UNIVERSIDAD DE OVIEDO

TRABAJO FIN DE MÁSTER:

INTRODUCCIÓN A LA TEORÍA COMBINATORIA DE GRUPOS

Isabel Fernández Martínez

Máster en Modelización e Investigación Matemática,
Estadística y Computación

Julio 2014

INTRODUCCIÓN A LA TEORÍA COMBINATORIA DE GRUPOS

Por Isabel Fernández Martínez

Realizado bajo la dirección de Consuelo Martínez López

Índice general

Introducción **3**

1. Una introducción a la teoría combinatoria de grupos **5**

1.1. El concepto de presentación de un grupo. Generadores y relaciones. 5

1.2. Las transformaciones de Tietze. 17

1.3. Grupos libres. 20

1.4. Los problemas de Dehn. 24

1.5. Grupos cociente. 28

1.6. Una aproximación alternativa al concepto de presentación de un grupo. 29

1.7. Presentaciones de subgrupos. 31

2. Producto libre y producto amalgamado de grupos. **37**

2.1. Producto libre de grupos. 37

2.2. Producto amalgamado de grupos 45

3. Grupos presentados con una única relación. **58**

3.1. El teorema de la independencia. Consecuencias. 58

3.2. El problema de la palabra para grupos presentados con una única relación. . . 68

4. Algunos desarrollos recientes sobre el problema de la palabra **76**

5. Algunas aplicaciones **84**

5.1. Protocolos de intercambio de claves. 84

5.1.1. El esquema de Anshel, Anshel y Goldfeld. 85

5.1.2. El esquema de Ko-Lee-Cheon-Han-Khan-Park. 86

5.2. Criptosistemas basados en problemas de la palabra y de la conjugación 87

5.2.1. El criptosistema de Wagner y Magyarik 89

5.2.2. El criptosistema de Garzón y Zalcstein 91

Conclusiones **93**

Bibliografía **94**

Introducción

La teoría combinatoria de grupos se puede ver como el estudio de los grupos dados mediante generadores y relaciones o, como diríamos hoy en día, mediante una presentación.

Desde que, en 1882, Dyck introdujo la idea de generadores y relaciones, la teoría combinatoria de grupos se ha desarrollado, en muchos casos de la mano de problemas topológicos, que a medida que se iban estudiando, demandaban un soporte algebraico que ayudase a formalizar nuevos conceptos topológicos. En 1908, Tietze publicó un artículo de 118 páginas que comienza con una definición de variedad e introduce el grupo fundamental de una variedad, probando que tiene una presentación finita. Demuestra también que es un invariante topológico, para lo que utiliza un resultado puramente algebraico, recogido también en el mismo artículo, que afirma que dos presentaciones finitas de un grupo pueden transformarse una en otra aplicando un número finito de veces las tranformaciones que hoy en día se conocen como transformaciones de Tietze.

En 1911 Dehn publicó un artículo que no sólo comienza con la formulación de tres de los problemas de decisión más conocidos en teoría de grupos (problema de la palabra, de la conjugación y del isomorfismo), sino que además se da una motivación topológica para su planteamiento. Haciendo corresponder a cada nudo K un grupo infinito G_K dado mediante una presentación finita, Dehn motiva el problema de la palabra argumentando que K no está anudado si y sólo si G_K es abeliano, lo que requiere la solución del problema de la palabra, que consiste en determinar si una palabra en los generadores de un grupo define o no el elemento neutro, o equivalentemente, si dos palabras definen el mismo elemento.

Además, la cuestión de si un nudo K' se puede deformar para obtener K requiere la solución del problema del isomorfismo para G_K y $G_{K'}$.

Fue sobre todo la topología la motivadora e impulsora de la teoría combinatoria de grupos, ejerciendo un efecto estimulante para su desarrollo que fue especialmente intenso hasta aproximadamente el final de la Primera Guerra Mundial, en 1918, cuando comenzaron a aparecer artículos publicados por Nielsen en los que se empezaron a investigar y resolver problemas en teoría combinatoria de grupos sin una obvia dependencia de problemas topológicos o de otros campos. Sin que ésto signifique que cesase su influencia, la teoría combinatoria de

grupos comenzó a desarrollar sus propios problemas y sus propios métodos.

