índex finit en F, llavors el rang de H és $1 + |F : H|(n-1)$.

Demostració. Anomenem A a la base del grup lliure F i considerem el graf Γ amb vèrtexs $\{H\omega \mid \omega \in F\}$ i arcs de la forma $H\omega \xrightarrow{a} H\omega a$, on $\omega \in F$ i $a \in A$, etiquetades per a.

Com que el graf Γ és feblement connex, té un arbre generador T. Aleshores, donat $\omega \in F$ hi ha un únic camí de H a $H\omega$ en T. Denotarem aquest camí com p_ω. En cas que $H\omega = H$, direm que $p_\omega = 1$.

Donats $\omega \in F$ i $a \in A$, siga $r_{H\omega,a} = [p_\omega a p_{\omega a}^{-1}]_F$, és a dir, el camí en Γ format pel camí en T que va de H a $H\omega$, seguit de l'aresta $H\omega \xrightarrow{a} H\omega a$ i del camí invers en T del que va de H a $H\omega a$, vist com un element de F. Anàlogament, definim $r_{H\omega,a^{-1}} = [p_\omega a^{-1} p_{\omega a^{-1}}^{-1}]_F = (r_{H\omega a^{-1},a})^{-1}$.

Si $H\omega \xrightarrow{a} H\omega a$ és un arc de T, aleshores $r_{H\omega,a} = r_{H\omega a,a^{-1}} = 1$. En altre cas, $r_{H\omega,a} = (r_{H\omega a,a^{-1}})^{-1} \neq 1$, ja que el camí amb etiqueta $p_\omega a$ que comença en H conté una vegada l'arc $H\omega \xrightarrow{a} H\omega a$ que no pertany a T, mentre que el camí etiquetat amb $p_{\omega a}$ que comença en H només conté arcs de T.

Notem que donat $\omega \in F$ tenim que $\omega \in H$ si, i només si, ω (vist com element de $\tilde{A}^*$) és l'etiqueta d'un camí en Γ de H a H. Siga

$$B = \{r_{H\omega,a} \mid \omega \in F,\, a \in A,\, H\omega \xrightarrow{a} H\omega a \text{ no és un arc de } T\}.$$

Provarem que H és un grup lliure amb base B.

Siga $U = \langle B \rangle$. Com els generadors de U (vists com a paraules en $\tilde{A}^*$) són etiquetes de camins de H a H, tenim que $U \leq H$. Ara siga $\omega \in \tilde{A}^*$ tal que $[\omega]_F \in H$. Llavors, ω és la etiqueta d'un camí de H a H. Suposem que $\omega = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_t^{\varepsilon_t}$, on $a_i \in A$, $\varepsilon_i \in \{-1, 1\}$, $1 \leq i \leq t$. Aleshores

$$\begin{aligned}
\prod_{i=1}^{t} r_{Ha_1^{\varepsilon_1}\dots a_{i-1}^{\varepsilon_{i-1}},a_i^{\varepsilon_i}} &= \prod_{i=1}^{t} [p_{a_1^{\varepsilon_1}\dots a_{i-1}^{\varepsilon_{i-1}}} a_i^{\varepsilon_i} p^{-1}_{a_1^{\varepsilon_1}\dots a_i^{\varepsilon_i}}]_F \\
&= [a_1^{\varepsilon_1} p^{-1}_{a_1^{\varepsilon_1}}]_F [p_{a_1^{\varepsilon_1}} a_2^{\varepsilon_2} p^{-1}_{a_1^{\varepsilon_1} a_2^{\varepsilon_2}}]_F \dots [p_{a_1^{\varepsilon_1}\dots a_{t-1}^{\varepsilon_{t-1}}} a_t^{\varepsilon_t} p^{-1}_{a_1^{\varepsilon_1}\dots a_t^{\varepsilon_t}}]_F \\
&= [a_1^{\varepsilon_1} \dots a_t^{\varepsilon_t}]_F [p^{-1}_{a_1^{\varepsilon_1}\dots a_t^{\varepsilon_t}}]_F = [\omega]_F [p_\omega^{-1}]_F = [\omega]_F.
\end{aligned}$$

Així $\omega \in U$ perquè els factors del producte són o bé uns o bé generadors de U o els seus inversos, i per tant $H \leq U$. Aleshores, $H = U$.

Suposem ara que $\prod_{i=1}^{t} r_{H\omega_i,a_i^{\varepsilon_i}} = 1$, on $r_{H\omega_i,a_i^{\varepsilon_i}} \in B$ si $\varepsilon_i = 1$ o $r_{H\omega_i a_i^{-1},a_i} = (r_{H\omega_i,a_i^{-1}})^{-1} \in B$ si $\varepsilon_i = -1$ per a $1 \leq i \leq t$ i $t \geq 1$ és el més menut possible.

Aleshores, $\prod_{i=1}^{t} r_{H\omega_i,a_i^{\varepsilon_i}}$ pot interpretar-se com l'etiqueta d'un camí en Γ que comença en H i amb tots els arcs en T excepte els de la forma $H\omega_i \xrightarrow{a_i} H\omega_i a_i$ (si $\varepsilon_i = 1$) o $H\omega_i a_i^{-1} \xrightarrow{a_i} H\omega_i$ (si $\varepsilon_i = -1$), per a $1 \leq i \leq t$.

Com el producte és 1, l'operació de reduir el camí simplificant els productes de factors consecutius de la forma aa^{-1} o $a^{-1}a$ ha de convertir el camí en un de longitud zero. En particular, hi ha dos arcs consecutius no continguts en T que se simplifiquen, de la forma $H\omega_i \xrightarrow{a_i} H\omega_i a_i$ i el seu invers, o viceversa. Aquests arcs corresponen a $r_{H\omega_i,a_i}$ i $r_{H\omega_i a_i,a_i^{-1}} = (r_{H\omega_i,a_i})^{-1}$. Però en aquest cas, el producte d'aquests dos factors és trivial i per tant, podem trobar una altra expressió de 1 com a producte de factors de la forma $r_{H\omega,a^{\varepsilon}}$ amb menys factors, el que contradiu la minimalitat de t. Per tant, H és lliure amb base B.

