Propiedades residuales y problemas de decisión en grupos

Jesús Rafael Palacio Alsina

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Conchita Martínez Pérez
Julio de 2016

Abstract

The aim of this dissertation is to introduce the classical decision problems in groups focusing on the word problem for polycyclic groups. We give two different solutions to that problem, the first and more theoretical one is using the fact that polycyclic groups are residually finite and the second, more practical, consist of creating an algorithm that tell us if a word is or is not the identity in the group.

First of all, we give the definition of free group and word:

Definition. Let F be a group, X a nonempty set and $\sigma : X \to F$ a function. Then F, or more exactly (F, σ) is said to be free on X if to each function α from X to a group G there corresponds a unique homomorphism $\beta : F \to G$ such that $\alpha = \sigma\beta$.

Definition. Let X be a set. We denote by $X^{-1} = \{x^{-1} | x \in X\}$ where of course x^{-1} is merely a symbol. By a word in X is meant a finite sequence of symbols from $X \cup X^{-1}$, written for convenience in the form

$$w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} \quad x_i \in X,\ \varepsilon_i = \pm 1,\ r \geq 0\ .$$

The next result is to detect whether a given group is free.

Proposition. *Let G be a group and X a subset of G. Assume that each element g of G can be uniquely written in the form $g = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s}$ where $x_i \in X$, $s \geq 0$, $l_i \neq 0$, and $x_i \neq x_{i+1}$. Then G is free on X.*

Proposition. *Let G be a group generated by a subset X and let F be a free group on a set Y. If $\alpha : Y \to X$ is a surjection, it extends to an epimorphism from F to G. In particular every group is an image of a free group.*

Now we have the tools to give a formal definition of a group presentation.

Definition. Let G be a group and π an epimorphism from a free group F to G. Thus if $R = \ker \pi$, we have $R \triangleleft F$ and $F/R \simeq G$. The elements of R are called the relators of the presentation.

Definition. A free presentation of a group G is an expression

$$G = \langle Y | S \rangle$$

where Y is a free generator set of G and S is a generator set of the subgroup of relators

Definition. A group is said to be finitely presented if it has a finite presentation $\langle X|R \rangle$, that is, one in which X and R are finite.

At this point we are ready to prove von Dyck theorem.

Theorem. *(von Dyck's Theorem). Let G and H be groups with presentations $\varepsilon : F \to G$ and $\delta : F \to H$ such that each relator of ε is also a relator of δ. Then the function $f^{\varepsilon} \mapsto f^{\delta}$ is a well-defined epimorphism from G to H.*

We can also prove two important properties about finitely presented groups.

Theorem. *(B.H. Neumann). If X is any set of generators of a finitely presented group G, the group has a finite presentation of the form $\langle X_0 | r_1 = r_2 = \cdots = t_t = 1 \rangle$ where $X_0 \subseteq X$.*

Theorem. *Let $N \triangleleft G$ and suppose that N and G/N are finitely presented groups. Then G is finitely presented.*

The proof of this last theorem will be very useful in the last section of this dissertation.
The three classical decision problems in group theory are.

- *The word problem*. Is there an algorithm which, when given a word w in the generators of a group G, decides if $w = 1$ in G?
- *The conjugacy problem*. Is there an algorithm to decide if two given words w_1, w_2 in the generators of a group G are conjugate?
- *The isomorphism problem*. Is there an algorithm which can decide if two given groups are isomorphic?

Definition. A group G is residually finite if given $g \neq 1$ in G, there is an $N \triangleleft G$ such that $g \notin N$ and G/N is finite.

We show that finitely presented residually finite groups have soluble word problem. As an example of residually finite groups we consider finitely generated abelian groups and also finitely generated linear groups (but we do not give a proof in this last case).

Definition. A group G is conjugacy separable if two elements are conjugate in G whenever their images in every finite quotient of G are conjugate.

We show that finitely presented conjugacy separable groups has soluble conjugacy problem. We also exhibit an example of finitely presented soluble groups with unsolvable word problem.

The main goal is to prove that polycyclic groups are residually finite. To do it begin by introducing some concepts about group series. The first is Zassenhaus Lema.

Lemma. *Let A_1, A_2, B_1, B_2 be subgroups of a group G such that $A_1 \triangleleft A_2$ and $B_1 \triangleleft B_2$. Let $D_{ij} = A_i \cap B_j$. Them $A_1D_{21} \triangleleft A_1D_{22}$ and $B_1D_{12} \triangleleft B_1D_{22}$. Furthermore the groups A_1D_{22}/A_1D_{21} and B_1D_{22}/B_1D_{12} are isomorphic.*

And the second is Schreier Refinement Theorem.

Theorem. *Any two series of a group possess isomorphic refinements.*

After that, we prove that subgroups and quotients of polycyclic groups are polycyclic too.

We prove that in a polycyclic group G the number of infinite factors in a cyclic series is independent of the series and hence is an invariant of G which is known as the Hirsch length. Also we define the notion of poly-infinite cyclic groups as groups with a series with infinite cyclic factors.

Some important notions are commutators and derived series.

Definition. Let G be a group, x_1, $x_2 \in G$ and X_1, X_2 nonempty sets of G. It is said that $[x_1,x_2] = x_1^{-1}x_2^{-1}x_1x_2$ is the *commutator* of x_1 and x_2. And it is said that $[X_1,X_2] = \langle [x_1,x_2] | x_1 \in X_1,\ x_2 \in X_2 \rangle$ is the *commutator subgroup* of X_1 and X_2. Finally it is said that $G' = [G,G]$ is the derived group of G.

We prove that for every group G, G/G' is abelian and define the derived series of a group.

Definition. Let be G a group then $G = G^{(0)} \geq G^{(1)} \geq \cdots$ where $G^{(n+1)} = (G^{(n)})'$ is called the derived series of G. The length of this series is the derived lenght of G.

Some easy properties are:

Proposition. *Let L and G be groups. If $L \triangleleft G$, then $L' \triangleleft G$.*

Proposition. *Let G be a soluble group with derived length d. Then the derived length of $G/G^{(d-1)}$ is $d-1$.*

We also give some important properties of finitely generated and polycyclic groups.

Proposition. *Let H be a subgroup of finite index in a finitely generated group G. Then H is finitely generated.*

Proposition. *A finitely generated abelian group G is finite if and only if it is a torsion group.*

Proposition. *A finitely generated soluble torsion group is finite.*

Proposition. *(i) Every polycyclic group has a normal poly-infinite cyclic subgroup of finite index.*
(ii) An infinite polycyclic group contains a nontrivial torsion-free abelian normal subgroup.

These results are used to prove our main theorem.

Theorem. *A polycyclic group is residually finite.*

Now we illustrate these theoretical results with some examples as the discrete Heisenberg group and Baumslag-Solitar groups. The discrete Heisenberg group is the unitriangular matrix group with $n = 3$ and integer entries. It is denoted by $UT(3,\mathbb{Z})$. We prove that this group G is polycyclic.

After that, we describe its derived series, showing that $G' = \langle z \rangle$ and $G^{(2)} = 1$ where z is the matrix with all entries zero except in the main diagonal and in the upper right corner where there are ones. We give the following presentation of G:

$$G = \langle x, y, z \mid [x,y] = z,\ [x,z] = [y,z] = 1 \rangle.$$

We know that G is residually finite because it is polycyclic but we give a different proof for this particular case using the fact that $UT(3,\mathbb{Z}3^n)$ is normal in G for all $n \in \mathbb{N}$.

And finally we give an easy and useful algorithm to solve the problem word for the discrete Heisenberg group.

In the other example we considerer Baumslag-Solitar groups. The Baumslag-Solitar groups are examples of two-generator one-relator groups. They are given by the group presentation $\langle x, y | (x^p)^y = x^q \rangle$. For each integer p and q, the Baumslag-Solitar group is denoted by $BS(p,q)$. We prove that $BS(1,2)$ is residually finite but $BS(2,3)$ is not. But both groups have soluble word problem. We also state the following general result.

Theorem. *The group $BS(p,q)$ is residually finite if and only if $p = \pm 1$ or $q = \pm 1$ or $p = \pm q$.*

In the last section we give an algorithm to solve the word problem for arbitrary polycyclic groups. This algorithm uses the so called power-conjugate presentation that we describe next. Let $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G$ be the polycyclic series of G. For $1 \leq i \leq n$ we choose $g_i \in G_i$ such that $G_i = \langle g_i, G_{i-1} \rangle$. Then the sequence $(g_1, ..., g_n)$ is called a polycyclic generating sequence of G. Let I be the set of those $i \in \{1, ..., n\}$ with $r_i := |G_i : G_{i-1}|$ finite. Each element of G can be written uniquely as $g_1^{e_1} \cdots g_n^{e_n}$ with $e_i \in \mathbb{Z}$ for $1 \leq i \leq n$ and $0 \leq e_i < r_i$ for $i \in I$.

Each polycyclic generating sequence of G gives rise to a power-conjugate presentation for G with the relators

$$g_j^{g_i} = g_{i-1}^{e(i,j,i-1)} \cdots g_1^{e(i,j,1)} \text{ for } 1 \leq j < i \leq n,$$

$$g_j^{g_i^{-1}} = g_{i-1}^{f(i,j,i-1)} \cdots g_1^{f(i,j,1)} \text{ for } 1 \leq j < i \leq n,$$

$$g_i^{r_i} = g_{i-1}^{l(i,i-1)} \cdots g_1^{l(i,1)} \text{ for } i \in I.$$

To finish, we give an example of this presentation for the unitriangular integer matrix group of dimension n, $UT(n,\mathbb{Z})$.

Índice general

Capítulo 1

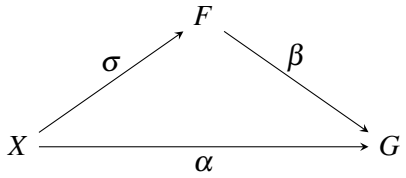
Grupos libres y presentaciones

En este capitulo se dará una breve introducción a los grupos libres y enunciaremos los problemas de decisión en la teoría de grupos, en especial el problema de la palabra.

La notación que usaremos será la usual en la teoría de grupos, es importante recordar los siguientes símbolos. A no ser que se diga lo contrario usaremos '1' para referirnos a la identidad del grupo. Con $K \leq G$ y $K < G$ nos referiremos a que un conjunto K es subgrupo del grupo G, con el primer símbolo consideraremos que K puede ser G mientras que en el segundo caso no. Y en el caso en el que K sea normal en G usaremos los símbolos $\trianglelefteq$ y $\triangleleft$. Por otra parte para denotar el subgrupo de un grupo G generado por una familia $X \subseteq G$ usaremos la notación $\langle X \rangle$. Añadir que $|G|$ denota el número de elementos que tiene el grupo G y para un subgrupo K de G usaremos $|G:K|$ para referirnos al índice de K sobre G, que es el número de coclases distintas $gK = \{gk | k \in K\}$. Finalmente dados dos elementos $x, y \in G$ la conjugación de x por y lo denotaremos con $x^y = y^{-1}xy$.

1.1 Grupos libres

Definición. Sea F un grupo, X un conjunto no vacío y $\sigma : X \to F$ una función. Diremos que F o de forma más rigurosa (F, σ) es *libre* sobre X si para cada función α de X a un grupo G le corresponde un único homomorfismo $\beta : F \to G$ tal que $\alpha = \sigma\beta$.



Un grupo que es libre sobre algún conjunto se dice que es un *grupo libre*.

Definición. Sea X un conjunto. Denotaremos por $X^{-1} = \{x^{-1} | x \in X\}$ donde x^{-1} es simplemente un símbolo. Nos referiremos por *palabra* a una secuencia finita de símbolos de $X \cup X^{-1}$. Lo escribiremos:

$$w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} \quad x_i \in X,\ \varepsilon_i = \pm 1,\ r \geq 0\ .$$

En el caso $r = 0$ la secuencia será nula y w será la palabra nula, la cual la escribiremos como 1.

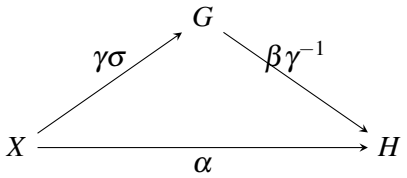
Definimos el producto de dos palabras como la yuxtaposición de las mismas, el inverso de una palabra w como $w^{-1} = x_r^{-\varepsilon_r} \cdots x_1^{-\varepsilon_1}$ y decimos que dos secuencias de símbolos de $X \cup X^{-1}$ son la misma palabra si se puede pasar de una a otra realizando las siguientes operaciones tantas veces sea necesario:

- Añadiendo xx^{-1} ó $x^{-1}x$ con $x \in X$.
- Sustrayendo xx^{-1} ó $x^{-1}x$ con $x \in X$.

Entonces se puede probar que el conjunto de todas las palabras de X forman un grupo que además es libre sobre X (ver [9, 2.1.1]). Tenemos así que para todo conjunto X existe un grupo libre sobre él.

Proposición 1.1. *Sea F un grupo libre sobre X y G un grupo isomorfo a F. Entonces, G también es libre sobre X.*

Demostración. Sea H un grupo, como F es libre sobre X, para cada función α de X en H existirá un único homomorfismo β de F en H. Luego llamando γ al isomorfismo de F en G, siendo σ la función de X en F, bastará tomar ahora:



viendo así que G es libre sobre X. □

Proposición 1.2. *Sea G un grupo y X un subconjunto de G. Asumamos que cada elemento g de G puede ser escrito de forma única como $g = x_1^{l_1}x_2^{l_2}\cdots x_s^{l_s}$ donde $x_i \in X$, $s \geq 0$, $l_i \neq 0$ y $x_i \neq x_{i+1}$. Entonces G es libre sobre X.*

Demostración. Sea F un grupo libre sobre el conjunto X con función asociada $\sigma : X \to F$. Por definición existe un homomorfismo $\beta : F \to G$ tal que $\sigma\beta : X \to G$ es la aplicación inclusión. Por hipótesis β es sobreyectiva y es inyectiva por la unicidad de la expresión anterior. Por lo que G es isomorfo a F, y como F es libre, lo será G. □

Ejemplo 1. Consideramos las funciones $x^\alpha = x+2$ y $x^\beta = \frac{x}{2x+1}$ sobre $\mathbb{C}_\infty$. Como α y β son biyecciones debido a que tienen inversos: $x^{\alpha^{-1}} = x-2$ y $x^{\beta^{-1}} = \frac{x}{1-2x}$, entonces α y β generan un grupo de permutaciones F de $\mathbb{C}_\infty$. Este grupo es libre sobre el conjunto $\{\alpha,\beta\}$. Para verlo se puede razonar así: Al aplicarle a un z que se encuentre en el interior del círculo unidad una potencia no nula de α el resultado estará en el exterior y si a un w que se encuentre en el exterior del círculo le aplicamos una potencia no nula de β el resultado estará en el interior sin el 0, a partir de esto se puede probar que ninguna palabra puede ser reducida a 1 salvo la trivial teniendo así que todo elemento de F se puede escribir de forma única en términos de α y β. Esto significa que se cumplen las hipótesis de (1.2) y F es libre en $\{\alpha,\beta\}$.