Esta memoria se organiza en cinco capítulos estructurados como se describe a continuación. El primero de ellos tiene una finalidad introductoria. En él se describen las primeras nociones sobre teoría combinatoria de grupos, comenzando por definir de manera formal qué se entiende por presentación de un grupo y en qué sentido un conjunto de símbolos y un conjunto de palabras en los mismos determinan, salvo isomorfismo, un único grupo. Se describe también la presentación de subgrupos y cocientes de un grupo G a partir de la presentación de G, y se introducen los ya mencionados problemas de Dehn.

El segundo capítulo se centra en construcciones básicas de grupos a partir de otros. Concretamente, se estudian el producto libre y el producto amalgamado de grupos, que serán herramientas útiles en el estudio de los grupos presentados con una única relación, el cual se aborda en el tercer capítulo.

A lo largo de esta primera parte de la memoria, nos encontramos como tema recurrente la solución del problema de la palabra para distintas clases de grupos, como los grupos libres en el primer capítulo o los grupos dados por una sola relación en el tercero. Se destaca también en la sección 2.1 que para resolver el problema de la palabra en productos libres de grupos se requiere la solución de dicho problema en cada uno de los factores.

Es precisamente en este primer problema de Dehn en el que nos centraremos de forma más específica en los dos últimos capítulos, dedicados respectivamente, a recopilar y enfatizar algunos resultados recientes sobre el problema de la palabra, y a destacar cómo dicho problema de decisión puede emplearse para la construcción de criptosistemas de clave pública o de esquemas de intercambio de claves.

Resulta interesante resaltar cómo los problemas de decisión en teoría de grupos, que surgieron motivados por su aplicación a la resolución de cuestiones topológicas, han evolucionado (principalmente por efecto del desarrollo de las ciencias de la computación) hasta convertirse en puntos de encuentro entre la propia teoría combinatoria de grupos, la teoría de grafos y la teoría de complejidad algorítmica.

Fue precisamente el desarrollo de ésta última el que permitió el estudio de estos problemas bajo una perspectiva computacional. Los resultados en este campo han atraído la atención por las potenciales aplicaciones de la teoría combinatoria de grupos a la criptografía, tema que se esboza brevemente en el último capítulo de esta memoria.

Capítulo 1

Una introducción a la teoría combinatoria de grupos

1.1. El concepto de presentación de un grupo. Generadores y relaciones.

Cuando se trabaja con grupos, una manera sencilla de describir un grupo (al menos en el caso de orden finito) es enumerar sus elementos y escribir la tabla de multiplicación. Por ejemplo, si consideramos A_3 (el grupo alternado de grado 3), podemos describirlo enumerando sus elementos:

$$A_3 = \{1, (1,2,3), (1,3,2)\}$$

y con una tabla que indique cómo se multiplica cada par de elementos.

$\cdot$	1	$(1,2,3)$	$(1,3,2)$
1	1	$(1,2,3)$	$(1,3,2)$
$(1,2,3)$	$(1,2,3)$	(1,3,2)	1
$(1,3,2)$	$(1,3,2)$	1	$(1,2,3)$

Sin embargo, este método es inviable para grupos infinitos y altamente ineficiente para grupos finitos de orden suficientemente grande.

Otra forma de describir A_3 es darse cuenta de que A_3 es un grupo cíclico de orden 3. Esta forma de describirlo consiste en considerar un generador del grupo, por ejemplo $(1,2,3)$, que tendrá orden 3. Así, $A_3 = \langle (1,2,3) \rangle$.

Si a representa el 3-ciclo $(1,2,3)$, entonces $a^3 = 1$. Podemos preguntarnos entonces si para describir A_3 (salvo isomorfismo) bastará con decir que está generado por un elemento que cumple que al elevarlo al cubo se obtiene el elemento neutro. Tal como está formulada

la pregunta, la respuesta es claramente negativa pues el grupo trivial $G = 1$ también cumple esto y no es isomorfo a un cíclico de orden 3. No obstante, hay una diferencia clara entre ambas situaciones: en el caso de $G = 1$ es imposible obtener, sabiendo simplemente que la potencia tercera del generador es 1, que dicho generador ha de ser necesariamente trivial. Sin embargo, en el caso de A_3 (cíclico de orden 3) toda relación que se cumple en el grupo se puede derivar del hecho de que $a^3 = 1$. En efecto, si en $A_3(\cong C_3)$ tenemos una relación, como el grupo es cíclico, todo elemento es potencia del generador a, luego la relación tomará la forma:

$$a^\alpha = a^\beta$$

que es equivalente a

$$a^{\alpha-\beta} = 1$$

Como $a^3 = 1$ tenemos que $a^{-1} = a^2$, de modo que la relación que tenemos se puede transformar en una relación en la que el exponente que intervenga sea no negativo. Además, de la relación $a^3 = 1$, también obtenemos que el exponente de a se puede reducir módulo 3, de modo que la relación que teníamos se transforma en

$$a^\epsilon = 1 \text{ con } \epsilon \in \{0, 1, 2\}$$

Pero si ϵ fuese 1 ó 2 entonces el lado izquierdo de la relación sería a o a^2, respectivamente. Sin embargo, a representa el 3-ciclo $(1, 2, 3)$ y a^2 representa el 3-ciclo $(1, 3, 2)$ y ninguno de ellos es trivial en A_3. De modo que necesariamente $\epsilon = 0$ y la relación es $1 = 1$.

Realizando los mismos pasos pero en orden inverso podemos derivar la relación $a^\alpha = a^\beta$ a partir de $a^3 = 1$, es decir, toda relación en $A_3(\cong C_3)$ se puede derivar de $a^3 = 1$.

Veamos otro ejemplo. Consideremos V el cuatro grupo de Klein formado por las funciones de $\mathbb{R}\backslash\{0\}$ en $\mathbb{R}\backslash\{0\}$ dadas por $f_1(x) = x, f_2(x) = -x, f_3(x) = 1/x, f_4(x) = -1/x$ con la ley de composición de aplicaciones. Denotaremos f_1, f_2, f_3, f_4 simplemente por $x, -x, 1/x, -1/x$. Las funciones $-x, 1/x$ generan V. Si a representa $-x$ y b representa $1/x$ entonces se tiene $a^2 = 1$, $b^2 = 1$, $ab = ba$ (aquí el elemento neutro de V, denotado por 1, es x). En V se verifican también otras relaciones además de éstas, por ejemplo, se cumple $a^3 = a$, $(ab)^2 = 1$,... pero todas ellas se pueden derivar de las tres relaciones anteriores y de relaciones que se verifican en todo grupo, por ejemplo, $aa^{-1} = 1$, $a1 = a$,... Suponiendo

$$a^{\alpha_1} b^{\beta_1} \dots a^{\alpha_r} b^{\beta_r} = a^{\gamma_1} b^{\delta_1} \dots a^{\gamma_s} b^{\delta_s} \tag{1.1}$$

es una relación que se verifica en V, se tiene que la relación 1.1 es equivalente a

$$a^{\alpha_1} b^{\beta_1} \dots a^{\alpha_r} b^{\beta_r - \delta_s} a^{-\gamma_s} \dots b^{-\delta_1} a^{-\gamma_1} = 1 \tag{1.2}$$

Usando que $a^2 = 1, b^2 = 1$ podemos deducir que $a = (a^2)a^{-1} = 1a^{-1} = a^{-1}$ y de igual forma $b = b^{-1}$. Por tanto 1.2 se puede transformar en una relación equivalente en la que todos los exponentes sean no negativos. Además, usando de nuevo $a^2 = 1, b^2 = 1$ podemos lograr que todos los exponentes de la relación sean 0 o 1 reduciéndolos módulo 2. Como en todo grupo $a^0 = b^0 = 1$, cualquier símbolo a o b que aparezca con exponente 0 se puede eliminar. Por último, usando la relación $ab = ba$ (y reduciendo los exponentes módulo 2 tantas veces como sea necesario), obtenemos la relación equivalente

$$a^{\epsilon_1} b^{\epsilon_1} = 1 \tag{1.3}$$

donde ϵ_1, ϵ_2 son 0 o 1. Pero si ϵ_1 ó ϵ_2 fuesen 1, el lado izquierdo de la relación 1.3 sería a, b o ab, que representan las funciones $-x, 1/x, -1/x$, respectivamente. Ninguno de ellos representa la función identidad x. Por tanto, ha de ocurrir $\epsilon_1 = \epsilon_2 = 0$, luego 1.3 se reduce a $1 = 1$. Realizando los mismos pasos pero en orden inverso podemos derivar la relación 1.1 a partir de $a^2 = 1, b^2 = 1, ab = ba$.

El 4-grupo de Klein es, por tanto, un grupo generado por dos elementos a, b que satisfacen las relaciones $a^2 = 1, b^2 = 1, ab = ba$ y en el que toda relación se puede derivar de éstas tres.

Así, podemos considerar la posibilidad de describir un grupo mediante símbolos generadores y ciertas relaciones que cumplan estos símbolos a partir de las cuales se pueda derivar cualquier otra relación del grupo.