Suposem ara que A i $|F : H|$ són finits. Llavors el graf Γ té $|F : H|$ vèrtexs i $n|F : H|$ arcs. Així, un arbre generador de Γ té exactament $|F : H| - 1$ arcs. Aleshores, Γ té $n|F : H| - (|F : H| - 1) = 1 + |F : H|(n - 1)$ arcs fora de l'arbre generador de Γ. Ara, com H és lliure en un conjunt amb el mateix cardinal que el conjunt d'arcs fora de l'arbre generador de Γ, H és lliure de rang $1+|F : H|(n-1)$, com volíem. □

3.2 El graf de Cayley i la construcció de l'extensió de Gaschütz

El següent és el resultat clàssic de Gaschütz sobre extensions universals que tractarem de generalitzar en els següents apartats:

Teorema 3.3 (Extensió de Gaschütz)**.** *Donat un grup finit A-generat G i un nombre primer p, aleshores existeixen un grup A-generat $G^\sharp$ i un epimorfisme $\varphi\colon G^\sharp \longrightarrow G$ que manté generadors el nucli del qual és un grup p-elemental abelià N amb la següent propietat universal:*

Si H és un grup A-generat i $\psi\colon H \longrightarrow G$ és un epimorfisme que manté generadors el nucli del qual és un grup p-elemental abelià K, aleshores existeix un epimorfisme $\beta\colon G^\sharp \longrightarrow H$ tal que $\beta\psi = \varphi$.

En la demostració d'aquest teorema es veu que si F és un grup lliure sobre A i R és un subgrup normal de F de manera que $F/R \cong G$, aleshores el grup $G^\sharp = F/R'R^p$ satisfà les condicions requerides. Una de les conseqüències més importants d'aquest resultat és que el grup $G^\sharp$ definit així, s'utilitza en la construcció del grup E: una extensió universal p-elemental de Frattini del grup finit G. E és un grup amb un subgrup normal $A \neq 1$ p-elemental abelià tal que $A \leq \Phi(E)$ i $E/A \cong G$. A més, aquesta extensió E juga un paper important en la prova del teorema de

Gaschütz, Lubeseder i Schmid que diu que tota formació saturada pot ser definida localment per una funció de formació.

La resta d'aquesta secció la dedicarem a construir, amb l'ajuda del graf de Cayley, un grup G^{Ab_p} i a demostrar que és isomorf a l'extensió $G^\sharp$ que dóna el teorema 3.3.

Considerem un grup finit A-generat G amb A finit. Si recordem la definició 2.13, el graf de Cayley de G amb respecte a A és aquell que té com a vèrtexs els elements de G i arestes de la forma $g \xrightarrow{a} ga$, on $g \in G$ i $a \in A$, etiquetades amb a. Anem a anomenar E al conjunt d'aquestes arestes.

Donat un nombre primer p, definim $V(E)$ l'espai vectorial sobre el cos $\mathbb{Z}/p\mathbb{Z}$ amb base E, és a dir, si $v \in V(E)$, aleshores $v = \sum_{i=1}^{|E|} m_i e_i$, on $m_i \in \mathbb{Z}/p\mathbb{Z}$ i $e_i \in E = \{e_1, \ldots, e_{|E|}\}$.

El grup G actua per l'esquerra sobre E com segueix:

$$\text{si } g \in G \text{ i } e_1 = h \xrightarrow{a} ha \in E, \text{ aleshores } g \cdot e_1 = e_2 = gh \xrightarrow{a} gha \in E,$$

per a tots $g, h \in G,\ a \in A$. Notem que aquesta acció la podem extendre de manera única a una acció de G sobre $V(E)$:

$$\text{si } g \in G \text{ i } v = \sum_{i=1}^{|E|} m_i e_i \in V(E), \text{ aleshores } g \cdot v = \sum_{i=1}^{|E|} m_i (g \cdot e_i) \in V(E).$$

Amb açò, podem considerar l'homomorfisme $\sigma\colon G \longrightarrow \mathrm{Aut}(V(E))$ tal que $g\sigma = \sigma_g \in \mathrm{Aut}(V(E))$ per a tot $g \in G$, on $v\sigma_g = g \cdot v$ per a $v \in V(E)$. Així, podem construir el producte semidirecte (extern) $U = [V(E)]G$ (via σ). Si recordem la definició 1.3, l'operació binària que fa que U siga grup és

$$(v, g)(v', g') = (v + v'\sigma_g, gg'),$$

per a tots $v, v' \in V(E),\ g, g' \in G$.[1]

Tot seguit, anem a considerar el subgrup

$$G^{Ab_p} = \langle (1 \xrightarrow{a} a, a) \mid a \in A \rangle$$

de U. Per veure quina forma tenen els elements de G^{Ab_p}, vegem primerament com funciona el producte de dos elements del seu sistema generador:

$$\begin{aligned}(1 \xrightarrow{a_1} a_1, a_1)(1 \xrightarrow{a_2} a_2, a_2) &= ((1 \xrightarrow{a_1} a_1) + \sigma_{a_1}(1 \xrightarrow{a_2} a_2), a_1 a_2) \\ &= ((1 \xrightarrow{a_1} a_1) + (a_1 \cdot (1 \xrightarrow{a_2} a_2)), a_1 a_2) \\ &= ((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1 a_2), a_1 a_2).\end{aligned}$$

[1] Notem que emprem notació additiva en el primer component malgrat que en el segon utilitzem notació multiplicativa perquè els elements de $V(E)$ commuten.

Notem que, en general, aquest producte no és commutatiu:

$$\begin{aligned}(1 \xrightarrow{a_2} a_2, a_2)(1 \xrightarrow{a_1} a_1, a_1) &= ((1 \xrightarrow{a_2} a_2) + (a_2 \xrightarrow{a_1} a_2a_1), a_2a_1)\\ &\neq (1 \xrightarrow{a_1} a_1, a_1)(1 \xrightarrow{a_2} a_2, a_2).\end{aligned}$$

Aleshores, com donat $u \in G^{Ab_p}$ existeixen $a_1, \dots, a_r$ en A (ordenats) amb r finit de manera que $u = \prod_{i=1}^{r}(1 \xrightarrow{a_i} a_i, a_i)$, desenvolupant el producte obtenim que els elements de G^{Ab_p} són de la forma

$$\begin{aligned}u &= \prod_{i=1}^{r}(1 \xrightarrow{a_i} a_i, a_i)\\ &= ((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1a_2) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} a_1 \cdots a_r), a_1 \cdots a_r).\end{aligned}$$

Per tant, podem interpretar cada element u de G^{Ab_p} com un camí del graf de Cayley de G que comença en 1, passa per les arestes que indica la primera component de u i acaba en el vèrtex indicat per la segona component.