Definición. Un *grupo lineal* G es un grupo isomorfo a un subgrupo de $GL(n,\mathbb{F})$ con $\mathbb{F}$ anillo abeliano y n un entero positivo.

Ejemplo 2. Consideremos las matrices $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. Usando un argumento similar al del ejemplo anterior se prueba que el grupo $F_2 = \langle A,B\rangle$ es libre sobre el conjunto $\{A,B\}$ además $F_2 \leq GL(2,\mathbb{Z})$ por lo que es un grupo lineal. Y se puede probar que F_2 contiene a todos los grupos libres finitamente generados, luego todo grupo libre finitamente generado es lineal.

Proposición 1.3. *Sea G un grupo generado por un conjunto X y sea F un grupo libre sobre un conjunto Y. Si $\alpha : Y \to X$ es sobreyectiva, existe un epimorfismo de F en G. En particular todo grupo es cociente de un grupo libre.*

Demostración. Como F es libre sobre Y, de la función α se puede extender un homomorfismo, que lo llamaremos igual por simplicidad, $\alpha : F \to G$. Debido a que X genera G, los elementos de G serán de la forma, $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_k^{\varepsilon_k}$ donde $x_i \in X$, $\varepsilon_i = \pm 1$ y $k \geq 0$. Para todo $x_i \in X$ $\exists y_i \in Y$ tal que $y_i^\alpha = x_i$, luego dado un elemento de G $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_k^{\varepsilon_k}$ existen $y_1, y_2, ..., y_k$ tal que $y_1^\alpha = x_1$, $y_2^\alpha = x_2$,..., $y_k^\alpha = x_k$, por lo que

$$(y_1^{\varepsilon_1}y_2^{\varepsilon_2}\cdots y_k^{\varepsilon_k})^\alpha = (y_1^\alpha)^{\varepsilon_1}(y_2^\alpha)^{\varepsilon_2}\cdots(y_k^\alpha)^{\varepsilon_k} = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_k^{\varepsilon_k}$$

siendo así α un epimorfismo. □

1.2 Presentaciones de grupos

Hemos visto en la proposición anterior que todo grupo es cociente de un grupo libre, luego podríamos pensar en describir cualquier grupo como un cociente.

Sea un epimorfismo π de un grupo libre F en G. Llamando R al núcleo de π tenemos que $R \lhd F$ y $F/R \simeq G$. A los elementos de R los llamaremos *relaciones*.

Elegimos ahora un conjunto de generadores libres de F, llamémosle Y, y un subconjunto S de F tal que $\ker\pi = S^F$ [1]. Si $X = Y^\pi$ entonces se tiene que X genera G. Por otra parte $r \in F$ es una relación si y solo si puede escribirse de la forma $\left(s_1^{\varepsilon_1}\right)^{f_1} \cdots \left(s_k^{\varepsilon_k}\right)^{f_k}$ donde $s_i \in S$, $\varepsilon_i \pm 1$, $f_i \in F$. La presentación π junto a la elección de Y y S determina un conjunto de generadores y de relaciones para G.

Definición. Llamaremos *presentación* de un grupo G a

$$G = \langle Y|S\rangle\,.$$

Vemos que la presentación de G se basa en la elección de Y y principalmente en la de π por lo que también se conoce como *presentación libre* de G al epimorfismo π.

En la práctica es más conveniente dar las relaciones como $s = 1,\ s \in S$ y siendo G generado por X, obtenemos

$$G = \langle X|s = 1,\ s \in S\rangle\,.$$

Nos referiremos a esta expresión como la presentación de G.

Ejemplo 3. Uno de los ejemplos más sencillo lo tenemos para los grupos cíclicos como por ejemplo, $G = \langle x|x^6 = 1\rangle$, el grupo cíclico de 6 elementos. Tenemos $X = \{x\}$, el grupo libre $F = \langle X\rangle = \langle x\rangle = \left\{1, \bar{x}, \bar{x}^{-1}, \bar{x}^2, \bar{x}^{-2}, ...\right\}$ y $\sigma : x \in X \mapsto \bar{x} \in F$. La función $\pi : \bar{x}^i \in F \to x^{\gamma(i)} \in G$ dada por $\gamma(i) = i$ modulo(6) claramente es un epimorfismo y se tiene $\ker\pi = \langle x^6\rangle$.

Ejemplo 4. $G = \langle x, y|x^2 = 1, y^2 = 1\rangle$. Este grupo se llama grupo diédrico infinito, se denota por D_∞. Veamos otra presentación de este grupo. Llamando $a = xy$ obtenemos que $G = \langle x, a|x^2 = 1, x^{-1}ax = a^{-1}\rangle$ realizando cálculos vemos que $x^{-1}ax = x^{-1}xyx = yx = a^{-1}$ pues $a(yx) = xyyx = xy^2x = xx = x^2 = 1$ y recíprocamente $y^2 = (x^{-1}a)^2 = x^{-1}axa = a^{-1}a = 1$. Utilizando las llamadas *transformaciones de Tietze* (ver [6, 2. Finite presentations]) se deduce que son presentaciones del mismo grupo.

Teorema 1.4. *(von Dyck). Sean G y H dos grupos con presentaciones $\varepsilon : F \to G$ y $\delta : F \to H$ tal que cada relación en ε es también una relación en δ, esto es,* $\ker\varepsilon \leq \ker\delta$. *Entonces la función $f^\varepsilon \mapsto f^\delta$ es un epimorfismo bien definido de G en H.*

Demostración. Por la definición de presentación se tiene que ε y δ son epimorfismos, luego dados $g \in G$ y $h \in H$ existirán $f_1,\ f \in F$ tal que $g = f_1^\varepsilon$ y $h = f^\delta$. Además la aplicación $f^\varepsilon \mapsto f^\delta$ está bien definida debido a que si $g = f_1^\varepsilon$ y $g = f^\varepsilon$ entonces por fuerza $f = f_1 k$ con $k \in \ker\varepsilon$ y como $\ker\varepsilon \leq \ker\delta$ tenemos que $k \in \ker\delta$ por lo que $f^\delta = f_1^\delta$. Y obviamente $f^\varepsilon \mapsto f^\delta$ es un epimorfismo. □

Definición. Un grupo se dice que es *finitamente presentado* si tiene una presentación finita $\langle X|S\rangle$, es decir, existe una presentación en la que X y S son finitos.

Teorema 1.5. *(B.H. Neumann) Si X es un conjunto generador de un grupo G finitamente presentado, el grupo tendrá una presentación finita de la forma $\langle X_0|r_1 = r_2 = \cdots = t_t = 1\rangle$ donde $X_0 \subseteq X$.*

Demostración. Sea $G = \langle y_1, ..., y_m|s_1 = \cdots = s_l = 1\rangle$ una presentación finita de G. Como X genera G, existirá un subconjunto finito $X_0 = \{x_1, ..., x_n\} \subseteq X$ donde cada x_i se podrá expresar en función de los y_i de tal forma que X_0 también generará G y hay, por lo tanto, expresiones para los y_i en función de los x_j y viceversa. Llamemos $y_i = w_i(x)$ y $x_j = v_j(y)$. Las relaciones en términos de los x_j's serán:

$$s_k(w_1(x), ..., w_m(x)) = 1 \quad k = 1, ..., l.$$

[1] $S^F = \langle f^{-1}Sf|f \in F\rangle$ es el subgrupo normal a F más pequeño que contiene a S

Habrá un número finito de estas relaciones.

Sea $\overline{G}$ un grupo con generadores $\bar{x}_1,...,\bar{x}_n$ y las relaciones descritas arriba para los $\bar{x}_1,...,\bar{x}_n$. Por (1.4) existe un epimorfismo de $\overline{G}$ en G en el que $\bar{x}_i \mapsto x_i$. Definimos ahora $\bar{y}_i = w_i(\bar{x})$. Partiendo de que $\bar{x}_j = v_j(w_1(\bar{x}),...,w_m(\bar{x}))\ j = 1,...n$. Se deduce que $\overline{G} = \langle \bar{y}_1,...,\bar{y}_m \rangle$. Debido a que $s_k(\bar{y}) = 1$ hay, de nuevo por (1.4), un epimorfismo de G en $\overline{G}$ en el cual $y_i \mapsto \bar{y}_i$. Estos epimorfismos son mutuamente inversos, luego son isomorfismos, por lo que G está generado por $x_1,...,x_n$ y tiene las relaciones de las x_i descritas antes. □

Un ejemplo de grupos finitamente presentados son los grupos cíclicos.

Teorema 1.6. *(P. Hall). Sea $N \triangleleft G$ si N y G/N son grupos finitamente presentados, entonces G es finitamente presentado.*

Demostración. Supongamos que N tiene una presentación con generadores $x_1,...,x_m$ y relaciones $r_1 = \cdots = r_k = 1$ y que G/N tiene una presentación con generadores $y_1N,...,y_nN$ y relaciones $s_1 = \cdots = s_l = 1_{G/N}$. Entonces, G está generado por $x_1,...,x_m,y_1,...,y_n$. Además cumplen las siguientes relaciones: $r_i(x) = 1,\ (i = 1,..,k)$ que son las que ya había en N, las relaciones que había en G/N son $s_j(y)N = N$ lo que nos dice que $s_j(y) \in N$ por lo que estas relaciones se podrán poner en función de los generadores de N:

$$s_j(y) = t_j(x)\ j = 1,...,l.$$

Y finalmente las relaciones de normalidad:

$$y_j^{-1}x_iy_j = u_{ij}(x) \quad y_jx_iy_j^{-1} = v_{ij}(x) \quad i = 1,...,m,\ \ j = 1,...,n.$$

Sea $\overline{G}$ un grupo con generadores $\bar{x}_1,...,\bar{x}_m,\bar{y}_1,...,\bar{y}_n$ y con las relaciones definidas arriba en términos de los $\bar{x}_i$ y $\bar{y}_j$. Por (1.4) hay un epimorfismo $\alpha : \overline{G} \to G$ tal que $\bar{x}_i^{\alpha} = x_i$ y $\bar{y}_j^{\alpha} = y_j$. Sea $K = \ker\alpha$. La restricción de α a $\overline{N} \equiv \langle \bar{x}_1,...,\bar{x}_m \rangle$ es un isomorfismo, en efecto, todas las relaciones en los x_j son relaciones en los $\bar{x}_j$ y de nuevo por (1.4) existe un epimorfismo de N en $\overline{N}$ en el que $x_i \mapsto \bar{x}_i$ siendo esta la aplicación inversa a la restricción de α en N. Por lo tanto $K \cap \overline{N} = 1$. Por otra parte $\overline{N} \triangleleft \overline{G}$ porque $\bar{y}_j^{-1}\bar{x}_i\bar{y}_j$ y $\bar{y}_j\bar{x}_i\bar{y}_j^{-1}$ pertenecen a $\overline{N}$ debido a que cumplen las relaciones de normalidad descritas arriba. Luego α induce un epimorfismo de $\overline{G}/\overline{N}$ en G/N en el que $\bar{y}_i\overline{N} \mapsto y_iN$ que es un isomorfismo debido a que todas las relaciones en los y_iN son también relaciones en los $\bar{y}_i\overline{N}$. □

Ejemplo 5. Retomemos el ejemplo 4 en el cual habíamos dado la siguiente presentación del grupo diédrico infinito: $G = \langle x,a | x^2 = 1, x^{-1}ax = a^{-1} \rangle$. Vamos a ver que este grupo también se puede expresar como el producto semidirecto de dos grupos, $G = X \ltimes N$ con el grupo cíclico infinito $N = \langle a \rangle$ y el grupo $X = \langle x \rangle$ cíclico de orden 2 y además x conjuga un elemento de N en su inverso, es decir, $x^{-1}ax = a^{-1}$. Para ello vamos a servirnos de la demostración del teorema (1.6). Tenemos que $N \triangleleft G$ y además N y $X = G/N$ son finitamente presentados con presentaciones:

$$N = \langle a | \ \rangle, \quad G/N = \langle xA | x^2A = A \rangle.$$

Entonces G estará generado por a, x y las relaciones serán las siguientes:

- $x^2 = a^n$ para algún $n \in \mathbb{N} \cup \{0\}$.
- $x^{-1}ax = a^l$ para algún $l \in \mathbb{N} \cup \{0\}$.
- $xax^{-1} = a^m$ para algún $m \in \mathbb{N} \cup \{0\}$.

Como x conjuga un elemento de N en su inverso entonces, $l = -1$ y $m = -1$ pues, $x^{-1}ax = a^{-1} \Leftrightarrow ax^{-1}ax = 1 \Leftrightarrow ax^{-1}a = x^{-1} \Leftrightarrow xax^{-1}a = 1 \Leftrightarrow xax^{-1} = a^{-1}$. Finalmente $x^{-1}a^nx = a^{-n}$ y $x^2 = a^n \Rightarrow a^{-n} = x^{-1}a^nx = x^{-1}x^2x = x^2$ teniendo así que $a^n = x^2 = a^{-n} \Rightarrow n = 0 \Rightarrow x^2 = 1$. Por tanto $G = \langle a,x | x^2 = 1, x^{-1}ax = a^{-1} \rangle$.