Antes de continuar, es necesario formalizar el concepto de "relación" y dar más precisión a la expresión "una relación es derivable de unas relaciones dadas".

Consideremos un conjunto de símbolos $X = \{a, b, c, \dots\}$ y formemos un nuevo conjunto de simbolos $X' = \{a^{-1}, b^{-1}, c^{-1}, \cdots\}$ disjunto y biyectivo con el anterior. Una palabra W en los símbolos $a, b, c, \dots$ es una secuencia finita

$$f_1, f_2, \cdots, f_n \tag{1.4}$$

donde cada $f_\nu \in X \cup X'$.

Llamaremos longitud de la palabra, y lo denotaremos $L(W)$, al entero n. Consideraremos también la palabra vacía (que denotaremos por 1) y diremos que su longitud es 0.

Si queremos hacer explícitos en la notación los símbolos que intervienen en W, escribiremos $W(a, b, c, \dots)$. Para simplificar la notación escribiremos la secuencia (1.4) sin las comas, de la manera

$$f_1 f_2 \cdots f_n \tag{1.5}$$

Así, por ejemplo,

$$aabb^{-1}c^{-1} \tag{1.6}$$

es una palabra en los símbolos a, b y c de longitud 5. Por otra parte,

$$aac^{-1} \tag{1.7}$$

es una palabra en los símbolos a, b y c de longitud 3, y es también una palabra en los símbolos a y c de longitud 3. Pero (1.6) y (1.7) no son la misma palabra. De hecho, consideraremos que dos palabras $f_1 f_2 \cdots f_n$ y $g_1 g_2 \cdots g_m$ son iguales si y sólo si $n = m$ y $f_\nu = g_\nu \ \forall \nu \in \{1 \cdots, n\}$. La palabra vacía 1 la podemos ver como una palabra de longitud cero en cualesquiera símbolos.

Habitualmente abreviaremos una secuencia de k símbolos idénticos consecutivos f_ν de la forma f_ν^k. Así, por ejemplo, la palabra (1.6) también la podemos reescribir de la forma $a^2bb^{-1}c^{-1}$, y la palabra (1.7) de la forma a^2c^{-1}. Del mismo modo, la palabra $b^{-1}b^{-1}a$ se puede reescribir como $(b^{-1})^2a$. Además, si $f_\nu \in X$ y k es un entero negativo, usaremos la notación f_ν^k para indicar $(f_\nu^{-1})^{-k}$, de modo que $b^{-2}a$ es la misma palabra que $(b^{-1})^2a$.

Llamaremos palabra inversa de la palabra W dada en (1.5) (y la denotaremos por W^{-1}) a la palabra

$$f_n^{-1} \cdots f_2^{-1} f_1^{-1}$$

donde si f_ν es a ó a^{-1} entonces f_ν^{-1} denota a^{-1} ó a, respectivamente, y análogamente en caso de que f_ν sea uno de los símbolos b ó b^{-1}, c ó c^{-1}, ...

Por ejemplo, la palabra inversa de la palabra (1.6) es $cbb^{-1}a^{-1}a^{-1}$, y la palabra inversa de la palabra (1.7) es $ca^{-1}a^{-1}$.

Por otra parte, diremos que la palabra inversa de la palabra vacía es ella misma, es decir, $1^{-1} = 1$.

Es claro que $L(W^{-1}) = L(W)$ y que $(W^{-1})^{-1} = W$.

Si W es la palabra $f_1 f_2 \cdots f_n$ y U es la palabra $f_1' f_2' \cdots f_m'$, definimos el producto de W y U (y lo denotaremos WU) como la palabra construida mediante yuxtaposición de W y U, es decir, $f_1 f_2 \cdots f_n f_1' f_2' \cdots f_m'$. Por ejemplo, si W es la palabra (1.6) y $U = bc^2$, entonces $WU = a^2bb^{-1}c^{-1}bc^2$ y $UW = bc^2a^2bb^{-1}c^{-1}$. En este ejemplo se observa claramente que el producto de palabras no es conmutativo en general. Por otra parte, es claro a partir de la definición que $L(WU) = L(W) + L(U)$, de modo que lo que sí se cumple en general es $L(WU) = L(UW)$. También resulta obvio que $(WU)^{-1} = U^{-1}W^{-1}$.