Considerem ara el següent epimorfisme:

$$\begin{array}{rccc}\psi\colon & G^{Ab_p} & \longrightarrow & G\\ & (1 \xrightarrow{a} a, a) & \mapsto & a\end{array}$$

A continuació, anem a estudiar les propietats del seu nucli, que anomenarem C.

Donat $u = \prod_{i=1}^{r}(1 \xrightarrow{a_i} a_i, a_i) \in G^{Ab_p}$, aleshores $u\psi = \prod_{i=1}^{r}(1 \xrightarrow{a_i} a_i, a_i)\psi = \prod_{i=1}^{r} a_i$. Per tant, tindrem que $u \in C = \ker\psi$ si, i només si, $a_1 \cdots a_r = 1$, és a dir, si u és de la forma

$$((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1a_2) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1).$$

Notem que $u \in C$ es pot interpretar com el camí en el graf de Cayley de G que comença i acaba en 1 i que passa per les arestes descrites en la primera component.

Amb açò, com hem definit $V(E)$ com l'espai vectorial sobre el cos $\mathbb{Z}/p\mathbb{Z}$ amb base E, podem veure fàcilment que C és p-elemental abelià: donats $u, v \in C$ existeixen $a_1, \dots, a_r, b_1, \dots, b_s$ en A (ordenats) amb r i s finits de manera que

$$\begin{aligned}u &= ((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1a_2) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1)\\ v &= ((1 \xrightarrow{b_1} b_1) + (b_1 \xrightarrow{b_2} b_1b_2) + \cdots + (b_1 \cdots b_{s-1} \xrightarrow{b_s} 1), 1)\end{aligned}$$

i llavors,

$$\begin{aligned}uv &= ((1 \xrightarrow{a_1} a_1) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1) + (1 \xrightarrow{b_1} b_1) + \cdots + (b_1 \cdots b_{s-1} \xrightarrow{b_s} 1), 1)\\ &= ((1 \xrightarrow{b_1} b_1) + \cdots + (b_1 \cdots b_{s-1} \xrightarrow{b_s} 1) + (1 \xrightarrow{a_1} a_1) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1) = vu\\ u^p &= (\bar{p}(1 \xrightarrow{a_1} a_1) + \bar{p}(a_1 \xrightarrow{a_2} a_1a_2) + \cdots + \bar{p}(a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1) = (0, 1)\end{aligned}$$

D'altra banda, com G^{Ab_p} és clarament un grup A-generat,[2] donada una paraula

[2]És suficient prendre $f\colon A \longrightarrow G^{Ab_p}$ tal que $a \mapsto (1 \xrightarrow{a} a, a)$.

$\omega \in \tilde{A}^*$ podem trobar-ne l'element de G^{Ab_p} associat, $[\omega]_{G^{Ab_p}}$, com en la nota 3.1. De fet, si donada una aresta $e \in E$, denotem per $\omega(e)$ al nombre de vegades (amb signe)[3] que passa per aquesta aresta el camí del graf de Cayley de G etiquetat per ω i que comença en 1, i anomenem $\omega_p(e) = \omega(e) \mod p$, tenim que

$$[\omega]_{G^{Ab_p}} = \left(\sum_{e \in E} \omega_p(e) e, [\omega]_G \right).$$

Lema 3.4. *Suposem que tenim tres grups G_1, G_2 i G_3 de manera que existeixen epimorfismes $\alpha\colon G_1 \longrightarrow G_2$ i $\beta\colon G_2 \longrightarrow G_3$. Aleshores,* $\ker(\alpha\beta)/\ker\alpha \cong \ker\beta$.

Demostració. Vegem que $f\colon \ker(\alpha\beta)/\ker\alpha \longrightarrow \ker\beta$ donada per $x\ker\alpha \mapsto x\alpha$, amb $x \in \ker(\alpha\beta)$, és un isomorfisme.

Si $x, y \in \ker(\alpha\beta)$, aleshores

$$\begin{aligned} x\ker\alpha = y\ker\alpha &\iff xy^{-1} \in \ker\alpha \iff (xy^{-1})\alpha = 1 \iff x\alpha(y\alpha)^{-1} = 1 \\ &\iff (x\ker\alpha)f = x\alpha = y\alpha = (y\ker\alpha)f, \end{aligned}$$

amb la qual cosa, f està ben definida i és injectiva. A més, com α és un homomorfisme, f també ho és.

Ara, si $y \in \ker\beta$, com α és suprajectiva, existeix $x \in G_1$ de manera que $x\alpha = y$. A més, $x\alpha\beta = y\beta = 1$ i llavors $x \in \ker(\alpha\beta)$. Així, l'antiimatge mitjançant f de y és $x\ker\alpha$ i f és suprajectiva. □

Teorema 3.5. *El grup G^{Ab_p} és isomorf al grup $G^\sharp$ del teorema 3.3.*

Demostració. Malgrat que en aquesta secció no ho hem provat ja que més endavant ho veurem en un cas més general, el grup $G^\sharp = F/R^\sharp$ amb $R^\sharp = R'R^p$, on F és el grup lliure sobre A i R és un subgrup normal de F amb $F/R \cong G$, verifica les condicions del teorema 3.3. A més, el nucli N de l'epimorfisme φ de l'enunciat és $N = R/R^\sharp$.

La construcció del Teorema 3.2 per a $H = R$ dóna un graf Γ isomorf al graf de Cayley de G si identifiquem els elements $g \in G$ amb coclasses a dreta $R\omega$ amb $\omega \in F$. Així, escriurem $r_{g,a}$ en lloc de $r_{R\omega,a}$. Per tant, R està generat per $B = \{r_{g,a} \mid g \in G,\ a \in A,\ g \xrightarrow{a} ga \text{ no està en } T\}$, on T és un arbre generador del graf de Cayley de G.

Notem que si associem cada element $g \in G$ amb una coclasses a dreta $R\omega$ amb $\omega \in F$, el neutre 1 de G s'identifica amb R. Aleshores, p_ω serà l'únic camí en T que va de 1 a $[\omega]_G$ (en cas que $[\omega]_G = 1$, direm que $p_\omega = 1$) i $r_{g,a} = [p_\omega a p_{\omega a}^{-1}]_F$ amb $[\omega]_G = g$ (si $g \xrightarrow{a} ga$ és un arc de T, aleshores $r_{g,a} = 1$).

[3] Cada vegada que el camí ω passa per una aresta $e = (g \xrightarrow{a} ga) \in E$ en sentit contrari (una de les lletres de la paraula ω és a^{-1}), $\omega(e)$ es redueix una unitat.