1.3 Problemas clásicos de decisión en grupos

En esta sección abordaremos los problemas clásicos de decisión en grupos, que fueron formulados por Max Dehn en 1911 [2, Über unendliche diskontinuierliche Gruppen]. En ellos se trata de saber si existe un algoritmo que nos demuestre si es verdad o no una determinada igualdad.

Suelen ser formulados para grupos finitamente presentados, ya que sin esta condición, la respuesta suele ser negativa pero también tienen sentido para grupos finitamente generados.

1.3.1 El problema de la palabra

Sea G un grupo finitamente presentado con generadores $x_1,...,x_n$ y relaciones $r_1,...,r_k$. El problema de la palabra se dice que es resoluble para la presentación dad si existe un algoritmo para determinar si una palabra w en términos de los x_i es o no es una relación, es decir, si $w=1$ en G. Se puede comprobar utilizando un razonamiento análogo al de la demostración de (1.5) que la respuesta a nuestro problema no depende de la presentación dada, sino del propio grupo G.

Un primer intento para resolver el problema de la palabra sería enumerar todas las consecuencias de nuestras relaciones $r_1,...,r_k$, es decir, todas las palabras de la forma $(r_{i_1}^{\pm 1})^{f_1}\cdots(r_{i_j}^{\pm 1})^{f_j}$, $(f_i \in F)$. De tal forma, si w es una relación, aparecerá en nuestra lista, y dado suficiente tiempo, la detectaremos. El verdadero problema viene cuando w no es una relación, esta no aparecerá en la lista y no podrá ser encontrada. Por lo que necesitaremos también una forma de enumerar las palabras que no son relaciones.

Tras este análisis no es de extrañar que haya grupos finitamente presentados que tienen un problema de la palabra irresoluble, que es justo lo que se demuestra en el famoso teorema de Novikov-Boone-Britton [10, Theorem 12.8]. Pero a pesar de esto el problema de la palabra tiene solución para muchas clases de grupos finitamente presentados. Veremos alguno.

Definición. Un grupo G se dice que es *residualmente finito* si dado $1 \neq g \in G$, existe $N \triangleleft G$ tal que $g \notin N$ y G/N es finito.

Proposición 1.7. *Los subgrupos de los grupos residualmente finitos también son residualmente finitos.*

Demostración. Sea K un grupo residualmente finito y H un subgrupo de este. Sea $1 \neq h \in H$ entonces $h \in K$. Luego por hipótesis existe $N \triangleleft K$ de índice finito en K tal que $h \notin N$ y en particular $H \cap N \triangleleft H$ y $h \notin H \cap N$. Como veremos en (2.4) $NH \leq K$. De tal forma que aplicando el segundo teorema de isomorfía tenemos que

$$\frac{H}{N \cap H} \simeq \frac{NH}{N} \leq \frac{K}{N}.$$

Tenemos así que $H/(N \cap H)$ es finito. □

Proposición 1.8. *Los grupos abelianos finitamente generados son residualmente finitos.*

Demostración. Como vamos a tratar con grupos abelianos usaremos la notación aditiva donde el 0 es la identidad. El teorema fundamental para grupos abelianos finitamente generados nos dice que sea tal grupo G existirán únicos $r,m \in \mathbb{N} \cup \{0\}$ y $n_1,...,n_r \in \mathbb{N}$, donde $n_1 | n_2 | \cdots | n_r$, tal que

$$G \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r} \oplus \mathbb{Z}^m.$$

Sea $0 \neq g \in G$ podremos escribirlo como $g = t + \alpha_1 t_1 + \cdots + \alpha_m t_m$ donde $t \in \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \mathbb{Z}_{n_r} \equiv T$, $t_1,...,t_m$ son los generadores de cada copia de $\mathbb{Z}$ y $\alpha_1,...,\alpha_n \in \mathbb{Z}$. Podemos suponer que $t = 0$ pues en caso contrario, $g \notin \mathbb{Z}^m$ y $G/\mathbb{Z}^m$ es finito. Sin pérdida de generalidad podemos suponer $\alpha_1 \neq 0$. Tomamos un p primo que no divida a α_1. Entonces $g \notin p\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus T$ y $G/(p\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus T)$ es finito (tiene orden p). □

Teorema 1.9. *(Mal'cev) Los grupos lineales finitamente generados son residualmente finitos.*

Demostración. Podemos encontrarla en [12]. □

Corolario 1.10. *El grupo $GL(n,\mathbb{Z})$ es residualmente finito para todo n entero positivo.*

Demostración. Se sigue de (1.9) por ser $\mathbb{Z}$ finitamente generado. □

Proposición 1.11. *Los grupos libres finitamente generados son residualmente finitos.*

Demostración. En el ejemplo (2) hemos visto que el grupo libre generado por dos elementos F_2 es un subgrupo de $GL(2,\mathbb{Z})$ el cual acabamos de decir que es residualmente finito. Luego por (1.7) F_2 es residualmente finito. Y como todos los grupos libres finitamente generados son subgrupo de F_2, los grupos libres finitamente generados son residualmente finitos. □

Observación 1.12. Los cocientes de grupos residualmente finitos no tienen porque ser residualmente finitos. En efecto, por (1.3) sabemos que todo grupo es cociente de un grupo libre, luego si lo fueran, tendríamos que los grupos finitamente generados son residualmente finitos, lo cual es falso.

Proposición 1.13. *Sea G un grupo residualmente finito y finitamente presentado. Entonces el problema de la palabra tiene solución para G.*

Demostración. Asumimos que G está dado por una presentación finita. Sea w una palabra en términos de los generadores de esta presentación. Vamos a describir dos procedimientos que una vez puestos en marcha, nos dirán si $w = 1$ o no.

El primer procedimiento consiste en enumerar todas las consecuencias de las relaciones dadas en la presentación e ir comprobando una a una si es igual a nuestra palabra w. Si resulta que hay alguna que sea igual a w, $w = 1$ en G y el procedimiento parará.

El segundo procedimiento consiste en enumerar todos los grupos finitos construyendo sus tablas de multiplicación. Para cada grupo finito F construimos todos los homomorfismos θ de G en F, para ello asignamos un elemento de F a cada generador de G y después comprobamos si las relaciones de la presentación se cumplen en F. Como F es finito, habrá finitos homomorfismos y se podrá hacer. Para cada homomorfismo θ calculamos w^θ y comprobamos si es igual a la identidad en F. Si resulta que $w^\theta \neq 1$ en F, entonces $w \neq 1$ en G y el procedimiento parará.

La clave reside en que si el grupo es residualmente finito, entonces uno de los dos procesos parará. En efecto, si $w \neq 1$ en G como G es residualmente finito, existirá $N \triangleleft G$ con $w \notin N$ y $F = G/N$ finito en el cual $w \neq 1$ y por lo tanto el segundo proceso parará. Por otra parte si $w = 1$ en G el primer proceso parará. □

Teorema 1.14. *Los grupos abelianos finitamente presentados tienen solución al problema de la palabra.*

Demostración. Se sigue de (1.13) y (1.8). □

En la práctica el algoritmo descrito en (1.13) no suele ser el más rápido, y como no podía ser de otra forma, para los grupos abelianos finitamente presentados hay otro algoritmo mucho más eficiente. Veámoslo. Sea A tal grupo con familia generadora minimal $\langle a_1,...,a_s,b_1,...,b_t\rangle$ siendo a_i los elementos generadores de orden finito. Por ser A abeliano, toda palabra w podrá ser reescrita de forma única como, $w = a_1^{\varepsilon_1}\cdots a_s^{\varepsilon_s}b_1^{\delta_1}\cdots b_t^{\delta_t}$ con $\varepsilon_1,...,\varepsilon_s,\delta_1,...,\delta_t \in \mathbb{N}\cup\{0\}$. Luego $w = 1$ si y solo si el orden de los a_i divide a ε_i para $i = 1,...,s$ y $\delta_i = 0$.

Esto también ocurre para los grupos policíclicos[2], lo veremos en el capitulo 4 después de demostrar en el capítulo 2 que son finitamente presentados y residualmente finitos.

Corolario 1.15. *Los grupos lineales finitamente generados y los grupos libres finitamente generados tienen solución al problema de la palabra.*

[2] Ver definición de *policíclico* en la pagina 9

1.3.2 El problema de la conjugación

Sea G un grupo finitamente presentado con generadores $x_1,...,x_n$ y relaciones $r_1,...,r_k$. El problema de la conjugación se dirá que es resoluble para G si existe un algoritmo, el cual, cuando se le introducen dos palabra w_1 y w_2 en términos de los x_i decide si son o no son conjugadas como elementos de G.

Observar que al igual que en el problema de la palabra, la respuesta a nuestro problema no depende de la presentación dada, sino del propio grupo G.

Observación 1.16. Todo grupo resoluble para el problema de la conjugación lo es para el de la palabra.

Definición. Diremos que un grupo G es separable para la conjugación si para todo par de elementos $g, h \in G$ no conjugados existe un subgrupo normal N de índice finito en G tal que las coclases de g y h en G/N no son conjugadas.

Observación 1.17. La propiedad de ser separable para la conjugación no se conserva para subgrupos. En efecto, sea $K < G$ donde G es separable para la conjugación. Sean $w_1, w_2 \in K$ no conjugados, no implica que w_1, w_2 no sean conjugados en G, luego no puedo usar que G es separable para la conjugación para ver que K lo es.

Proposición 1.18. *Todo grupo G separable para la conjugación es residualmente finito.*

Demostración. Sea $1 \neq w \in G$ entonces, 1 y w no serán conjugadas luego existe $N \triangleleft G$ con G/N finito donde $\nexists h \in G$ tal que $1N = h^{-1}whN$ de lo que se deduce $N \neq wN$ luego $w \notin N$. □

Proposición 1.19. *Sea G un grupo separable para la conjugación y finitamente presentado. Entonces el problema de la conjugación tiene solución para G.*

Demostración. Al igual que para el problema de la palabra vamos a dar dos algoritmos de manera que una vez puestos en marcha uno de ellos parará y nos dará el resultado.

En el primero, dadas las dos palabras w_1 y w_2 en términos de los generadores de la presentación, conjugaremos w_1 por los diferentes elementos distintos de la unidad de G, pues por (1.16) G tiene solución al problema de la palabra y por tanto sabemos que elementos son la unidad y cuales no. Tenemos así que si estas palabras son conjugadas este procedimiento parará.

Y el segundo consiste en construir todos los cocientes finitos. Para cada cociente finito F construimos los homomorfismos θ de G en F y comprobamos si w_1^θ y w_2^θ son conjugados, si encuentra uno en el que no sean conjugados, tenemos que w_1 es no es conjugado de w_2 y este procedimiento parará.

Por lo que dado el tempo necesario uno de los dos procedimientos parará. □

Teorema 1.20. *Los grupos policíclicos tienen solución al problema de la conjugación.*

Demostración. Ver [5, Corolary 9.1.2]. □

1.3.3 El problema del isomorfismo

Diremos que el problema del isomorfismo es resoluble en una clase de grupos si existe un algoritmo que decida si son isomorfos o no dos grupos de esa clase.

Este problema fue propuesto por primera vez para clases de grupos finitamente generados por Heinrich Franz Friedrich Tietze en 1908 e identificado por Dehn en 1911 como uno de los tres problemas fundamentales de la teoría de decisión de grupos. Sergei Ivanovich Adian y Michael Oser Rabin probaron 50 años después de su formulación la existencia de clases en las cuales el problema es irresoluble. Usando estos resultados, Markov en 1958 probó la irresubilidad del llamado problema fundamental de la topología: El problema del homeomorfismo, que consiste en decidir si existe un algoritmo que determine si dados dos poliedros son homeomorfos o no.

1.3.4 Resultados negativos para grupos resolubles finitamente presentados

Estos tres problemas de decisión para grupos finitamente presentados estuvieron sin solución durante años hasta la llegada del teorema de Boone-Novikov. Posteriormente fue demostrado por Olga Kharlampovich en 1981 que el problema de la palabra no tiene solución para determinados grupos resolubles finitamente presentados. Esto también fue probado de forma independiente por Baumslag, Gildenhuys y Strebel en 1985 y en ambos trabajos los autores usan resultados de M.Misnsky. En [1] se demuestra el siguiente teorema.

Teorema 1.21. *Existe un grupo resoluble finitamente presentado U de longitud derivada[3] tres y un conjunto de palabras $w_1, w_2, \ldots$ en términos de los generadores de U tal que $w_i^p = 1$ con p primo y w_i centrado en U, en el que no hay un algoritmo para decidir si dada una palabra w es o no es igual a la identidad en U.*

El grupo U tiene un subgrupo normal A tal que $\forall a \in A\ a^{p^2} = 1$ y el cociente U/A es abeliano libre de torsión[4].

Se sigue de forma directa por (1.16) que U también proporciona un ejemplo en el que el problema de la conjugación no tiene solución.

Por último añadir que el grupo U también puede ser usado para probar que el problema del isomorfismo no tiene solución en la clase de los grupos resolubles finitamente presentados de longitud derivada tres. Para ver esto tomamos un grupo cíclico $\langle x \rangle$ de orden p^3 y definimos los grupos G_i, con $i = 1, 2 \ldots$ como

$$G_i = \frac{U \times \langle x \rangle}{\left\langle x^{p^2} w_i^{-1} \right\rangle}$$

donde $w_1,\ w_2, \ldots$ es el conjunto de palabras anterior.