Es importante destacar que el conjunto de palabras en los símbolos $a, b, c, \ldots$ con la ley de yuxtaposición no forma un grupo pues no toda palabra tiene inverso (en el sentido de inverso en un grupo). Sería natural pensar que la palabra que hemos denotado W^{-1} (y de hecho, hemos llamado palabra inversa) es el inverso de W, pero esto no es cierto pues no se cumple que $WW^{-1} = W^{-1}W = 1$ salvo que W sea la palabra vacía. Sólo la palabra vacía tiene inverso. Ello se debe a que, si W es una palabra tal que existe otra palabra U cumpliendo

$WU = UW = 1$, entonces se tiene $L(WU) = L(W) + L(U) = L(1) = 0$; pero la longitud de una palabra es siempre un número entero no negativo, de modo que $L(W) = 0$, es decir, W es la palabra vacía.

Usaremos las palabras para representar, de manera formal, un producto de elementos en un grupo. Dada una aplicación α de un conjunto de símbolos $X = \{a, b, c, \dots\}$ en un grupo G de tal manera que $\alpha(a) = g$, $\alpha(b) = h$, $\alpha(c) = k$, $\dots$, consideramos el conjunto X' tal como lo definíamos anteriormente. Diremos entonces que (bajo α) a define g, b define h, c define k, $\dots$, a^{-1} define g^{-1}, b^{-1} define h^{-1}, c^{-1} define k^{-1}, $\dots$; más aun, si W es la palabra (1.5), entonces diremos que W define el elemento (denotado $W(g, h, k, \dots)$) de G dado por el producto $g_1 g_2 \cdots g_n$ donde f_ν define g_ν. Diremos, además, que la palabra vacía 1 define el elemento neutro 1 de G.

Claramente, si las palabras U y V definen los elementos p y q de G, entonces U^{-1} define p^{-1} y UV define pq.

Si todo elemento de G está definido por una palabra en los símbolos $a, b, c, \dots$ diremos que $a, b, c, \dots$ son símbolos generadores de G (bajo la aplicación α) y que $g, h, k, \dots$ son elementos generadores de G. Si el contexto lo deja claro, nos referiremos a ambos indistintamente como generadores de G. Por ejemplo, consideremos como antes G el 4-grupo de Klein formado por las funciones $x, -x, 1/x, -1/x$ donde la ley del grupo viene dada por la composición de aplicaciones. Y consideremos la aplicación

$$\alpha_1 : \{a, b\} \to G$$

$$a \to -x$$

$$b \to 1/x$$

Entonces la palabra a^2 define x (que es el elemento neutro de G) y la palabra ab define $-1/x$, por tanto a, b son símbolos generadores de G (bajo α_1). Sin embargo, a y b no son símbolos generadores de G bajo la aplicación α_2 dada por $\alpha_2(a) = x, \alpha_2(b) = -x$.

En adelante supondremos que $a, b, c, \dots$ son símbolos generadores de G bajo una aplicación α.

Una palabra $R(a, b, c \dots)$ que define el elemento neutro en G se dirá relator. Una ecuación de la forma $R(a, b, c, \dots) = S(a, b, c, \dots)$ se dirá relación si RS^{-1} es un relator, es decir, si R y S definen el mismo elemento en G.

Las palabras 1, $aa^{-1}, a^{-1}a, bb^{-1}, b^{-1}b, cc^{-1}, c^{-1}c \dots$ siempre son relatores. Los llamaremos relatores triviales.

Una palabra W se dirá derivable de los relatores $P, Q, R, \dots$ si W se puede transformar en la palabra vacía aplicando un número finito de veces las siguientes operaciones:

1. Insertar alguna de las palabras $P, P^{-1}, Q, Q^{-1}, R, R^{-1}, \dots$ o alguno de los relatores triviales entre dos símbolos consecutivos de W, al principio de W o al final de W.

2. Eliminar las palabras $P, P^{-1}, Q, Q^{-1}, R, R^{-1}, \dots$ o un relator trivial en caso de que forme un bloque de símbolos consecutivos en W.

Obviamente, si W es una palabra derivable de los relatores $P, Q, R, \dots$, entonces la propia palabra W es un relator, puesto que las operaciones 1. y 2. aplicadas a una palabra no cambian el elemento del grupo que define la palabra y, como se alcanza la palabra vacía, W debe definir el elemento neutro de G.