A continuació, considerem l'epimorfisme $\mu\colon F \longrightarrow G^{Ab_p}$ tal que $\omega \mapsto [\omega]_{G^{Ab_p}}$. Anem a veure que el conjunt $\overline{B} = \{\overline{r}_{g,a} \mid r_{g,a} \in B\}$, on $\overline{r}_{g,a}$ denota la imatge de $r_{g,a}$ sota l'epimorfisme que acabem de definir, és una base del $\mathbb{Z}/p\mathbb{Z}$-espai vectorial C, amb la qual cosa, la dimensió de C serà $|\overline{B}| = |B|$.

Com $\overline{r}_{g,a} \in \overline{B}$ representa un camí en el graf de Cayley que comença i acaba en 1, tenim que $\overline{r}_{g,a} \in C$. A més, com cada $\overline{r}_{g,a}$ té un únic arc que no està en T, l'arc $g \xrightarrow{a} ga$, i aquest no forma part de cap dels altres camins de $\overline{B}$, tenim que $\overline{B}$ és linealment independent.

Donat $u \in C$, existeix $\omega \in \tilde{A}^*$ de manera que $u = [\omega]_{G^{Ab_p}}$ i $[\omega]_G = 1$. Si $\omega = a_1 \dots a_t$, per a cada $i = 1, \dots, t$, denotarem per $\omega_i = a_1 \dots a_i$ i per $g_i = [\omega_i]_G$. Aleshores, de manera semblant al que hem fet en la prova del teorema de Nielsen–Schreier,

$$\begin{aligned}\prod_{i=1}^{t} r_{g_{i-1},a_i}\mu &= \left(\prod_{i=1}^{t} r_{g_{i-1},a_i}\right)\mu = \left(\prod_{i=1}^{t} [p_{\omega_{i-1}} a_i p_{\omega_i}^{-1}]_F\right)\mu \\ &= \left([\omega]_F [p_\omega^{-1}]_F\right)\mu = [\omega]_{G^{Ab_p}} = u.\end{aligned}$$

Ara bé, els únics factors que no són trivials en el producte anterior són els $r_{g_{i-1},a_i}\mu$ tals que l'arc $g_{i-1} \xrightarrow{a_i} g_i$ no està en T, amb la qual cosa, $r_{g_{i-1},a_i}\mu = \overline{r}_{g_{i-1},a_i} \in \overline{B}$. Així, $\overline{B}$ és un sistema generador de C i per tant, n'és base.

D'altra banda, com $R/R^\sharp$ és p-elemental abelià, el podem veure com a $\mathbb{Z}/p\mathbb{Z}$-espai vectorial i com el conjunt $\{r_{g,a}R^\sharp \mid r_{g,a} \in B\}$ n'és un conjunt generador, la dimensió de $R/R^\sharp$ com a $\mathbb{Z}/p\mathbb{Z}$-espai vectorial és com a molt $|B|$.

Per la universalitat de $G^\sharp$, existeix un epimorfisme $\beta\colon G^\sharp \longrightarrow G^{Ab_p}$ tal que $\beta\psi = \varphi$.

$$\begin{array}{ccc} G^\sharp & \xrightarrow{\beta} & G^{Ab_p} \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \psi} \\ & & G \end{array}$$

Per tant, com $G^{Ab_p} \cong G^\sharp/\ker\beta$, si veiem que $K = \ker\beta = 1$, tindrem que G^{Ab_p} i $G^\sharp$ són isomorfs. Pel lema 3.4, tenim que

$$\frac{R/R^\sharp}{K} = \frac{\ker\varphi}{\ker\beta} \cong \ker\psi = C.$$

Així, veient $R/R^\sharp$ i C com a $\mathbb{Z}/p\mathbb{Z}$-espais vectorials, existeix una aplicació lineal suprajectiva $\gamma\colon R/R^\sharp \longrightarrow C$ amb nucli K, i llavors

$$|B| \geq \dim R/R^\sharp = \dim K + \dim C = \dim K + |B| \Longrightarrow \dim K = 0,$$

i així, $K = \ker\beta = 1$. □

Exemple: Anem a calcular l'extensió de Gaschütz amb $p = 2$ del grup G cíclic d'ordre 3 de dues formes: treballant com en el teorema 3.3 i calculant el grup G^{Ab_p}.

1. Sabem que G es pot veure com a quocient del grup lliure de rang 1: $G = \mathbb{Z}/3\mathbb{Z}$. Així, si anomenem $F = \mathbb{Z}$ i $R = 3\mathbb{Z}$, el grup que busquem és $G^\sharp = F/(R'R^2)$. Ara bé, com R és abelià, $R' = 1$ i $R^2 = 2(3\mathbb{Z}) = 6\mathbb{Z}$ (emprem notació additiva perquè estem treballant amb grups abelians). Per tant, l'extensió que busquem és $G^\sharp = \mathbb{Z}/6\mathbb{Z}$, el grup cíclic d'ordre 6.

2. La figura 3.1 mostra el graf de Cayley de G. Aleshores, el grup que busquem és $G^{Ab_2} = \langle (1 \xrightarrow{a} a, a) \rangle$. Anem a comprovar que aquest és el grup cíclic d'ordre 6:

$$
\begin{aligned}
(1 \xrightarrow{a} a, a)^2 &= ((1 \xrightarrow{a} a) + (a \xrightarrow{a} a^2), a^2);\\
(1 \xrightarrow{a} a, a)^3 &= ((1 \xrightarrow{a} a) + (a \xrightarrow{a} a^2) + (a^2 \xrightarrow{a} 1), 1);\\
(1 \xrightarrow{a} a, a)^4 &= ((1 \xrightarrow{a} a) + (a \xrightarrow{a} a^2) + (a^2 \xrightarrow{a} 1) + (1 \xrightarrow{a} a), a)\\
&= (2 \cdot (1 \xrightarrow{a} a) + (a \xrightarrow{a} a^2) + (a^2 \xrightarrow{a} 1), a)\\
&= ((a \xrightarrow{a} a^2) + (a^2 \xrightarrow{a} 1), a);\\
(1 \xrightarrow{a} a, a)^5 &= (2 \cdot (a \xrightarrow{a} a^2) + (a^2 \xrightarrow{a} 1), a^2)\\
&= (a^2 \xrightarrow{a} 1, a^2);\\
(1 \xrightarrow{a} a, a)^6 &= (2 \cdot (a^2 \xrightarrow{a} 1), 1) = (0, 1).
\end{aligned}
$$

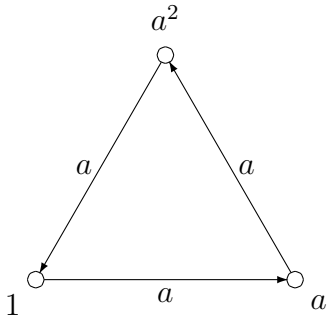


Figura 3.1: Graf de Cayley de $\mathbb{Z}/3\mathbb{Z}$

3.3 Extensió a m del teorema de Gaschütz

Tot seguit, generalitzarem el resultat de Gaschütz mostrat en l'apartat anterior per a qualsevol natural m. A continuació, veurem si existeix alguna relació entre aquesta extensió i les que s'obtenen amb les potències de nombres primers de la descomposició de m. Per acabar, veurem si en aquest cas també podem obtindre un grup isomorf a l'extensió tipus Gaschütz mitjançant el graf de Cayley del grup original.