Veamos que $w_i = 1$ en G si y solo si G_i no tiene elementos de orden p^3. En efecto, supongamos que $w_i = 1$ y veamos que U no tiene elementos de orden p^3. Sea $b \in U$ tal que $b^{p^3} = 1$ tenemos que $b^{p^3} A = A$ y como U/A es libre de torsión entonces $bA = A$, luego, $b \in A$ y sabemos que $\forall a \in A\ a^{p^2} = 1$, por lo que $b^{p^2} = 1$. Luego b tiene orden p ó p^2. Ademas,

$$G_i = \frac{U \times \langle x \rangle}{\langle x^{p^2} \rangle} \simeq U \times \frac{\langle x \rangle}{\langle x^{p^2} \rangle} \simeq U \times \mathbb{Z}_{p^2}$$

luego los elementos de G_i no tendrán orden p^3. Reciprocamente, supongamos que $w_i \neq 1$. Ponemos que $T = \left\langle x^{p^2} w_i^{-1} \right\rangle$. Vamos a probar que xT tiene orden p^3. Obviamente $x^{p^3} T = T$ luego, el orden de $xT \in G$ puede ser $1,\ p,\ p^2,\ p^3$. Como queremos ver que xT tiene orden p^3 será suficiente ver que $x^{p^2} \notin T$, supongamos que $x^{p^2} \in T$, notemos que T está generado por el elemento $x^{p^2} w_i^{-1}$ que tiene orden p ya que $(w_i^{-1})^p = 1$. Entonces existirá un $0 \leq r < p$ tal que $x^{p^2} = (x^{p^2} w_i^{-1})^r = x^{rp^2} w_i^{-r}$ luego $w_i^r = x^{rp^2 - p^2}$ y como $w_i \neq 1$ tendrá que ser $r = 0$ luego $1 = x^{-p^2}$ lo que implica que $x^{p^2} = 1$ pero esto es imposible ya que x tiene orden p^3.

En el caso de que $w_i = 1$ tenemos que G_i es isomorfo a $G^* = U \times \mathbb{Z}_{p^2}$ y como no existe un algoritmo que nos diga si $w_i = 1$ tampoco existirá uno que nos diga si $G_i \simeq G^*$.

[3] Ver definición de *longitud derivada* en la página 13.

[4] Ver definición de *libre de torsión* en la página 14

Capítulo 2

Cadenas, descomposición de grupos y grupos policíclicos

El propósito de este capítulo será demostrar que los grupos policíclicos son finitamente presentados y residualmente finitos y por tanto resolubles para el problema de la palabra. Para ello daremos una serie de conceptos de descomposición de grupos y ciertas propiedades que poseen determinados grupos que nos serán útiles en la demostración final.

2.1 Cadenas de grupos

Definición. Diremos que un grupo G es *policíclico* (*resoluble*) si existe una cadena de subgrupos

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_i \triangleleft G_{i+1} \triangleleft \cdots \triangleleft G_n = G$$

donde cada G_{i+1}/G_i es cíclico (abeliano). Llamaremos *términos* de la cadena a los G_i y *factores* de la cadena a los G_{i+1}/G_i. Si todos los G_i son distintos, al entero n lo llamaremos *longitud de la serie*.

Proposición 2.1. *Los grupos policíclicos son finitamente presentados.*

Demostración. $1 = G_0$ es trivialmente finitamente presentado. Como $G_1/G_0 = G_1/1 = G_1$ es cíclico, será finitamente presentado y aplicando el teorema (1.6) obtenemos que G_1 es finitamente presentado, al realizar este razonamiento recursivamente, obtenemos que G es finitamente presentado. □

Teorema 2.2. *Todo grupo policíclico es isomorfo a un subgrupo de $GL(n,\mathbb{Z})$.*

Demostración. Ver [5, Sección 3.3]. □

Observación 2.3. Como $GL(n,\mathbb{Z})$ es finitamente generado, podemos deducir por (1.9) que los grupos policíclicos son residualmente finitos.

Definición. Sea G grupo con una cadena de subgrupos $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ que llamaremos **S**. Dada otra cadena **T** de G diremos que es un *refinamiento* de **S** si **T** contiene a todos los términos de la cadena **S**. Si hay un término en **T** que no esté en **S** diremos que es un *refinamiento propio*. Se dice que dos cadenas **S** y **T** de un grupo G son isomorfas si los factores de **S** y **T** son isomorfos.

En general si H y K son subgrupos de G, HK no tiene porque ser un subgrupo de G. Un sencillo ejemplo de ello es el grupo generado por las permutaciones de tres elementos, S_3, y los subgrupos $H = \{1,(1,2)\}$ y $K = \{1,(1,3)\}$. En este caso $HK = \{1,(1,2),(1,3),(1,2,3)\}$ que no es un subgrupo de S_3.

Lema 2.4. *Sean dos subgrupos H, K, de un grupo G. Si uno de ellos es normal en G, entonces $HK \leq G$. En tal caso $HK = KH$.*

Demostración. Supongamos que $H \triangleleft G$. Sean $h_1k_1,\ h_2k_2 \in HK$, veamos que su producto también está en HK. Por ser $H \triangleleft G$ y $K \subseteq G$, $k_1h_2k_1^{-1} \in H$. Luego $h_1k_1h_2k_2 = \underbrace{h_1\overbrace{k_1h_2k_1^{-1}}^{\in H}}_{\in H}\underbrace{k_1k_2}_{\in K} \in HK$. □

Lema 2.5. *Si $N \trianglelefteq G$ y $H \trianglelefteq K \leq G$, entonces $HN \trianglelefteq KN$.*

Demostración. Por (2.4) HN y KN serán subgrupos de G. Veamos que son normales. Sean $k_1 \in K$, $n_1, n_2 \in N$, y $h_1 \in H$. Hay que probar que $k_1n_1h_1n_2(k_1n_1)^{-1} \in HN$.

$$k_1n_1h_1n_2(k_1n_1)^{-1} = k_1n_1h_1n_2n_1^{-1}k_1^{-1} = \underbrace{k_1n_1k_1^{-1}}_{\in N}\underbrace{k_1h_1k_1^{-1}}_{\in H}\underbrace{k_1n_2n_1^{-1}k_1^{-1}}_{\in N}.$$

Y como por (2.4) $NH = HN$, tenemos que $k_1n_1h_1n_2(k_1n_1)^{-1} \in HN$. □

Lema 2.6. *Sean A, K y G grupos cumpliendo $A \triangleleft G$, $A \triangleleft K$ entonces $K/A \triangleleft G/A$ si y solo si $K \triangleleft G$ y en tal caso $(G/A)/(K/A) \simeq G/K$.*

Demostración. Para probar que $K \triangleleft G$ hay que ver que $g^{-1}kg \in K\ \ \forall k \in K,\ g \in G$. Sean $k \in K,\ g \in G$, por hipótesis sabemos que $g^{-1}kgA \in K/A$. Luego $g^{-1}kgA = k_1A$ para algún $k_1 \in A$, multiplicando por k_1^{-1} por la izquierda tenemos que $k_1^{-1}g^{-1}kg \in A$. Luego $k_1^{-1}g^{-1}kg = a$ para algún $a \in A$. Multiplicando ahora por k_1 por la izquierda llegamos a que $g^{-1}kg = k_1a \in KA \subseteq K$ debido a que $A \leq K$ y queda probado que $K \triangleleft G$. Se sigue por el tercer teorema de isomorfía que $(G/A)/(K/A) \simeq G/K$.

Reciprocamente tenemos que ver que $gkg^{-1}A \in K/A\ \ \forall g \in G, k \in K$. Sea $g \in G, k \in K$, como $K \triangleleft G$, $gkg^{-1} \in K$. Luego $\exists k_1 \in K$ tal que $gkg^{-1} = k_1$ por lo que $gkg^{-1}A = k_1A$, es decir, $gkg^{-1}A \in K/A$. □

Proposición 2.7. *(Lema de Zassenhaus). Sean A_1, A_2, B_1, B_2 subgrupos de un grupo G tales que $A_1 \triangleleft A_2$ y $B_1 \triangleleft B_2$. Sea $D_{ij} = A_i \cap B_j$. Entonces, $A_1D_{21} \triangleleft A_1D_{22}$ y $B_1D_{12} \triangleleft B_1D_{22}$. Además, los grupos A_1D_{22}/A_1D_{21} y B_1D_{22}/B_1D_{12} son isomorfos.*

Demostración. En primer lugar, observamos que como $A_1 \triangleleft A_2$, $D_{22} \leq A_2$ y $D_{21} \leq A_2$ se sigue por (2.4) que A_1D_{21} y A_1D_{22} son grupos.

Como $D_{22} \leq A_2$ y $A_1 \triangleleft A_2$ tenemos que D_{22} normaliza a A_1. Por otra parte $B_1 \triangleleft B_2$ implica que $D_{21} \triangleleft D_{22}$. Tenemos así que D_{22} normaliza a A_1D_{21}.

De formal trivial $A_1 \triangleleft A_1$, luego si vemos que para todo $g \in D_{21}$ y para todo $x \in A_1$ se cumple que $g^x \in A_1D_{22}$ habremos probado que $A_1D_{21} \triangleleft A_1D_{22}$. Veamoslo, sea $g \in D_{21}$ y $x \in A_1$ tenemos que $g^x = x^{-1}gx$ como $x^{-1}g \in A_1D_{21} = D_{21}A_1$ existirán $g_1 \in D_{21}$ y $x_1 \in A_1$ tales que $x^{-1}g = g_1x_1$ de tal forma que $g^x = x^{-1}gx = g_1x_1x \in D_{21}A_1 = A_1D_{21}$. De forma análoga se prueba que B_1D_{12} es normal en B_1D_{22}.

El segundo teorema de isomorfía nos dice que dados un subgrupo H y un subgrupo normal N de un grupo G. Entonces $N \cap H \triangleleft H$ y $H/(N \cap H) \simeq (NH)/N$. Aplicándolo para $H = D_{22}$ y $N = A_1D_{21}$ tenemos que $D_{22}/(A_1D_{21} \cap D_{22}) \simeq (A_1D_{21}D_{22})/(A_1D_{21})$. Y como $D_{21} \subseteq A_1$, por la ley modular:

$$(A_1D_{21}) \cap D_{22} = (A_1 \cap D_{22})D_{21} = (A_1 \cap A_2 \cap B_2)D_{21} = (A_1 \cap B_2)D_{21} = D_{12}D_{21}.$$

Y juntando ambos resultados obtenemos que $D_{22}/(D_{12}D_{21}) \simeq (A_1D_{22})/(A_1D_{21})$. De forma análoga vemos que $D_{22}/(D_{12}D_{21}) \simeq (B_1D_{22})/(B_1D_{21})$. Y se sigue que

$$\frac{A_1D_{22}}{A_1D_{21}} \simeq \frac{B_1D_{22}}{B_1D_{21}}.$$

□

Teorema 2.8. *(Teorema del refinamiento de Schereier). Dos cadenas cualesquiera de un grupo tienen refinamientos isomorfos.*

Demostración. Sean $1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_l = G$ y $1 = K_0 \triangleleft K_1 \triangleleft \cdots \triangleleft K_m = G$ dos cadenas de G. Definimos: $H_{i,j} = H_i(H_{i+1} \cap K_j)$ y $K_{i,j} = K_j(H_i \cap K_{j+1})$. Aplicando (2.7) a $A_1 = H_i, A_2 = H_{i+1}, B_i = K_j$ y $B_2 = K_{j+1}$ obtenemos que:

$$H_{i,j} \triangleleft H_{i,j+1}, \;\; K_{i,j} \triangleleft K_{i+1,j},$$

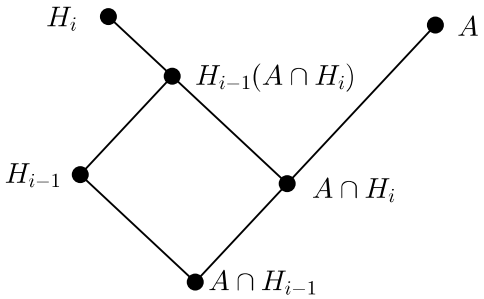
$$\frac{H_{i,j+1}}{H_{i,j}} = \frac{H_i(H_{i+1} \cap K_{j+1})}{H_i(H_{i+1} \cap K_j)} \simeq \frac{K_j(H_{i+1} \cap K_{j+1})}{K_j(H_i \cap K_{j+1})} = \frac{K_{i+1,j}}{K_{i,j}}.$$

Como $H_{i,0} = H_i(H_{i+1} \cap K_0) = H_i(H_{i+1} \cap 1) = H_i$ y $H_{i,m} = H_i(H_{i+1} \cap K_m) = H_i(H_{i+1} \cap G) = H_iH_{i+1} = H_{i+1}$ tenemos que la cadena $\{H_{i,j} | i = 0, ..., l-1, \; j = 0, ..., m\}$ es un refinamiento de $\{H_i | i = 0, ..., l\}$ de forma análoga $\{K_{i,j} | i = 0, ..., l, \; j = 0, ..., m-1\}$ lo es de $\{K_j | j = 0, ..., m\}$. Y estos refinamientos son isomorfos. □

2.2 Propiedades de grupos resolubles y policíclicos

Proposición 2.9. *Sea G un grupo policíclico (resoluble) y $A \leq G$, entonces A es policíclicos (resolubles). En el caso $A \triangleleft G$, entonces G es policíclico (resoluble) si y solo si A y G/A son policíclicos (resolubles).*

Demostración. Sea $A \leq G$ y sea una cadena de G, $1 \triangleleft H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = G$, consideramos $1 = H_0 \cap A \triangleleft H_1 \cap A \triangleleft \cdots \triangleleft H_n \cap A = A$ que es una cadena de A. Veamos ahora que sus factores son cíclicos (abelianos). Para ello notaremos que como $H_{i-1} \triangleleft H_i$ y $A \cap H_i \leq H_i$ por (2.4) $H_{i-1}(A \cap H_i)$ es un subgrupo de H_i y por la ley modular $H_{i-1}(A \cap H_i) = H_{i-1}A \cap H_i$.