Habiendo definido lo que significa que una palabra sea derivable de unos relatores dados, podemos dar la siguiente definición:

Se dice que una relación $W = V$ es derivable de las relaciones $P_1 = P_2,\ Q_1 = Q_2,\ R_1 = R_2, \dots$ si la palabra WV^{-1} es derivable de los relatores $P_1P_2^{-1},\ Q_1Q_2^{-1},\ R_1R_2^{-1}, \dots$ Por ejemplo, la relación $ab^{-1} = a^2ba$ es derivable de las relaciones $a^2 = 1, b^2 = 1, ab = ba$ pues aplicando operaciones del tipo 1 y 2 obtenemos la siguiente secuencia de palabras, que alcanza la palabra vacía: $ab^{-1}a^{-1}b^{-1}a^{-2}, ab^2b^{-1}a^{-1}b^{-1}a^4a^{-2}, aba^{-1}b^{-1}a^2, aba^{-1}b^{-1}, 1$.

Si $P, Q, R, \dots$ son relatores en G y todo relator de G se puede derivar de $P, Q, R, \dots$, diremos que $P, Q, R, \dots$ forman un conjunto completo de relatores de G en los generadores $a, b, c, \dots$ bajo la aplicación α. Si $P, Q, R, \dots$ es un conjunto completo de relatores para G en los generadores $a, b, c, \dots$ entonces diremos que

$$\langle a, b, c, \dots ; P(a, b, c, \dots), Q(a, b, c, \dots), R(a, b, c, \dots), \dots \rangle$$

es una presentación de G y escribiremos

$$G = \langle a, b, c, \dots ; P, Q, R, \dots \rangle.$$

Un grupo G se dirá finitamente generado si existe una presentación de G con un número finito de generadores, finitamente relacionado si existe una presentación con un conjunto completo de relatores finito, y finitamente presentado si existe una presentación de G con un número finito de generadores y un conjunto completo de relatores finito.

Aunque hemos definido las presentaciones de grupos de tal manera que en ellas aparezcan generadores y relatores, también es frecuente encontrar presentaciones escritas de forma que en ellas aparezcan generadores y relaciones, o bien generadores, relatores y relaciones. Por ejemplo, la presentación

$$\langle a, b; a^3, b^2, b^{-1}aba \rangle$$

también se puede escribir usando sólo relaciones en la forma

$$\langle a, b; a^3 = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$$

o usando relatores y relaciones en la forma

$$\langle a, b; a^3, b^2, b^{-1}ab = a^{-1} \rangle.$$

Llegados a este punto, surgen de manera natural dos preguntas.

- ¿Todo grupo posee alguna presentación?
- Dada una presentación cualquiera, ¿siempre existe algún grupo que se puede describir mediante dicha presentación? En caso afirmativo, ¿cuántos grupos (salvo isomorfismo) hay que se puedan describir mediante dicha presentación?

A continuación nos centraremos en contestar ambas preguntas.

La respuesta a la primera pregunta es afirmativa, de hecho, dado cualquier grupo G podemos tomar un símbolo generador diferente para cada uno de los elementos de G, y como relaciones, todas las que se verifiquen en G.

Otra presentación de G se obtiene a partir de su tabla de multiplicación de la siguiente manera: consideremos un símbolo generador diferente para cada uno de los elementos de G y como relatores tomemos todas las palabras de longitud 3 de la forma abc^{-1} donde el producto en G del elemento definido por a y el elemento definido por b es el elemento definido por c. Obviamente, tales palabras son relatores en G pues definen el elemento neutro. Además, todo relator en G se puede derivar de los anteriores. En efecto, sea W el relator $f_1 f_2 \dots f_n$. Podemos eliminar los exponentes negativos de W de la siguiente manera: supongamos que aparece b^{-1} en W, puesto que hay un símbolo generador (por ejemplo, c) tal que define el mismo elemento que b^{-1}, entonces la palabra bce^{-1} es uno de los relatores que consideramos en la presentación (e es el símbolo que define el elemento neutro). Insertemos bce^{-1} a la derecha de b^{-1} y eliminemos el relator trivial $b^{-1}b$ obteniendo ce^{-1}. Ahora, insertemos a la derecha de ce^{-1} el relator eee^{-1} y eliminemos los relatores triviales $e^{-1}e$ y ee^{-1}, obteniendo c. Repitiendo este procedimiento tantas veces como sea necesario, podemos eliminar todos los exponentes negativos en W. A continuación, vamos a reducir la longitud de W. Si a y d son símbolos consecutivos en W, busquemos el relator adq^{-1} e insertemos a la derecha de d el relator trivial $q^{-1}q$, eliminando a continuación el relator adq^{-1}, de manera que obtenemos q. Repitiendo este procedimiento llegaremos a reducir la longitud de W hasta un único símbolo, que (puesto que ha de definir el elemento neutro) ha de ser e. Insertando el relator trivial ee^{-1} a la derecha de e y eliminado eee^{-1} obtenemos la palabra vacía, es decir, el relator W es derivable de los relatores que hemos considerado en la presentación, de manera que éstos constituyen un conjunto completo de relatores.