Teorema 3.6. *Donats un grup finit A-generat G i un nombre natural m, aleshores existeixen un grup A-generat $G^\sharp$ i un epimorfisme $\varphi\colon G^\sharp \longrightarrow G$ que manté generadors el nucli del qual és un grup N abelià i amb exponent m amb la següent propietat universal:*

Si H és un grup A-generat i $\psi\colon H \longrightarrow G$ és un epimorfisme que manté generadors el nucli del qual és un grup K abelià amb exponent m, aleshores existeix un epimorfisme $\beta\colon G^\sharp \longrightarrow H$ tal que $\beta\psi = \varphi$.

Demostració. Siga G un grup A-generat amb epimorfisme associat $\varphi_G\colon F \longrightarrow G$, on F és el grup lliure amb base A. Aleshores, $R = \ker\varphi_G$ és subgrup normal de F i $G \cong F/R$.

Construïm $R^\sharp = R'R^m$ i considerem $G^\sharp = F/R^\sharp$. Aleshores, $G^\sharp$ és un grup A-generat perquè

$$\begin{array}{rccc} \varphi_{G^\sharp}\colon & F & \longrightarrow & G^\sharp \\ & \omega & \mapsto & \omega R^\sharp \end{array}$$

és un epimorfisme del grup lliure F sobre A en $G^\sharp$.

Ara podem considerar l'epimorfisme

$$\begin{array}{rccc} \varphi\colon & G^\sharp = F/R^\sharp & \longrightarrow & G = F/R \\ & \omega R^\sharp & \mapsto & \omega R \end{array}$$

el nucli del qual és $N = R/R^\sharp$ ja que $(\omega R^\sharp)\varphi = \omega R = R$ si, i només si, $w \in R$. Anem a comprobar que $N = R/R^\sharp$ és un subgrup normal abelià amb exponent m de $F/R^\sharp$:

$$(r_1R^\sharp)(r_2R^\sharp) = r_1r_2R'R^m = r_1r_2\underbrace{r_2^{-1}r_1^{-1}r_2r_1}_{\in R'}R'R^m = r_2r_1R'R^m = (r_2R^\sharp)(r_1R^\sharp);$$

$$(rR^\sharp)^m = r^mR^\sharp = r^mR'R^m = \underbrace{1\cdot r^m}_{\in R'R^m}R'R^m = R'R^m = R^\sharp.$$

A més, φ manté generadors perquè si veiem φ_G com

$$\begin{array}{rccc} \varphi_G\colon & F & \longrightarrow & G = F/R \\ & \omega & \mapsto & \omega R \end{array}$$

clarament $\varphi_{G^\sharp}\varphi = \varphi_G$.

Vegem ara que es verifica la propietat universal de l'enunciat del teorema: siga H un grup A-generat amb epimorfisme associat $\varphi_H\colon F \longrightarrow H$ i siga $\psi\colon H \longrightarrow G$ un epimorfisme que manté generadors amb nucli un subgrup normal K abelià i d'exponent m.

Donat $\omega \in R$, com ψ manté generadors, $\omega\varphi_H\psi = \omega\varphi_G = 1$. Així, en particular, $\omega\varphi_H \in K$. Aleshores, si $\omega_1, \omega_2 \in R$, per les propietats de K, tenim que:

$$\begin{aligned}([\omega_1,\omega_2])\varphi_H &= (\omega_1^{-1}\omega_2^{-1}\omega_1\omega_2)\varphi_H = (\omega_1\varphi_H)^{-1}(\omega_2\varphi_H)^{-1}(\omega_1\varphi_H)(\omega_2\varphi_H)\\ &= (\omega_1\varphi_H)^{-1}(\omega_2\varphi_H)^{-1}(\omega_2\varphi_H)(\omega_1\varphi_H) = 1.\\ (\omega_1^m)\varphi_H &= (\omega_1\varphi_H)^m = 1.\end{aligned}$$

Donat $\omega \in R^\sharp = R'R^m$, existeixen $\omega_1, \omega_2, \omega_3 \in R$ amb $\omega = [\omega_1,\omega_2]\omega_3^m$ i, pel que acabem de veure, la imatge de ω en H és

$$\omega\varphi_H = ([\omega_1,\omega_2])\varphi_H(\omega_3^m)\varphi_H = 1.$$

Per tant, H satisfà les relacions de $G^\sharp$ i llavors, pel teorema de von Dyck, existeix un epimorfisme $\beta\colon G^\sharp \longrightarrow H$ que manté generadors tal que $\beta\psi = \varphi$. □

3.3.1 Factorització en producte subdirecte de l'extensió

Suposem que tenim G un grup finit A-generat i un nombre natural $m = m_1m_2$ on m_1 i m_2 són nombres coprimers. Anem a veure que l'extensió universal $G_m^\sharp$ del teorema 3.6 es pot veure com a producte subdirecte de les extensions $G_1^\sharp = F/R_1^\sharp = F/(R'R^{m_1})$ i $G_2^\sharp = F/R_2^\sharp = F/(R'R^{m_2})$.