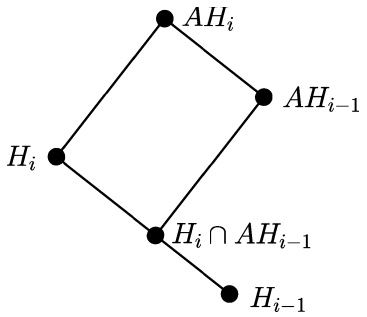


Por el segundo teorema de isomorfía se sigue que:

$$\frac{H_{i-1}A \cap H_i}{H_{i-1}} = \frac{H_{i-1}(A \cap H_i)}{H_{i-1}} \simeq \frac{A \cap H_i}{A \cap H_i \cap H_{i-1}} = \frac{A \cap H_i}{A \cap H_{i-1}}.$$

Como H_i/H_{i-1} es cíclico (abeliano) y $(H_{i-1}A \cap H_i)/H_{i-1}$ es un subgrupo de este, tenemos que $(H_{i-1}A \cap H_i)/H_{i-1}$ es cíclico (abeliano) y por tanto $(A \cap H_i)/(A \cap H_{i-1})$ será cíclico (abeliano).

Probemos ahora que un cociente de un grupo policíclico (resoluble) es policíclico (resoluble). Como $A \triangleleft G$ y $H_{i-1} \triangleleft H_i$, se sigue por (2.5) que $AH_{i-1} \triangleleft AH_i$.



Por tanto, por (2.6) tenemos que $AH_i/A \trianglelefteq AH_{i+1}/A$. Tenemos así que $H_i \leq AH_i$ y $AH_{i-1} \trianglelefteq AH_i$. Por el segundo y tercero teorema de isomorfía se sigue que:

$$\frac{H_i}{H_i \cap AH_{i-1}} \simeq \frac{AH_{i-1}H_i}{AH_{i-1}} = \frac{AH_i}{AH_{i-1}} \simeq \frac{(AH_i)/A}{(AH_{i-1})/A}.$$

Y al igual que antes como H_i/H_{i-1} es cíclico (abeliano), lo será $H_i/(H_i \cap AH_{i-1})$, por lo que lo será $\frac{(AH_i)/A}{(AH_{i-1})/A}$. Tenemos una cadena $1 = AH_0/A \triangleleft AH_1/A \triangleleft \cdots \triangleleft AH_n/A = G/A$. Luego G/A es policíclico (resoluble). El recíproco se sigue fácilmente usando (2.6). □

Proposición 2.10. *En un grupo policíclico el número de grupos cociente infinitos en una cadena es independiente de la cadena escogida y por tanto es fijo para G.*

Demostración. Sea una cadena $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ se deduce de (2.8) que todo refinamiento de esta cadena tendrá el mismo número de factores cíclicos infinitos. □

Definición. A este número se le conoce como *longitud de Hirsch*, lo denotaremos por $l(G)$.

Observación 2.11. La longitud de Hirsch se puede definir para grupos resolubles como la suma de los rangos libres de los factores abelianos.

Observación 2.12. Sea $A \triangleleft G$, entonces $l(G) = l(G/A) + l(A)$.

Observación 2.13. Sea A un grupo policíclico infinito entonces $l(A) > 0$.

Definición. Diremos que un grupo es *poli-infinito cíclico* si tiene una cadena con factores cíclicos infinitos, esto es, un grupo policíclico en la que todos sus factores son infinitos.

Observación 2.14. Un subgrupo H de un grupo poli-infinito cíclico G es también poli-infinito cíclico.

2.3 Conmutadores y la cadena derivada

Definición. Sea G un grupo, x_1, x_2 elementos de G y X_1, X_2 conjuntos no vacíos de G. Llamaremos *conmutador* de x_1 y x_2 a

$$[x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$$

y *subgrupo conmutador* de X_1 y X_2 a

$$[X_1, X_2] = \langle [x_1, x_2] | x_1 \in X_1,\ x_2 \in X_2 \rangle.$$

Finalmente, se llama grupo derivado de G y se denota por G', al generado por todos los conmutadores de G, esto es, $G' = [G, G]$.

Proposición 2.15. *Sean L y G grupos si $L \trianglelefteq G$. Entonces $L' \trianglelefteq G$.*

Demostración. Sea $g \in G$ tenemos que ver que $g^{-1} l g \in L' \ \ \forall l \in L'$. Sera suficiente ver que dado $[l_1, l_2] \in L$, entonces $g^{-1}[l_1, l_2]g \in L$. Como $L \trianglelefteq G$ tenemos

$$g^{-1}[l_1, l_2]g = g^{-1} l_1^{-1} l_2^{-1} l_1 l_2 g = g^{-1} l_1^{-1} g g^{-1} l_2^{-1} g g^{-1} l_1 g g^{-1} l_2 g = (g^{-1} l_1 g)^{-1} (g^{-1} l_2 g)^{-1} g^{-1} l_1 g g^{-1} l_2 g \in L'.$$

□

Corolario 2.16. *El derivado de un grupo es normal en este.*

Demostración. Inmediato por (2.15) con $L = G$. □

Proposición 2.17. *Para todo grupo G, G/G' es abeliano.*

Demostración. Sean $x_1, x_2 \in G$. Veamos que $(x_1G')(x_2G') = x_1x_2G'$ y $(x_2G')(x_1G') = x_2x_1G'$ son el mismo elemento de G/G'. La igualdad $x_1x_2G' = x_2x_1G'$ es cierta si y solo si $x_1^{-1}x_2^{-1}x_1x_2G' = G'$ lo cual se cumple si y solo si $x_1^{-1}x_2^{-1}x_1x_2 \in G'$ que es cierto, luego G/G' es abeliano. □

Corolario 2.18. *Para todo grupo G, el subgrupo normal más pequeño de G cuyo cociente es abeliano es G'.*

Demostración. Sea $K \triangleleft G$ tal que G/K es abeliano. Sean $x, y \in G$ entonces que $xyK = yxK$ implica que $x^{-1}y^{-1}xy \in K$, o bien que $[x,y] \in K$. Por tanto $G' \leq K$. □

Definición. Llamaremos *cadena derivada* de G a:

$$G = G^{(0)} \geq G^{(1)} \geq \cdots$$

donde $G^{(n+1)} = (G^{(n)})'$. Notar que esta cadena podría no llegar a 1 o incluso no terminar. Por supuesto todos los factores serán abelianos por (2.17).

Al número de factores de esta cadena lo llamaremos *longitud derivada* de G.

Observación 2.19. Por inducción sobre (2.15) obtenemos que $L^{(d)} \triangleleft G$.

Proposición 2.20. *Para todo A normal en G e $i \geq 0$, $G^{(i)}/A = (G/A)^{(i)}$.*

Demostración. Probémoslo por inducción sobre i. Para $i = 0$ el resultado es trivial. Supongámoslo cierto para $i-1$ y probémoslo para i.

$$\begin{aligned}(G/A)^{(i)} &= [(G/A)^{(i-1)}, (G/A)^{(i)}] = [G^{(i-1)}/A, G^{(i-1)}/A] = \langle [x_1A, x_2A] | x_1, x_2 \in G^{(i-1)} \rangle = \\ &= \langle x_1^{-1}x_2^{-1}x_1x_2A | x_1, x_2 \in G^{(i-1)} \rangle = [G^{(i-1)}, G^{(i-1)}]/A = G^{(i)}/A.\end{aligned}$$

□

Proposición 2.21. *Si $1 = G_0 \triangleleft G_1 \triangleleft \cdots G_n = G$ es una cadena cuyos factores son abelianos, entonces $G^{(i)} \leq G_{n-i}$. En particular $G^{(n)} = 1$.*

Demostración. Si $i = 0$ el teorema se cumple trivialmente. Supongámoslo cierto para $i-1$ y probémoslo para i. Tenemos que $G^{(i)} = (G^{(i-1)})' = [G^{(i-1)}, G^{(i-1)}] \leq [G_{n-(i-1)}, G_{n-(i-1)}] = (G_{n-(i-1)})'$. Por otra parte como $G_{n-(i-1)}/G_{n-i}$ es abeliano, su derivado será el grupo trivial, y por (2.20) se sigue que $(G_{n-(i-1)})'/G_{n-i} = 1$ teniendo así que $(G_{n-(i-1)})' \leq G_{n-i}$. Por lo tanto $G^{(i)} \leq G_{n-i}$. Se sigue que una cadena con factores abelianos no puede ser mas corta que la derivada. □

Observación 2.22. La longitud derivada de G es la longitud de la cadena abeliana más corta de G.

Proposición 2.23. *Sea G un grupo resoluble con longitud deriva d. Entonces la longitud derivada de $G/G^{(d-1)}$ es $d-1$.*

Demostración. Sabemos que la cadena derivada de G es

$$1 = G^{(d)} \trianglelefteq G^{(d-1)} \trianglelefteq G^{(d-2)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

Como hemos visto en (2.15) $G^{(d-1)} \trianglelefteq G^{(i)}$ $\forall 0 \leq i \leq d-1$ y al hacer uso del tercer teorema de isomorfía tenemos que

$$1 = G^{(d-1)}/G^{(d-1)} \trianglelefteq G^{(d-2)}/G^{(d-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)}/G^{(d-1)} \trianglelefteq G^{(0)}/G^{(d-1)} = G/G^{(d-1)}$$

cuyos factores son abelianos y es la cadena derivada de $G/G^{(d-1)}$ debido a que por (2.20) sabemos que $G^{(i)}/G^{(d-1)} = (G/G^{(d-1)})^{(i)}$ por lo que la distancia derivada de $G/G^{(d-1)}$ es $d-1$. □

2.4 Propiedades de grupos finitamente generados y policíclicos

Definición. Diremos que un grupo G es *libre de torsión* si $g^n \neq 1\ \forall g \in G,\ \forall\, 0 \neq n \in \mathbb{Z}$ mientras que diremos que G es *de torsión* si $\forall g \in G\ \ \exists\, 0 \neq n \in \mathbb{Z}$ tal que $g^n = 1$.

Observación 2.24. Todo grupo finito es de torsión.

Proposición 2.25. *Sea H un subgrupo de índice finito en un grupo finitamente generado G, entonces, H es finitamente generado.*

Demostración. Sea X un conjunto finito de generadores de G y sea $\{1 = t_1, t_2, ..., t_n\} = \mathbf{T}$ un transversal a derecha de H en G. Esto es, $Ht_i \neq Ht_j\ \forall 1 \leq i, j \leq n$ y $G = \bigcup_{i \in \mathbf{T}} Ht_j$. Si $g \in G$, entonces para cada t_j existirá un elemento del transversal que dependerá de j y g, llamémosle $t_{(j,g)}$, de forma que $Ht_j g = Ht_{(j,g)}$ y por tanto existirá un elemento de H que dependerá de j y g, llamémosle $h_{(j,g)}$, de forma que

$$t_j g = h_{(j,g)} t_{(j,g)}.$$

Todo $a \in H$ podremos escribirlo como producto de generadores de G, es decir $a = y_1 \cdots y_k$ con $y_l \in X$. Aplicando ahora la igualdad anterior de forma reiterada:

$$\begin{aligned} a = t_1 a = t_1 y_1\, y_2 \cdots y_k = h_{(1,y_1)}\, t_{(1,y_1)} y_2\, y_3 \cdots y_k = h_{(1,y_1)} h_{((1,y_1),y_2)} t_{((1,y_1),y_2)} y_3\, y_4 \cdots y_n = ... = \\ = h_{(1,y_1)} h_{((1,y_1),y_2)} \cdots t_{((\cdots((1,y_1),y_2)\cdots),y_n)}. \end{aligned}$$

Entonces como $a \in H$ se deduce $t_{((\cdots((1,y_1),y_2)\cdots),y_n)} \in H$, luego $t_{((\cdots((1,y_1),y_2)\cdots),y_n)} = t_1 = 1$ por lo que los h's, los cuales unicamente dependen de los generadores de G, generaran H. Siendo así H finitamente generado. □

Proposición 2.26. *Un grupo abeliano finitamente generado es finito si y solo si es de torsión.*

Demostración. Sea G de torsión. Sean $g_1, ..., g_n$ generadores asociados a la descomposición de (1.8) tenemos que $G = \langle g_1, ..., g_n \rangle$ y $G_i = \langle g_i \rangle$, como G es de torsión todos los G_i serán finitos. Sabiendo que G es la suma de $G_1, ..., G_n$ tenemos que G es finito. El reciproco es la observación (2.24). □

Proposición 2.27. *Un grupo de torsión resoluble y finitamente generado es finito.*

Demostración. Sea G dicho grupo y llamemos d a su longitud derivada. Vamos a probarlo por por inducción sobre d. Si $d = 0$, no hay nada que probar. Así que sea $d > 0$ supongamos el resultado cierto para $d-1$ y probémoslo para d, escribimos $A = G^{(d-1)}$ el cual será el último miembro de la cadena distinto de 1 y por tanto será abeliano. Como sabemos por (2.23) que la distancia derivada de G/A es $d-1$, G/A es finito. Y por (2.25) tenemos que A es finitamente generado. Finalmente como un subgrupo de un grupo de torsión también es de torsión, aplicando (2.26) obtenemos que A es finito y por tanto G finito. □

Proposición 2.28. *Sea G un grupo policíclico infinito:*

(i) G tiene un subgrupo poli-infinito cíclico normal de índice finito.

(ii) G contiene un subgrupo normal abeliano no trivial libre de torsión.

Demostración. (i) Sea $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ una cadena cíclica de un grupo policíclico G. Si $n \leq 1$, entonces G es cíclico y el resultado es obvio. Sea $n > 1$ y definimos $N = G_{n-1}$. Por inducción sobre n hay un subgrupo normal M de N tal que M es poli-infinito cíclico y N/M es finito. Consideramos ahora $M_G = \bigcap_{g \in G} M^g$ el cual es normal en G y como $N \leq G$, $M_G \triangleleft N$ por lo que podemos pensar en N/M_G que es finitamente generado, en efecto, como N es policíclico, N es finitamente generado y N/M_G también lo será. Veamos que N/M_G es de torsión. Sabemos que N/M es finito, sea m su orden. Sea un $x \in N$. Entonces, para cualquier $g \in G$, $x^g \in N$, por ser G normal en N, luego $(x^g)^m \in M$ por

tanto $(x^m)^g = (x^g)^m \in M$ luego $x^m \in M^{g^{-1}}$ para cualquier $g \in G$, lo que implica que $x^m \in M_G$ deduciendo así que N/M_G es de torsión. Finalmente como N es policíclico, entonces N/M_G será policíclico y en particular resoluble luego podemos aplicar (2.27) teniendo así que N/M_G es finito. Por otra parte M_G es poli-infinito cíclico por ser subgrupo de M. Por lo que no hay perdida de generalidad en asumir que $M \triangleleft G$. Si G/N es finito, entonces $|G:M| = |G:N||N:M| < \infty$ por lo que G/M será finito y habremos terminado.