A partir de la presentación derivada de la tabla de multiplicación resulta obvio que todo grupo finito es finitamente presentado. No obstante, esta presentación suele contener mucha información redundante.

Respecto a la segunda cuestión, veamos que, dada una presentación, siempre existe un grupo que se describe por ella y, además, es único salvo isomorfismo.

Dada una presentación

$$\langle a, b, c, \ldots ; P, Q, R, \ldots \rangle$$

buscamos construir un grupo descrito por dicha presentación. Para ello introducimos la siguiente relación de equivalencia: dos palabras W_1 y W_2 se dirán equivalentes (y se denotará $W_1 \sim W_2$) si las siguientes operaciones, aplicadas un número finito de veces, transforman W_1 en W_2.

1. Insertar una de las palabras $P, P^{-1}, Q, Q^{-1}, R, R^{-1}, \ldots$ o uno de los relatores triviales entre dos símbolos consecutivos de W_1, al principio de W_1 o al final de W_1.

2. Eliminar una de las palabras $P, P^{-1}, Q, Q^{-1}, R, R^{-1}, \ldots$ o uno de los relatores triviales en caso de que formen un bloque de símbolos consecutivos en W_1.

La relación $\sim$ es de equivalencia.

- Es reflexiva ($W \sim W$), pues W puede transformarse en ella misma insertando la palabra vacía, que es un relator trivial.

- Es simétrica ($W_1 \sim W_2$ implica $W_2 \sim W_1$), pues las operaciones que se llevan a cabo para transformar W_1 en W_2 se pueden realizar a la inversa para transformar W_2 en W_1.

- Es transitiva ($W_1 \sim W_2$ y $W_2 \sim W_3$ implica $W_1 \sim W_3$), pues W_1 se puede transformar en W_2 y después ésta en W_3 en un número finito de pasos, lo que permite transformar W_1 en W_3 en un número finito de pasos.

Además, se cumple que

$$W_1 \sim W_2 \text{ y } W_3 \sim W_4 \text{ implica } W_1 W_3 \sim W_2 W_4 \tag{1.8}$$

ya que primero podemos transformar $W_1 W_3$ en $W_2 W_3$ y despúes ésta en $W_2 W_4$.

La clase de equivalencia de una palabra W se denotará $\{W\}$. Definimos el producto de clases de la siguiente manera:

$$\{W_1\}\{W_2\} = \{W_1 W_2\} \tag{1.9}$$

Esta ley está bien definida en el conjunto cociente gracias a (1.8).

A continuación, probaremos que el conjunto de clases de equivalencia bajo esta relación con la ley de multiplicación (1.9) es el grupo (único salvo isomorfismo) definido por la presentación $\langle a, b, c, \dots ; P, Q, R, \dots \rangle$.

Teorema 1.1.1 El conjunto G de clases de equivalencia de palabras en $a, b, c, \dots$ bajo la relación $\sim$ es un grupo con el producto definido en (1.9). Más aun, bajo la aplicación

$$a \to \{a\}, b \to \{b\}, c \to \{c\}, \dots \tag{1.10}$$

G tiene la presentación

$$\langle a, b, c, \dots ; P(a, b, c, \dots), Q(a, b, c, \dots), R(a, b, c, \dots), \dots \rangle. \tag{1.11}$$

Además, si G' es un grupo con la presentación (1.11), entonces G' es isomorfo a G.

Demostración: Veamos primero que G es un grupo.

La ley en G es asociativa por serlo la yuxtaposición de palabras:

$$(\{W_1\}\{W_2\})\{W_3\} = \{W_1W_2\}\{W_3\} = \{(W_1W_2)W_3\} =$$

$$= \{W_1(W_2W_3)\} = \{W_1\}\{W_2W_3\} = \{W_1\}(\{W_2\}\{W_3\}).$$

La clase $\{1\}$ es el elemento neutro en G por (1.9).