Considerem els epimorfismes

$$\begin{array}{rccc}\varepsilon_1\colon & G_1^\sharp = F/R_1^\sharp & \longrightarrow & F\\ & \omega R'R^{m_1} & \mapsto & \omega\end{array}$$

$$\begin{array}{rccc}\varepsilon_2\colon & G_2^\sharp = F/R_2^\sharp & \longrightarrow & F\\ & \omega R'R^{m_2} & \mapsto & \omega\end{array}$$

Aleshores, el producte subdirecte de $G_1^\sharp$ i $G_2^\sharp$ amb factor de grup amalgamat F és

$$G = \{(g_1,g_2) \mid g_1 \in G_1^\sharp,\ g_2 \in G_2^\sharp,\ g_1\varepsilon_1 = g_2\varepsilon_2\} = \{(\omega R_1^\sharp, \omega R_2^\sharp) \mid \omega \in F\}.$$

Si trobem un isomorfisme entre aquest grup i $G_m^\sharp$ ja ho tindrem. Considerem l'aplicació

$$\begin{array}{rccc}\phi\colon & G & \longrightarrow & G_m^\sharp\\ & (\omega R'R^{m_1}, \omega R'R^{m_2}) & \mapsto & \omega R'R^m\end{array}$$

Clarament, ϕ és un homomorfisme sobrejectiu i per tant, només ens falta veure que també és injectiu:

$$\begin{aligned}(\omega R'R^{m_1}, \omega R'R^{m_2}) \in \ker\phi &\Leftrightarrow \omega \in R'R^m \\ &\Leftrightarrow \omega = [r_1, r_2]r_3^m = [r_1, r_2](r_3^{m_2})^{m_1} = [r_1, r_2](r_3^{m_1})^{m_2} \\ &\Leftrightarrow w \in R'R^{m_1} \cap R'R^{m_2} \\ &\Leftrightarrow (\omega R'R^{m_1}, \omega R'R^{m_2}) = (R'R^{m_1}, R'R^{m_2})\end{aligned}$$

Per tant, $\ker\phi = \{(R_1^\sharp, R_2^\sharp)\}$ i ϕ és un isomorfisme.

Emprant aquest raonament successivament, si prenem un nombre natural m de manera que la seua descomposició en factors primers siga $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, l'extensió universal $G_m^\sharp$ del teorema 3.6 es pot veure com a producte subdirecte de les extensions $G_1^\sharp, G_2^\sharp, \ldots, G_n^\sharp$, on $G_i^\sharp = F/R_i^\sharp = F/(R'R^{p_i^{\alpha_i}})$ per a cada $i = 1, \ldots, n$.

3.3.2 Interpretació en termes del graf de Cayley

A continuació, anem a veure si podem trobar una interpretació en termes del graf de Cayley equivalent a la vista en la secció anterior per a l'extensió $G_m^\sharp$ amb m un nombre natural.

Considerem el graf de Cayley del grup A-generat G amb respecte a A i anomenem E al conjunt d'arestes d'aquest. Tot seguit, considerem M el $\mathbb{Z}/m\mathbb{Z}$-mòdul lliure sobre E. Així, si $x \in M$, aleshores existeixen uns únics $m_e \in \mathbb{Z}/m\mathbb{Z}$ tals que $x = \sum_{e\in E} m_e e$.

Recordem que el grup G actua per l'esquerra sobre E com segueix:

$$\text{si } g \in G \text{ i } e_1 = h \xrightarrow{a} ha \in E, \text{ aleshores } g \cdot e_1 = e_2 = gh \xrightarrow{a} gha \in E.$$

Podem extendre l'acció a una acció de G per l'esquerra sobre M fent

$$g \cdot x = \sum_{e\in E} m_e g \cdot e,$$

per a cada $g \in G$ i $x \in M$.

Llavors, tenim que $\sigma\colon G \longrightarrow \mathrm{Aut}(M)$ tal que $g\sigma = \sigma_g \in \mathrm{Aut}(M)$ per a tot $g \in G$, on $x\sigma_g = g\cdot x$ per a $x \in M$, és un homomorfisme. Amb açò, podem construir el producte semidirecte (extern) $U = [M]G$ amb l'operació

$$(x, g)(x', g') = (x + x'\sigma_g, gg'),$$

per a tots $x, x' \in M,\ g, g' \in G$.

Seguidament, prenem el subgrup de U definit com segueix:

$$G^{Ab_m} = \langle (1 \xrightarrow{a} a, a) \mid a \in A\rangle.$$

Treballant de manera similar al que hem fet per a un nombre primer p, cada element $u \in G^{Ab_m}$ es pot escriure com

$$\begin{aligned} u &= \prod_{i=1}^{r} (1 \xrightarrow{a_i} a_i, a_i) \\ &= ((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1a_2) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} a_1 \cdots a_r), a_1 \cdots a_r). \end{aligned}$$

per a determinats $a_1, \ldots, a_r$ en A (ordenats) amb r finit. A més, donada una paraula $\omega \in \tilde{A}^*$,

$$[\omega]_{G^{Ab_m}} = \left(\sum_{e \in E} \omega_m(e)e, [\omega]_G \right),$$

on $\omega_m(e)$ denota el nombre de vegades (amb signe) mòdul m que l'aresta e és creuada pel camí del graf de Cayley de G que comença en 1 i té ω per etiqueta.

D'altra banda, si considerem l'epimorfisme

$$\begin{array}{rccc} \psi\colon & G^{Ab_m} & \longrightarrow & G \\ & (1 \xrightarrow{a} a, a) & \mapsto & a \end{array}$$

és fàcil veure que el seu nucli, $\ker \psi = C$, és abelià i té exponent m: en primer lloc, $u \in C$ si, i només si, u és de la forma

$$((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1a_2) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1),$$

per a determinats $a_1, \ldots, a_r \in A$ ordenats. De nou, els elements de C es poden interpretar com camins del graf de Cayley de G que comencen i acaben en 1. Ara, donats $u, v \in C$ existeixen $a_1, \ldots, a_r, b_1, \ldots, b_s$ en A (ordenats) de manera que

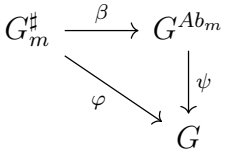
$$\begin{aligned} u &= ((1 \xrightarrow{a_1} a_1) + (a_1 \xrightarrow{a_2} a_1a_2) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1) \\ v &= ((1 \xrightarrow{b_1} b_1) + (b_1 \xrightarrow{b_2} b_1b_2) + \cdots + (b_1 \cdots b_{s-1} \xrightarrow{b_s} 1), 1) \end{aligned}$$

i com hem definit M com el $\mathbb{Z}/m\mathbb{Z}$-mòdul lliure sobre E, tenim que

$$\begin{aligned} uv &= ((1 \xrightarrow{a_1} a_1) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1) + (1 \xrightarrow{b_1} b_1) + \cdots + (b_1 \cdots b_{s-1} \xrightarrow{b_s} 1), 1) \\ &= ((1 \xrightarrow{b_1} b_1) + \cdots + (b_1 \cdots b_{s-1} \xrightarrow{b_s} 1) + (1 \xrightarrow{a_1} a_1) + \cdots + (a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1) = vu \\ u^m &= (\bar{m}(1 \xrightarrow{a_1} a_1) + \bar{m}(a_1 \xrightarrow{a_2} a_1a_2) + \cdots + \bar{m}(a_1 \cdots a_{r-1} \xrightarrow{a_r} 1), 1) = (0, 1) \end{aligned}$$

Teorema 3.7. *El grup G^{Ab_m} és isomorf al grup $G_m^\sharp$ del teorema 3.6.*

Demostració. Per la universalitat de $G_m^\sharp$ vista al teorema 3.6, existeix un epimorfisme $\beta\colon G_m^\sharp \longrightarrow G^{Ab_m}$ tal que $\beta\psi = \varphi$.