Por lo que ahora consideramos el caso en el que G/N es cíclico infinito. Sea xN con $x \in G$ un generador de dicho grupo. Como xN genera $G/N = C_\infty$ entonces $x \in G$ tiene orden infinito y es claro que $G = \langle x, N\rangle$. El elemento x actuará por conjugación en cualquier subgrupo de G. Por ser $M \triangleleft G$, $M^x = M$. Luego también actuará por conjugación en N/M el cual es finito. Al ser este cociente finito, existirá un r tal que x^r actúa trivialmente sobre N/M, es decir, $g^{x^r}M = gM \ \ \forall g \in N$. Llamamos $L = \langle x^r, M\rangle$. En el resto de la demostración vamos a probar que L es el grupo que buscamos.

Veamos que $L = \langle x^r, M\rangle \triangleleft \langle x, N\rangle = G$. Como $M \triangleleft N$ y $M^x = M$ la normalidad se seguirá si probamos que N normaliza a $\langle x^r, M\rangle$. Sabemos que $n^{x^r}M = nM \ \forall n \in N$ lo que es lo mismo que $(x^r)^{-1}nx^rM = nM \leftrightarrow (x^r)^{-1}n^{-1}x^rnM = M$ teniendo así que $(x^r)^{-1}n^{-1}x^rn \in M$ luego $(x^r)^n \in \langle x^r, M\rangle$ y se prueba lo que queríamos. Vamos ahora a probar que G/L es finito. Por un lado es producto de $\langle x, L\rangle/L$ y NL/L. En efecto, como $L \leq M \leq N$, tenemos

$$\frac{\langle x,L\rangle}{L} \cdot \frac{NL}{L} = \frac{\langle x\rangle L}{L} \cdot \frac{NL}{L} = \frac{\langle x\rangle LNL}{L} = \frac{\langle x\rangle N}{L} = \frac{\langle x,N\rangle}{L} = \frac{G}{L}.$$

Veamos ahora que estos grupos son finitos. El segundo teorema de isomorfía implica que:

$$\frac{LN}{L} \simeq \frac{N}{L\cap M} = \frac{N}{M}$$

debido a que $M \subseteq L$ luego como N/M es finito, LN/L también lo será. Veamos ahora que $\langle x, L\rangle/L$ es finito. Se tiene que $\langle x^r\rangle \leq L \cap \langle x\rangle \leq \langle x\rangle$ y es claro que el índice de $\langle x\rangle$ en $\langle x^r\rangle$ es r, luego, $\langle x\rangle/(L\cap\langle x\rangle)$ es finito y el segundo teorema de isomorfía nos dice que

$$\frac{\langle x,L\rangle}{L} = \frac{\langle x\rangle L}{L} \simeq \frac{\langle x\rangle}{L\cap\langle x\rangle}.$$

Luego $\langle x, L\rangle/L$ es finito. y deducimos que G/L también lo es. Unicamente nos falta de ver que L es poli-infinito.

Como no hay ninguna potencia de x que pueda pertenecer a N, debido a que xN genera un grupo cíclico infinito, si L/M fuera finito existiría un $m \in \mathbb{N}$ tal que $(x^r)^m = x^{rm} \in M \leq N$ lo cual es una contradicción, luego el factor L/M es infinito. Por el segundo teorema de isomorfía.

$$\frac{L}{M} = \frac{\langle x^r\rangle M}{M} \simeq \frac{\langle x^r\rangle}{M\cap\langle x^r\rangle}$$

que es cíclico por lo que L/M es cíclico infinito. Como M es poli-infinito cíclico, enlazando las cadenas tenemos una cadena con factores cíclicos en la que todos son infinitos por lo que L será poli-infinito cíclico.

(ii) Si G es infinito, entonces $L \neq 1$ y se sigue de (2.14) que L también será poli-infinito cíclico, y en particular será un grupo resoluble. El término mas pequeño de la cadena derivada de L, llamémosle A, es abeliano, normal en G por (2.15) y libre de torsión por ser cíclico e infinito. □

Definición. Llamaremos G^m al conjunto generado por los g^m tales que $g \in G$ para cualquier grupo G y $0 \neq m \in \mathbb{Z}$.

Lema 2.29. *Sea $A \trianglelefteq G$, entonces $A^m \trianglelefteq G$.*

Demostración. Sea $g \in G$ y $a^m \in A^m$. Se tiene que $ga^mg^{-1} = \underbrace{gag^{-1}}_{\in A}\underbrace{gag^{-1}}_{\in A}\cdots\underbrace{gag^{-1}}_{\in A} \in A^m$. □

Observación 2.30. Para un grupo G y $0 \neq m \in \mathbb{Z}$, $|G : G^m|$ no tiene porqué ser finito.

Lema 2.31. *Sea A abeliano y $B \triangleleft A$ con $|A : B| < \infty$, entonces $\exists m > 0$ tal que $A^m \leq B$.*

Demostración. Llamamos $m = |A : B|$ entonces A/B será finito de orden m por lo que $(aB)^m = B \; \forall a \in A$ luego $a^m B = B$ tenemos así que $a^m \in B$ y como A es abeliano $a^m b^m = (ab)^m$ de forma que

$$A^m = \langle a^m | a \in A \rangle = \{a^m | a \in A\} \leq B.$$

□

Lema 2.32. *Sea un grupo abeliano finitamente generado A entonces $|A : A^m| < \infty \; \forall m \in \mathbb{N}$.*

Demostración. Es trivial que $A^m \trianglelefteq A \; \forall m \in \mathbb{N}$ por ser A abeliano. Sea $a \in A$, entonces, $a^m \in A^m$. Teniendo así $(aA^m)^m = a^m A^m = 1_{A/A^m}$ luego todo elemento de A/A^m tiene orden m o divisor de m y como A/A^m es finitamente generado es finito por (2.26). □

Teorema 2.33. *Los grupos policíclicos son residualmente finitos.*

Demostración. Lo primero de todo es decir que como G es policíclico, será finitamente presentado y en particular finitamente generado por lo que si además es abeliano por (1.8) será residualmente finito.

Veamos ahora el caso general en el que G no tiene porque ser abeliano. Habrá que demostrar que para cualquier $1 \neq g \in G$, con G policíclico, existe $N \triangleleft G$ tal que $g \notin N$ y G/N es finito.

Sea l la longitud de Hirsch de G. En el caso en el que $l = 0$ el grupo G es finito y no hay nada que probar. Supongamos cierto para todo G policíclico con $l(G) < n$ siendo $n > 0$ y razonaremos por inducción. Por (2.28) existe un subgrupo normal de G abeliano, no trivial y libre de torsión $A \neq 1$. Por (2.13) $l(A) > 0$ entonces como $l(G) = l(G/A) + l(A)$ tenemos que $l(G/A) < l(G)$ y por inducción sobre l, partiendo de que G/A es policíclico por (2.9) entonces, será residualmente finito.

Sea $g \in G$, hay que encontrar un subgrupo K tal que $|G : K| < \infty$ y $g \notin K$. Si $g \notin A$ entonces $1 \neq gA \in G/A$ y como G/A es residualmente finito, existirá $K/A \triangleleft G/A$ con $gA \notin K/A$ lo que implica por (2.6) que $K \triangleleft G$ y $(G/A)/(K/A) \simeq G/K$ finito y que $g \notin K$. Veamos ahora el caso en el que $g \in A$.

Por el caso abeliano existe un subgrupo B de A que además es normal en A con $|A : B| < \infty$ y $g \notin B$. Por otra parte por (2.31) tenemos que $A^m \leq B$ para algún $m > 0$ y por (2.32) sabemos que $|A : A^m| < \infty$. Notaremos que A^m y G/A^m serán policíclicos pues A^m es un subgrupo normal de G por (2.29). Y A^m será infinito debido a que A lo es y $|A : A^m| < \infty$.

Por otra parte como G es finitamente presentado, A será finitamente presentado. Ya hemos visto que A/A^m es finito. Al igual que antes, por (2.13), $l(A^m) > 0$ y $l(G) = l(G/A^m) + l(A^m)$ lo que implica que $l(G/A^m) < l(G)$ y como G/A^m por (2.9) es policíclico, por inducción sobre l el teorema será cierto para G/A^m. Luego si, $g \notin A^m$ entonces $1 \neq gA^m \in G/A^m$ por lo que existe H/A^m con $gA^m \notin H/A^m$ tal que $H/A^m \triangleleft G/A^m$ y $(G/A^m)/(H/A^m)$ es finito y por (2.6), $H \triangleleft G$ y $(G/A^m)/(H/A^m) \simeq G/H$ será finito y $g \notin H$, siendo así G residualmente finito. En el caso en el que $g \in A^m$ como $A^m \leq B$ entonces $g \in B$ lo cual contradice que $g \notin B$. □

Corolario 2.34. *Los grupos policíclicos tienen solución al problema de la palabra.*

Demostración. Se sigue de (2.1), (2.33) y (1.13). □

Capítulo 3

Ejemplos

3.1 El grupo discreto de Heisenberg

Definición. Dada una matriz triangular superior diremos que es *unitriangular* si todos los elementos de la diagonal principal son unos.

El conjunto de estas matrices de tamaño $n \times n$ con entradas en $\mathbb{Z}$ junto con la operación producto forman un grupo conocido como *grupo unitriangular*, lo denotaremos por $UT(n,\mathbb{Z})$. Estos grupos son policíclicos para todo $n \in \mathbb{N}$ y el caso en el que $n = 3$ se conoce como *Grupo de Heisenberg discreto* mientras que el *grupo de Heisenberg continuo* es $UT(3,\mathbb{R})$. Las aplicaciones más destacadas de este grupo las encontramos en la descripción de sistemas de partículas cuánticos y en el análisis de Fourier (en algunas formulaciones del teorema de Stone-Von Neumann).

Ejemplo 6. Se ve fácilmente que $UT(2,\mathbb{Z})$ es isomorfo al grupo $(\mathbb{Z},+)$.

$$UT(2,\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\} = \left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\rangle \simeq (\mathbb{Z},+).$$

Ahora probaremos que el grupo de Heisenberg es policíclico, buscaremos su cadena derivada, veremos que es residualmente finito, daremos una presentación y construiremos un algoritmo más sencillo para resolver el problema de la palabra.

3.1.1 El grupo de Heisenberg discreto como grupo policíclico

Tenemos que el grupo discreto de Heisenberg es el formado por el siguiente conjunto de matrices:

$$UT(3,\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{Z} \right\}.$$

Tomemos la matriz $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = z$. Notaremos que $z^n = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ para todo $n \in \mathbb{Z}$. En particular $z^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Al igual que en el ejemplo 6, el grupo generado por esta matriz, que llamaremos Z, es isomorfo a $(\mathbb{Z},+)$ de lo que deducimos que este grupo es cíclico.

Por otra parte $\langle z\rangle = Z$ es normal en $UT(3,\mathbb{Z})$, en efecto, tomando $A = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ tenemos que:

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & -a & ab-c+n \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Lo que prueba que Z no solo es normal en $UT(3,\mathbb{Z})$, sino que además lo centraliza.

Por lo que tenemos que $1 \triangleleft Z \triangleleft UT(3,\mathbb{Z})$ con Z cíclico, luego si vemos que $UT(3,\mathbb{Z})/Z$ es policíclico se seguirá de (2.9) que $UT(3,\mathbb{Z})$ es policíclico. Para ver esto veamos si es isomorfo a algún grupo conocido.

Pensemos en las matrices $x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Vemos que $xy = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = yx$ pero $xy = yxz$. De lo que deducimos que $x^a y^b = \begin{pmatrix} 1 & a & ab \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = y^b x^a z^{ab}$ $\forall a,b,c \in \mathbb{Z}$ teniendo así que $x^a y^b$ e $y^b x^a$ pertenecen a la misma coclase de nuestro grupo cociente. Luego $UT(3,\mathbb{Z})/Z$ es abeliano.

Por otra parte, dado un elemento del cociente, $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} Z$ este quedará unequívocamente determinado por $x^a y^b Z$ luego $UT(3,\mathbb{Z})/Z \simeq \langle xZ, yZ\rangle$. Luego, la aplicación $f : \langle xZ, yZ\rangle \longrightarrow \mathbb{Z}\oplus\mathbb{Z}$ tal que a cada $x^a y^b Z \mapsto (a,b)$ es un isomorfismo de grupos. Esto implica que $UT(3,\mathbb{Z})/Z \simeq \mathbb{Z}\oplus\mathbb{Z}$ es policíclico.

3.1.2 Cadena derivada del grupo discreto de Heisenberg

Empecemos viendo cual es el derivado de $UT(3,\mathbb{Z}) = G$. Recordaremos que

$$G' = [G,G] = \langle [x_1,x_2] | x_1, x_2 \in G\rangle.$$

Sabemos por (2.18) que G' es el menor grupo normal con G/G' abeliano, por tanto $G' \leq Z$ y $(G')' = 1$.