Per tant, $G^{Ab_m} \cong G_m^\sharp/K$, on $K = \ker\beta$. Pel lema 3.4, tenim que

$$\frac{R/R^\sharp}{K} = \frac{\ker\varphi}{\ker\beta} \cong \ker\psi = C.$$

Seguidament provarem que $|R/R^\sharp| \leq m^t$ i $|C| \geq m^t$, on t és el nombre d'arestes que hi ha fora d'un arbre generador del graf de Cayley de G. Aleshores, tindrem que

$$\frac{m^t}{|K|} \geq \frac{|R/R^\sharp|}{|K|} = |C| \geq m^t \Longrightarrow 1 \geq |K| \Longrightarrow K = 1,$$

i així, β serà un isomorfisme.

D'una banda, si en la demostració del teorema 3.2 prenem com a H el grup R, tenim que el graf Γ és isomorf al graf de Cayley de G (identificant els elements $g \in G$ amb coclasses $R\omega$ amb $\omega \in F$). Llavors, R és un grup lliure sobre el conjunt $B = \{r_{g,a} \mid g \in G,\, a \in A,\, g \xrightarrow{a} ga \text{ no està en } T\}$, on T és un arbre generador del graf de Cayley de G i clarament, $|B| = t$. Per facilitar la notació, podem enumerar els elements de B; així, $B = \{r_1, r_2, \ldots, r_t\}$. Notem que, donat un element qualsevol $xR^\sharp \in R/R^\sharp$, tenim que x es pot veure com una paraula $x = s_1 \ldots s_n$ amb cada $s_i \in B \cup B^{-1}$. Ara bé, com $R/R^\sharp$ és abelià i té exponent m, reordenant els factors quan calga i tenint en compte que $(r_iR^\sharp)^{-1} = (r_iR^\sharp)^{m-1}$, tenim que

$$xR^\sharp = (s_1 \ldots s_n)R^\sharp = (s_1R^\sharp)\cdots(s_nR^\sharp) = (r_1R^\sharp)^{\alpha_1}\cdots(r_tR^\sharp)^{\alpha_t},$$

amb $\alpha_i \in \{0, 1, \ldots, m\}$ per a cada $i = 1, \ldots, t$. Llavors, com per a cada α_i hi ha m possibilitat i açò passa per a tot element de $R/R^\sharp$, tenim que $|R/R^\sharp| \leq m^t$.

D'altra banda, els elements de B es poden veure com a camins del graf de Cayley de G que comencen i acaben en 1 i amb una única aresta fora de l'arbre generador T, amb la qual cosa, els podem veure com elements distints de C. A més, si $r_i \in C$, els elements $\{r_i^0, r_i^1, \ldots, r_i^{m-1}\}$ són tots distints ja que si anomenem ω a la paraula en A que dóna lloc a l'element r_i^j $(0 \leq j \leq m-1)$, llavors en l'expressió

$$[\omega]_{G^{Ab_m}} = \left(\sum_{e\in E} \omega_m(e)e, [\omega]_G\right),$$

es té que $\omega_m(\bar{e}) = j$, on $\bar{e}$ és l'aresta de r_i^j que no està en l'arbre generador. Aleshores, els m^t possibles elements de C de la forma $r_1^{\alpha_1} \cdots r_t^{\alpha_t}$ amb $\alpha_j \in \{0, 1, \ldots, m-1\}$ són tots distints, i així, $|C| \geq m^t$. □

3.4 Extensió universal infinita

En els apartats anteriors, donat un grup finit A-generat $G = F/R$ amb F un grup lliure sobre A (A finit), hem estudiat les seues extensions universals $G_m^\sharp = F/(R'R^m)$ per a qualsevol m natural i la seua interpretació en termes de grafs. Per això, tot seguit estudiarem què ocorre si considerem l'extensió natural $G^* = F/R'$.

Teorema 3.8. *Donats un conjunt finit A i un grup finit A-generat G, aleshores existeixen un grup A-generat G^* i un epimorfisme $\varphi\colon G^* \longrightarrow G$ que manté generadors el nucli del qual és un grup G_0^* abelià amb la següent propietat universal:*

Si H és un grup A-generat i $\psi\colon H \longrightarrow G$ és un epimorfisme que manté generadors el nucli del qual és un grup K abelià, aleshores existeix un epimorfisme $\beta\colon G^\sharp \longrightarrow H$ tal que $\beta\psi = \varphi$.

Demostració. Com G és A-generat, podem considerar l'epimorfisme $\varphi_G\colon F \longrightarrow G$, on F és el grup lliure amb base A. Aleshores, denotant $R = \ker \varphi_G$, tenim que $G \cong F/R$.

Considerem $G^* = F/R'$ i notem que és un grup A-generat ja que

$$\begin{array}{rccc} \varphi_{G^*}\colon & F & \longrightarrow & G^* \\ & \omega & \mapsto & \omega R' \end{array}$$

és un epimorfisme del grup lliure F sobre A en G^*.

Aleshores, l'epimorfisme

$$\begin{array}{rccc} \varphi\colon & G^* = F/R' & \longrightarrow & G = F/R \\ & \omega R' & \mapsto & \omega R \end{array}$$

manté generadors i té com a nucli $G_0^* = R/R'$, que és abelià: donats r_1 i r_2 en R,

$$(r_1R')(r_2R') = r_1r_2R' = r_1r_2[r_2, r_1]R' = r_2r_1R' = (r_2R')(r_1R').$$

Vegem ara que es verifica la propietat universal: siga H un grup A-generat amb epimorfisme associat $\varphi_H\colon F \longrightarrow H$ i siga $\psi\colon H \longrightarrow G$ un epimorfisme que manté generadors ($\varphi_H\psi = \varphi_G$) i tal que el seu nucli és un grup abelià K.

Si prenem $\omega \in R$, $\omega\varphi_H\psi = \omega\varphi_G = 1$ i per tant, $\omega\varphi_H \in K$. Aleshores, si $\omega_1, \omega_2 \in R$, com K és abelià,

$$([\omega_1, \omega_2])\varphi_H = (\omega_1\varphi_H)^{-1}(\omega_2\varphi_H)^{-1}(\omega_1\varphi_H)(\omega_2\varphi_H) = 1.$$

Per tant, si $\omega \in R'$, existeixen $\omega_1, \omega_2 \in R$ amb $\omega = [\omega_1, \omega_2]$ i, pel que acabem de veure, $\omega\varphi_H = 1$. Així, H satisfà les relacions de G^* i llavors, pel teorema de von Dyck, existeix un epimorfisme $\beta\colon G^* \longrightarrow H$ que manté generadors tal que $\beta\psi = \varphi$. □

A continuació, anem a tractar de construir l'extensió G^* emprant el graf de Cayley de G. Com en els casos anteriors, utilitzarem el graf de Cayley per obtindre un grup amb les propietats desitjades i seguidament provarem que hi ha un isomorfisme entre aquest grup i el grup G^* del teorema anterior.

Considerem el graf de Cayley de G amb respecte a A i en particular ens fixarem en el conjunt d'arestes d'aquest, que anomenarem E. A continuació, prenem el grup abelià lliure $W = \bigoplus_{e\in E} W_e$ amb base E, és a dir, si $x \in W$ aleshores existeixen uns únics $m_e \in \mathbb{Z}$ tals que $x = \sum_{e\in E} m_e e$.

Llavors, podem extendre l'acció per l'esquerra de G sobre el conjunt E donada per $g \cdot (h \xrightarrow{a} ha) = gh \xrightarrow{a} gha$ a una acció de G sobre W fent simplement $g \cdot x = \sum_{e\in E} m_e g \cdot e$. Així, de manera anàloga als casos anteriors, podem construir el producte semidirecte de W amb G, $T = [W]G$, i considerar el subgrup

$$H = \langle (1 \xrightarrow{a} a, a) \mid a \in A \rangle.$$

Aleshores, la interpretació del grup H és la següent: donada una paraula $\omega \in \tilde{A}^*$,

$$[\omega]_H = \left(\sum_{e\in E} \omega(e)e, [\omega]_G \right),$$

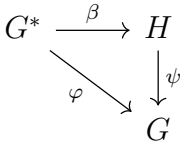
on $\omega(e)$ denota el nombre de vegades (amb signe) que l'aresta e és creuada pel camí del graf de Cayley de G etiquetat per ω.

Teorema 3.9. *El grup H és isomorf al grup G^* del teorema 3.8.*

Demostració. Comencem prenent el grup $U = H \cap W$. Com W és abelià, tenim que U és un subgrup normal abelià de H. A més, pel segon teorema d'isomorfia, també tenim que

$$\frac{H}{U} = \frac{H}{H \cap W} \cong \frac{HW}{W} = \frac{T}{W} \cong G.$$

Aleshores, si $\psi\colon H \longrightarrow G$ és l'epimorfisme amb nucli U, per la universalitat provada al teorema 3.8, existeix un epimorfisme $\beta\colon G^* \longrightarrow H$ que manté generadors i tal que $\beta\psi = \varphi$.



Recordem que φ és l'epimorfisme de G^* en G que manté generadors i té com a nucli $G_0^* = R/R'$. Notem que com F és lliure, pel teorema de Nielsen–Schreier, R també ho és i pel lema 1.32, tenim que R/R' és abelià lliure amb base $B_\sharp = \{xR' \mid x \in B\}$. A més, $G_0^* = R/R'$ és també finitament generat ja que $|B_\sharp| \leq |B|$ i sabem que $|B|$ és finit perquè com $|F : R| = |G|$ és finit podem aplicar la segona part del teorema de Nielsen–Schreier.

Anomenem $N = \ker \beta$. Si veiem que $N = 1$, β serà un isomorfisme i ja ho tindrem. Notem que si $x \in N$, aleshores $x\varphi = x\beta\psi = 1\psi = 1$ i, per tant, tenim que $x \in \ker \varphi = G_0^*$. Així, $N \trianglelefteq G_0^*$ i com G_0^* és abelià lliure de rang finit (diguem-ne n), pel teorema 1.17, existeixen una base $\{a_1, \ldots, a_n\}$ de G_0^* i enters positius $d_1, \ldots, d_k$ amb $1 \leq k \leq n$ i $d_1 \mid \cdots \mid d_k$ de manera que

$$G_0^* = \sum_{i=1}^{n} \langle a_i \rangle \quad \text{i} \quad N = \sum_{i=1}^{k} \langle d_i a_i \rangle.$$

En particular, $G_0^*/N \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^{n-k}$.

D'altra banda, pel lema 3.4, tenim que

$$\frac{G_0^*}{N} = \frac{\ker \varphi}{\ker \beta} \cong \ker \psi = U.$$

Però U, per ser subgrup de W, és un grup abelià lliure finitament generat (diguem-ne de rang r) i llavors té una descomposició $U \cong \mathbb{Z}^r$. Aleshores, pel corol·lari 1.27, $r = n - k$ i $d_i = 0$ per a cada $i = 1, \ldots, k$. Per tant, $N = 1$, com volíem. □

Bibliografia

[1] A. Ballester-Bolinches, E. Cosme-Llópez i R. Esteban-Romero. Group extensions and graphs. *Expo. Math.*, 34(3), 2016.

[2] K. Doerk i T. Hawkes. *Finite Soluble Groups*, volum 4 de *De Gruyter Expositions in Mathematics*. Walter de Gruyter, Berlin, New York, 1992.

[3] W. Gaschütz. Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden. *Math. Z.*, 60:274–286, 1954.

[4] T. W. Hungerford. *Algebra*, volum 73 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reimpressió de l'original de 1974.

[5] D.J.S. Robinson. *A course in the theory of groups*. Springer-Verlag, New York, 1996.

[6] J. J. Rotman. *An introduction to the theory of groups*, volum 119 de *Graduate Texts in Mathematics*. Springer, New York, 1995.

[7] J. Stallings. Topology of finite graphs. *Invent. Math.*, 71(3):551–565, 1983.

[8] B. Steinberg. Finite state automata: a geometric approach. *Trans. Amer. Math. Soc.*, 353:3409–3464, 2001.