Tomemos dos matrices genéricas de G, $x_1 = \begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix}$ y $x_2 = \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$ y calculemos su conmutador

$$[x_1,x_2]=x_1^{-1}x_2^{-1}x_1x_2=\begin{pmatrix}1&a_1&c_1\\0&1&b_1\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&a_2&c_2\\0&1&b_2\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&a_1&c_1\\0&1&b_1\\0&0&1\end{pmatrix}\begin{pmatrix}1&a_2&c_2\\0&1&b_2\\0&0&1\end{pmatrix}=$$

$$=\begin{pmatrix}1&-a_1&a_1b_1-c_1\\0&1&-b_1\\0&0&1\end{pmatrix}\begin{pmatrix}1&-a_2&a_2b_2-c_2\\0&1&-b_2\\0&0&1\end{pmatrix}\begin{pmatrix}1&a_1&c_1\\0&1&b_1\\0&0&1\end{pmatrix}\begin{pmatrix}1&a_2&c_2\\0&1&b_2\\0&0&1\end{pmatrix}=$$

$$=\begin{pmatrix}1&-a_1-a_2&a_1b_1+a_1b_2+a_2b_2-c_1-c_2\\0&1&-b_1-b_2\\0&0&1\end{pmatrix}\begin{pmatrix}1&a_1+a_2&a_1b_2+c_1+c_2\\0&1&b_1+b_2\\0&0&1\end{pmatrix}=$$

$$=\begin{pmatrix}1&0&-a_2b_1+a_1b_2\\0&1&0\\0&0&1\end{pmatrix}.$$

Por lo que $G'=\left\langle\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}\right\rangle$.

Comprobemos la teoría calculando $(G')'$. El derivado de G' será el generado por:

$$\begin{pmatrix}1&0&a_1\\0&1&0\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&0&a_2\\0&1&0\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&0&a_1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&a_2\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}.$$

Tenemos así que la cadena derivada es $1\triangleleft G'\triangleleft G$, que es la obtenida anteriormente.

3.1.3 Presentación del grupo discreto de Heisenberg

Veamos una presentación de este grupo. Para ello vamos a hacer uso del teorema (1.6). En nuestro caso tendremos $G=UT(3,\mathbb{Z})$ y $N=\langle z\rangle$. Veamos la representación del grupo cociente G/N. Hemos visto antes que $N=G'=\langle[x_1,x_2]|x_1,x_2\in G\rangle$. luego $G/N=\langle x,y|[x,y]=1\rangle$.

La demostración del teorema (1.6) nos dice que existe una presentación de G generada por x,y,z con las siguientes relaciones entre ellos: $[x,y]=z^k$ para algún $k\in\mathbb{Z}$ y las relaciones de normalidad, $x^{-1}zx=z^j$, $y^{-1}zy=z^i$ con $j,i\in\mathbb{Z}$. Por otra parte hemos visto antes que $\langle z\rangle$ centraliza a G, luego $i=j=1$ y también que $xy=yxz$. Por lo tanto $[x,y]=x^{-1}y^{-1}xy=z$ teniendo así que $k=1$, luego nuestra presentación de G queda:

$$G=\langle x,y,z\mid[x,y]=z,\ [x,z]=[y,z]=1\rangle.$$

3.1.4 El grupo discreto de Heisenberg como ejemplo de grupo residualmente finito

Ahora probaremos que $UT(3,3^n\mathbb{Z})=N$ es normal en G para todo $n\in\mathbb{N}$.

Tomemos $g=\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}$ con $a,b,c\in\mathbb{Z}$ y $h=\begin{pmatrix}1&d&f\\0&1&e\\0&0&1\end{pmatrix}$ con $d,e,f\in 3^n\mathbb{Z}$

$$g^{-1}hg=\begin{pmatrix}1&-a&ab-c\\0&1&-b\\0&0&1\end{pmatrix}\begin{pmatrix}1&d&f\\0&1&e\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}=\begin{pmatrix}1&d&bd-ae+f\\0&1&e\\0&0&1\end{pmatrix}\in N$$

y $G/N=UT(3,\mathbb{Z}_{3^n})$ que es finito. Luego dado $g\in G$ existirá un $N\triangleleft G$ asociado a n tal que 3^n no divida a las entradas de g y como $|G:N|$ es finito, tenemos que G es residualmente finito.

3.1.5 El problema de la palabra para el grupo discreto de Heisenberg

En la practica no suele ser eficiente usar el algoritmo descrito en (1.13) para comprobar si una palabra es la identidad en un grupo o no, y el caso del grupo discreto de Heisenberg no va a ser una excepción, existe una forma mucho más eficiente y sencilla de comprobarlo, veámosla.

Una palabra w se dará en términos de los elementos x,y,z anteriores. Sabemos que z centraliza al grupo, luego podemos pasar todas las z's a la derecha obteniendo que $w = vz^l$ donde v es una palabra en términos de x,y.

También sabemos que $xy = yxz$ luego cada vez que veamos un producto xy lo cambiamos por un yxz y reagrupamos la z a la derecha. Realizamos esto hasta que obtengamos todos los y's en la parte izquierda, llegamos así a una palabra $w = x^i y^j z^k$. Esta palabra es la identidad si y solo si $i = j = k = 1$.

3.2 Grupos de Baumslag-Solitar

Definición. Los grupos dados por la presentación $\langle x,y|(x^p)^y = x^q\rangle$ con $q,p \in \mathbb{Z}$ se llaman *grupos de Baumslag-Solitar*. Los denotaremos por $BS(p,q)$.

Fueron introducidos por Gilbert Baumslag y Donald Solitar en 1962. Tienen especial importancia en la teoría combinatoria de grupos y en la teoría geométrica de grupos en donde suelen aparecer como contraejemplos. En nuestro caso vamos a ver si son residualmente finitos y si tienen solución al problema de la palabra.

Estos grupos también se pueden ver como extensiones HNN[1] de $\langle x\rangle$ con letra estable y, lo cual es fundamental para poder emplear el lema de Britton[2], el cual nos dice cuando una palabra w es o no es la identidad del grupo. En nuestro caso el lema se reduce a que si en una palabra $w \in BS(p,q)$ no hay una secuencia consecutiva de la forma $y^{-1}x^{p\alpha}y$ ó $yx^{q\alpha}y^{-1}$ con $\alpha \in \mathbb{Z}$, entonces $w \neq 1$.

3.2.1 EL grupo $BS(1,2)$

Proposición 3.1. *El grupo $BS(1,2) = \langle x,y|y^{-1}xy = x^2\rangle$ tiene solución al problema de la palabra.*

Demostración. Sea una palabra w en términos de x e y, la relación $xy = yx^2$ puede usarse para mover la letra y a la izquierda. De forma similar usando la relación $y^{-1}x = yx^2$ puede usarse para mover y^{-1} a la derecha, de tal forma que reduciendo cuando sea posible, tras un número finito de iteraciones llegamos a tener la palabra w de la siguiente forma

$$w = y^i x^j y^{-k}$$

donde $i,k \geq 0$ y $j \in \mathbb{Z}$.

En el caso en el que j sea par, $j = 2m$, y $i,j > 0$ podemos aplicar la relación $x^m = yx^{2m}y^{-1}$ obtenida a partir de $x = yx^2y^{-1}$ y deducimos que $w = y^{i-1}x^m y^{-(k-1)}$ si de nuevo m es par y $i-1, j-1 > 0$ repetimos este proceso. De tal forma que tras un número finito de iteraciones obtenemos que $w = y^a x^b y^{-c}$ donde o bien b es impar o bien $a = 0$ o $c = 0$. Tenemos así que por el lema de Britton, $w = 1$ si y solo si $b = 0$ y $a = c$. □

Proposición 3.2. *El grupo $BS(1,2)$ es residualmente finito.*

Demostración. Tal y como hemos visto en la demostración anterior, cualquier palabra $w \in BS(1,2) = G$ se puede reducir a la forma $w = y^a x^b y^{-c}$ donde o bien b impar o bien $a = 0$ o $c = 0$. Luego dada $1 \neq w = y^a x^b y^{-c}$ de esta forma, sabemos que, o bien $b > 0$, o bien $a \neq c$. En el caso en el que $b \neq 0$ elegimos un p primo impar que no divida a b y consideramos el subgrupo de G generado por y, x^p entonces se puede probar que w no está en este subgrupo y que este subgrupo tiene índice finito en

[1] Ver definición de extensión HNN con una única letra en [6, página 180]

[2] Lema de Britton en [6, página 181]

G. Por otra parte si $b = 0$, tenemos que $w = y^d$ con $0 \neq d \in \mathbb{Z}$, elegimos un p que no divida a d y consideramos el subgrupo de G generado por y^p, x y al igual que antes, se puede probar que w no está en este subgrupo y que este subgrupo tiene índice finito en G. □

Otra propiedad interesante de este grupo es que es lineal. Veamoslo. Consideramos la aplicación $\alpha : BS(1,2) \to G$ donde G es el grupo generado por las matrices $x^\alpha = A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $y^\alpha = B = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$ veamos que es un isomorfismo. Es claro que está bien definida porque conserva las relaciones, en efecto,

$$B^{-1}AB = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = A^2.$$

Por el teorema de von Dyck (1.4) tenemos que es un epimorfismo. Y por último usando el lema de Britton se prueba la inyectividad.

3.2.2 El grupo $BS(2,3)$

Lo interesante de este grupo es que no es residualmente finito pero si que tiene solución al problema de la palabra, comencemos con un lema que necesitaremos para probar que no es residualmente finito.

Lema 3.3. *Sea K un grupo finito y $a, b \in K$. Si a y b son conjugados y se cumple $a^2 = b^3$, entonces $[a,b] = 1$.*

Demostración. Como a y b son conjugados, tienen el mismo orden m. Supongamos que m es par. Entonces $m = 2n$ para algún n entero positivo y se cumple que $b^{2n} = 1$ y que $b^n \neq 1$. Elevamos la relación $a^2 = b^3$ a n y queda $1 = a^m = a^{2n} = b^{3n}$. Ahora, tenemos $b^{2n} = b^{3n} = 1$ lo que implica $b^n = 1$, que es una contradicción. Por lo tanto, el orden de a y b es impar. Esto significa, por la identidad de Bezout, que existen enteros s y t de manera que $1 = 2s + mt$. Por tanto $2s = 1 - mt$. Elevamos la relación $a^2 = b^3$ a s y queda $a = a^{2s+mt} = a^{2s} = b^{3s}$ de lo que se deduce que a y b conmutan. □

Proposición 3.4. *El grupo $BS(2,3) = \langle x, y | y^{-1}x^2y = x^3 \rangle$ no es residualmente finito.*

Demostración. El resultado quedará probado si encontramos un $1 \neq w \in N$ tal que $w \in N$ para todo $N \triangleleft G = BS(2,3)$ de índice finito. Para ello consideramos la palabra $w = [y^{-1}xy, x] = y^{-1}x^{-1}yx^{-1}y^{-1}xyx$. Al aplicar el lema de Britton, que en nuestro caso nos dice que si en una palabra $z \in G$ no hay una secuencia consecutiva de la forma $y^{-1}x^{2\alpha}y$ ó $yx^{3\alpha}y^{-1}$ con $\alpha \in \mathbb{Z}$, entonces $z \neq 1$. Obtenemos así que $w \neq 1$.

Veamos ahora que w pertenece a todos los grupos N normales y de índice finito en G. Sea N tal grupo, entonces G/N es finito y que $y^{-1}x^2yN = x^3N$ implica que $(y^{-1}xyN)^2 = y^{-1}x^2yN = (xN)^3$ luego tomando $a = y^{-1}xyN$ y $b = xN$ se sigue de (3.3) que $[y^{-1}xyN, xN] = N$ luego $w = [y^{-1}xy, x] \in N$. □

Observación 3.5. El grupo $BS(2,3)$ no es lineal. Pues de serlo sería residualmente finito.

Proposición 3.6. *El grupo $BS(2,3)$ tiene solución al problema de la palabra.*

Demostración. Sea w una palabra de G en términos de x, y. El lema de Britton, enunciado en la demostración anterior, nos dice que si no hay una secuencia consecutiva de la forma $y^{-1}x^{2\alpha}y$ ó $yx^{3\alpha}y^{-1}$ con $\alpha \in \mathbb{Z}$, entonces $w \neq 1$ con lo cual si no las hay, ya sabemos que $w \neq 1$ y en el caso de que las haya, aplicamos la relación $y^{-1}x^2y = x^3$ o su inversa $yx^3y^{-1} = x^2$ hasta obtener o $w = 1$ o bien una palabra en la que no hay secuencias consecutivas de la forma mencionada anteriormente. Esto se alcanzará en un número finito de iteraciones debido a que cada vez que aplico una relación obtengo una palabra más corta. □

Enunciamos ahora una serie de teoremas generales para saber si un grupo de Baumslag-Solitar es o no es residualmente finito.

Lema 3.7. *Si p y q no son potencias del mismo primo y son distintos en valor absoluto entre ellos o de* 1*, entonces, el grupo $BS(p,q)$ no es residualmente finito.*

Demostración. Ver [7, Lemma 2.1]. □

Lema 3.8. *Si p y q son distintos en valor absoluto entre ellos o de* 1 *y uno de ellos divide al otro, entonces el grupo $BS(p,q)$ no es residualmente finito.*

Demostración. Ver [7, Lemma 2.2]. □

Teorema 3.9. *El grupo $BS(p,q)$ es residualmente finito si y solo si $p = \pm 1$ ó $q = \pm 1$ ó $p = \pm q$.*

Demostración. Ver [7, Theorem C]. □

Capítulo 4

Un algoritmo para el problema de la palabra para grupos policíclicos

Como hemos visto anteriormente, emplear el algoritmo expuesto en la demostración de (1.13) no suele ser la forma más eficiente para resolver el problema de la palabra.

En este capítulo veremos un algoritmo sencillo y eficiente para comprobar si una palabra de un grupo policíclico es o no la identidad.

4.1 Presentación de un grupo policíclico

Sea G un grupo policíclico y $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G$ una cadena policíclica, es decir, una cadena de G cuyos factores son cíclicos no triviales. Para $1 \leq i \leq n$ podemos elegir $g_i \in G_i$ tal que $G_i = \langle g_i, G_{i-1} \rangle$. A la secuencia $(g_1, ..., g_n)$ la llamaremos *secuencia policíclica generadora* de G. Sea I el conjunto de los $i \in \{1, ..., n\}$ tales que $r_i := |G_i : G_{i-1}|$ es finito. Entonces cada elemento de G_i se puede poner de forma única como $g_i^{e_i} w_i$ con $0 \leq e_i < r_i$ y $w_i \in G_{i-1}$. Lo que nos induce a deducir que cada elemento de G podrá ser escrito de forma única como $g_1^{e_1} \cdots g_n^{e_n}$ con $e_i \in \mathbb{Z}$ para $1 \leq i \leq n$ y $0 \leq e_i < r_i$ para $i \in I$.

Proposición 4.1. *Para cada secuencia generadora de G tenemos una presentación, que llamaremos presentación potencia conjugada, con las siguientes relaciones:*

$$g_j^{g_i} = g_{i-1}^{e(i,j,i-1)} \cdots g_1^{e(i,j,1)} \text{ para } 1 \leq j < i \leq n,$$

$$g_j^{g_i^{-1}} = g_{i-1}^{f(i,j,i-1)} \cdots g_1^{f(i,j,1)} \text{ para } 1 \leq j < i \leq n,$$

$$g_i^{r_i} = g_{i-1}^{l(i,i-1)} \cdots g_1^{l(i,1)} \text{ para } i \in I.$$

Demostración. Sea $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G$ la cadena policíclica de G. Realizaremos la demostración por inducción sobre n. Para $n = 0$ es trivial. Supongámoslo cierto para $n-1$ y probémoslo para n.

Sabemos que G_{n-1} es policíclico y por hipótesis de inducción tiene una presentación potencia conjugada. Definiendo $I_n = \{k \in \{1, ..., n-1\} | r_k := |G_k : G_{k-1}| \text{ finito}\}$. Esta presentación tendrá las siguientes relaciones:

$$g_j^{g_k} = g_{k-1}^{e(k,j,k-1)} \cdots g_1^{e(k,j,1)} \text{ para } 1 \leq j < k \leq n-1,$$

$$g_j^{g_k^{-1}} = g_{k-1}^{f(k,j,k-1)} \cdots g_1^{f(k,j,1)} \text{ para } 1 \leq j < k \leq n-1,$$

$$g_k^{r_k} = g_{k-1}^{l(k,k-1)} \cdots g_1^{l(k,1)} \text{ para } k \in I_n.$$

Por otra parte, tenemos que $G_{n-1} \triangleleft G_n$ y G_n/G_{n-1} es cíclico luego existirá $g_n \in G_n$ tal que $G_n/G_{n-1} = \langle g_n G_{n-1} | g_n^{r_n} G_{n-1} = G_{n-1} \rangle$ con $r_n \in \mathbb{Z} \cup \{\infty\}$, si $r_n = \infty$ no habrá relación.

Luego se sigue de la demostración de (1.6) que G está generado por g_n y G_{n-1} con las siguientes relaciones:

(1). Las ya existentes en G_{n-1}.

(2). Si $r_n \neq \infty$, tenemos $g_n^{r_n} = g_{n-1}^{l(n,n-1)} \cdots g_1^{l(n,1)}$.

(3). Las relaciones de normalidad:

- $g_j^{g_n} = g_{n-1}^{f(n,j,i)} \cdots g_1^{f(n,j,1)}$ para $1 \leq j < n$.
- $g_j^{g_n^{-1}} = g_{n-1}^{l(n,j,n-1)} \cdots g_1^{l(n,j,1)}$ para $1 \leq j < n$.

Quedando probada la proposición para n. □

Una vez estudiada esta presentación, el procedimiento a seguir para ver si un elemento, dado en términos de una secuencia policíclica generadora de un grupo es la identidad o no, es bastante sencillo, veámoslo. Nos dan la palabra w que es un elemento de G y está escrita en potencias de la secuencia policíclica $(g_1, ..., g_n)$. El procedimiento a seguir será el siguiente:

Paso 1. Buscamos la potencia g_n más a la derecha de nuestra palabra.

Paso 2. Si tiene exponente $e_n \geq r_n$ procederemos a reducirlo. Para ello calcularemos q_n, s_n tales que $e_n = r_n q_n + s_n$ con $s_n < r_n$ y escribiremos $g_n^{e_n} = g_n^{s_n}(g_n^{r_n})^{q_n}$ ahora aplicamos reiteradamente la relación (2) a $(g_n^{r_n})^{q_n}$ obteniendo así que la potencia de g_n mas a la derecha de nuestra palabra tiene exponente $s_n < r_n$. Sin perdida de generalidad renombramos $e_n = s_m$.

Paso 3. Tenemos $g_n^{e_n}$ con $e_n < r_n$. Lo moveremos hacia la izquierda reiterando relaciones del tipo $g_j g_n^{e_n} = g_n^{e_n} g_{n-1}^{f'(n,,i)} \cdots g_i^{f'(n,j,1)}$ obtenidas por inducción a partir de las relaciones de tipo (3).

Obtendremos así que nuestro elemento habrá avanzado una posición hacia la izquierda. Realizaremos este procedimiento hasta que obtengamos que todos los g_n están a la izquierda. Una vez conseguido esto, procederemos con los g_{n-1} y así sucesivamente hasta llegar a los g_1. Al final del proceso nuestra palabra será de la forma $g_n^{e_n} \cdots g_1^{e_1}$ con $e_i \in \mathbb{Z}$ para $1 \leq i \leq n$ y $0 \leq e_i < r_i$ para $i \in I$. Una palabra de este tipo es la identidad en G si y solo si todos los exponentes son 0.

4.2 Presentación del grupo $UT(n, \mathbb{Z})$

En las siguientes lineas usaremos el método descrito en la sección anterior para dar una presentación del grupo policíclico $G = UT(n, \mathbb{Z})$ con n un entero positivo.

Lo primero es encontrar un cadena policíclica de G. Tomemos los siguientes conjuntos de G:

$$G_{1,n} = \left\{ \begin{pmatrix} 1 & 0 & \dots & 0 & a \\ \vdots & \ddots & \ddots & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix} \right\}, \quad G_{1,n-1} = \left\{ \begin{pmatrix} 1 & 0 & \dots & b & a \\ \vdots & \ddots & \ddots & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix} \right\},$$

$$G_{2,n} = \left\{ \begin{pmatrix} 1 & 0 & \dots & b & a \\ \vdots & \ddots & \ddots & & c \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix} \right\}, \quad G_{1,n-2} = \left\{ \begin{pmatrix} 1 & 0 & \dots & d & b & a \\ 0 & 1 & \ddots & & 0 & c \\ \vdots & & \ddots & \ddots & & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ \vdots & & & & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \right\}, \dots$$

Con $a,b,c,d,... \in \mathbb{Z}$.

Es decir $G_{i,j}$ es el conjunto de matrices unitriangulares con entradas nulas excepto posiblemente en los elementos $e_{k,l}$ (siendo k la fila del elemento y l la columna) con, o bien $l-k < j-i$, o bien $l-k = j-i$ y $i < k$.

De tal forma que $G_{i,j} \subset G_{k,l}$ si, o bien $l-k < j-i$, o bien $l-k = j-i$ y $i < k$ siempre y cuando $1 < i < j \leq n$ y $1 < k < l \leq n$.

Se puede ver fácilmente que estos subconjuntos son subgrupos de G y que forman un cadena policíclica $1 = G_0 \triangleleft G_{1,n} \triangleleft G_{1,n-1} \triangleleft G_{2,n} \triangleleft \cdots \triangleleft G_{n-2,n-1} \triangleleft G_{n-1,n} = G$ de longitud $(n-1)!$. Ahora tenemos que elegir $g_{i,j} \in G_{i,j}$ tal que $G_{i,j} = \langle g_{i,j}, G_{i-1,j-1} \rangle$ si $j \neq n$ ó $G_{i,j} = \langle g_{i,j}, G_{1,2+n-i} \rangle$ si $j = n$. Es fácil comprobar que las matrices $g_{i,j}$ definidas como matrices unitriangulares $n \times n$ con un 1 en la entrada de fila i y columna j y en el resto ceros, lo cumplen.

Tenemos así que nuestra secuencia policíclica generadora de G es $(g_{1,n}, g_{1,n-1}, g_{2,n-1}, g_{1,n-2}, \ldots, g_{n-2,n-1}, g_{n-1,n})$. Por otra parte todos los cocientes de nuestra cadena son infinitos luego no hay relaciones del tipo $g_k^{r_k} = g_{k-1}^{l(k,k-1)} \cdots g_1^{l(k,1)}$.

Vemos que en nuestro grupo las relaciones de la presentación potencia conjugada son relaciones del tipo $[g_{i,j}, g_{k,l}] = g_{m,t}$ con $1 \leq i < j \leq n$, $1 \leq k < l \leq n$ y $1 \leq m < t \leq n$. Veamos cuales son. Para ello lo primero es ver como se multiplican los elementos de nuestra secuencia policíclica. Sean dos elementos, $g_{i,j}$ y $g_{k,l}$. Tenemos que $g_{i,j}g_{k,l} = (I_n + E_{i,j})(I_n + E_{k,l}) = I_n + E_{i,j} + E_{k,l} + E_{i,j}E_{k,l}$ donde $E_{i,j}$ es la matriz $n \times n$ con ceros en todas las entradas y un uno en la entrad de fila i y columna j. El producto $E_{i,j}E_{k,l}$ es igual a la matriz nula si $j \neq k$ y es $E_{i,l}$ si $j = k$. Por otra parte el inverso de un elemento $g_{i,j} = I_n + E_{i,j}$ es $I_n - E_{i,j}$, en efecto, $(I_n + E_{i,j})(I_n - E_{i,j}) = I_n + E_{i,j} - E_{i,j} - E_{i,j}E_{i,j} = I_n$. Una vez conocido el resultado de estas operaciones veamos cuales son las relaciones.

$$\begin{aligned}
[g_{i,j}, g_{k,l}] &= g_{i,j}^{-1} g_{k,l}^{-1} g_{i,j}, g_{k,l} = (I_n - E_{i,j})(I_n - E_{k,l})(I_n + E_{i,j})(I_n + E_{k,l}) = \\
&= (I_n - E_{k,l} - E_{i,j} + E_{i,j}E_{k,l})(I_n + E_{k,l} + E_{i,j} + E_{i,j}E_{k,l}) = \\
&= I_n + E_{k,l} + E_{i,j} + E_{i,j}E_{k,l} - E_{k,l} - E_{k,l}E_{i,j} - E_{k,l}E_{i,j}E_{k,l} - E_{i,j} - E_{i,j}E_{k,l} + \\
&\quad + E_{i,j}E_{k,l} + E_{i.j}E_{k,l}E_{i,j} + E_{i,j}E_{k,l}E_{i,j}E_{k,l} = \\
&= I_n - E_{k,l}E_{i,j} - E_{k,l}E_{i,j}E_{k,l} + E_{i,j}E_{k,l} + E_{i,j}E_{k,l}E_{i,j} + E_{i,j}E_{k,l}E_{i,j}E_{k,l}
\end{aligned}$$

A partir de aquí tenemos varias posibilidades

- $j = k$. En cuyo caso $i < j = k < l$ luego, $i \neq l$. Tenemos $[g_{i,j}, g_{k,l}] = I_n - E_{k,l}E_{i,j} - E_{k,l}E_{i,l} + E_{i,l} + E_{i,l}E_{i,j} + E_{i,l}E_{i,l} = I_n + E_{i,l} = g_{i,l}$.
- $j \neq k$. Nos queda que $[g_{i,j}, g_{k,l}] = I_n - E_{k,l}E_{i,j}$.
  - $i = l$. $[g_{i,j}, g_{k,l}] = I_n - E_{k,j} = g_{k,j}^{-1}$. La cual es la misma relación que la obtenida antes debido a que esta relación implica que $g_{k,j} = [g_{k,l}, g_{i,j}]$.
  - $i \neq l$. $[g_{i,j}, g_{k,l}] = I_n = 1$.

Tenemos así que una presentación potencia-conjugada de nuestro grupo es la siguiente:

$$UT(n,\mathbb{Z}) = \left\langle g_{i,j} \text{ con } 1 \leq i < j < n \;\middle|\; \begin{array}{ll} [g_{i,j}, g_{k,l}] = 1 & \text{si } j \neq k,\ i \neq l \text{ con } 1 \leq i < j \leq n,\ 1 \leq k < l \leq n \\ [g_{i,j}, g_{j,l}] = g_{i,l} & \text{si } 1 \leq i < j < l \leq n \end{array} \right\rangle.$$

Bibliografía

[1] BAUMSLAG, GILBERT, GILDENHYS, DION, STREBEL, RALPH, *Algorithmically insoluble Problems about Finitely Presented Solvable Groups, Lie and Associative Algebras, II*, Journal of algebra 97, 278-285 (1985).

[2] DEHN, MAX, *Über unendliche diskontinuierliche Gruppen*, Mathematische Annalen 71 (1): 116-144 (1911).

[3] EICK, BETTINA, HORN, MAX, NICKEL, WERNER, *Polycyclic*, Version 2.11 (2013).

[4] HALL, PHILIP, *On the Finiteness of Certain Soluble Groups*, Proc. London Math. Soc. (1959) s3-9: 595-622.

[5] LENNOX, JOHN C., ROBINSON, DEREK J. S., *The Theory of Infinite Soluble Groups*, Oxford Mathematical monographs (2004).

[6] LYNDON, ROGER C., SCHUPP, PAUL E., *Combinatorial Group Theory*, Springer, 1977.

[7] MESKIN, STEPHEN, *Nonresidually Finite One-Relator Groups*, transactions of the American Mathematical Society 164 (1972): 105-14.

[8] NAVARRO, GABRIEL, *Un curso de álgebra*, Universitat de València (2002).

[9] ROBINSON, DEREK J.S., *A course in the Theory of Groups*, Second edidition, Graduate texts in Mathematics (1996).

[10] ROTMAN, JOSEPH J., *An Introduction to the Theory of Groups*, Springer-Verlag. Fourth edition. (1995).

[11] STILLWELL, JOHN, *The Word Problem and the Isomorphic Problem for Groups*, Bulletin (New Series) of the American Mathematical Society. Volume 6, Number 1, 33-56(1982).

[12] WEHRFRITZ, B. A. F., *Infinite Linear Groups. An Account of the Group theoretic Properties of Infinite Groups of Matrices*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 76. Springer-Verlag, New York and Heidelberg. (1973).