El inverso de la clase $\{W\}$ es la clase $\{W^{-1}\}$, es decir,

$$\{W\}^{-1} = \{W^{-1}\} \tag{1.12}$$

ya que $\{W\}\{W^{-1}\} = \{WW^{-1}\}$ y mediante eliminación de relatores triviales WW^{-1} puede transformarse en la palabra vacía, es decir, $WW^{-1} \sim 1$, de modo que $\{WW^{-1}\} = \{1\}$. Análogamente, $\{W^{-1}\}\{W\} = \{1\}$, por tanto todo elemento de G tiene inverso.

Una vez visto que G es un grupo, veamos que tiene la presentación (1.11) bajo la aplicación (1.10). Primero probemos que $a, b, c, \dots$ son generadores de G. Gracias a (1.9) y (1.12), tenemos

$$W(\{a\}, \{b\}, \{c\}, \dots) = \{W(a, b, c, \dots)\}. \tag{1.13}$$

Así, bajo (1.10), la palabra $W(a, b, c, \dots)$ define la clase $\{W(a, b, c, \dots)\}$ y, por tanto, $a, b, c, \dots$ son símbolos generadores de G.

Probemos ahora que $P, Q, R, \dots$ es un conjunto completo de relatores para G. La clase definida por $P(a, b, c, \dots)$ bajo (1.10) es, por (1.13), la clase $\{P(a, b, c, \dots)\}$. Pero por eliminación de P, P se puede transformar en la palabra vacía, luego $P \sim 1$ y $\{P\} = \{1\}$, el elemento neutro de G. Por tanto, haciendo lo mismo para $Q, R, \dots$, obtenemos que $P, Q, R, \dots$ son relatores. Supongamos ahora que $S(a, b, c, \dots)$ es cualquier relator en G. Entonces, por

(1.13), S define la clase $\{S(a,b,c,\dots)\}$, que debe ser $\{1\}$. Por tanto, $S \sim 1$, luego S se puede transformar en la palabra vacía mediante las operaciones 1 y 2. Luego S es derivable de los relatores $P, Q, R, \dots$. Por tanto, $P, Q, R, \dots$ forman un conjunto completo de relatores para G.

Sólo nos falta probar la última afirmación del teorema. Supongamos que G' tiene la presentación (1.11) bajo la aplicación

$$a \to g', b \to h', c \to k', \dots$$

Probaremos que la aplicación

$$\{W(a,b,c,\dots)\} \to W(g',h',k',\dots) \tag{1.14}$$

es un isomorfismo de G en G'.

Veamos primero que la aplicación (1.14) está bien definida, es decir, que si $W_1 \sim W_2$ entonces $W_1(g',h',k',\dots) = W_2(g',h',k',\dots)$. Pero si $W_1 \sim W_2$, entonces $W_1 W_2^{-1}$ se puede transformar en $W_2 W_2^{-1}$ y después en la palabra vacía mediante las operaciones 1 y 2. Por tanto, $W_1 W_2^{-1}$ es derivable de $P, Q, R, \dots$ y por tanto es un relator en G', de modo que $W_1(g',h',k',\dots) = W_2(g',h',k',\dots)$.

A continuación, probaremos que la aplicación es biyectiva. Es suprayectiva puesto que $a, b, c, \dots$ son generadores de G'. Para ver que es inyectiva supongamos que $W_1(g',h',k',\dots) = W_2(g',h',k',\dots)$. Entonces $W_1 W_2^{-1}$ es un relator en G' y, como G' tiene la presentación (1.11), $W_1 W_2^{-1}$ es derivable de $P, Q, R, \dots$ Por tanto, $W_1 W_2^{-1}$ se puede transformar en la palabra vacía mediante las operaciones 1 y 2, luego W_1 se puede transformar en $W_1 W_2^{-1} W_2$ y luego en W_2 mediante las operaciones 1 y 2. Así, $W_1 \sim W_2$ y la aplicación (1.14) es inyectiva.

Finalmente, (1.14) es un homomorfismo gracias a (1.9) y porque el elemento definido por $W_1 W_2$ es el producto de los elementos definidos por W_1 y por W_2. □

Observación 1.1.2 Para cada presentación $\mathcal{P}$ hemos construido un modelo concreto de un grupo con la presentación $\mathcal{P}$. Este modelo concreto es el grupo de las clases de equivalencia de palabras y lo denotaremos $G(\mathcal{P})$.

Corolario 1.1.3 Cualesquiera dos grupos con la presentación (1.11) son isomorfos bajo el isomorfismo obvio.

Demostración: Ambos son isomorfos al grupo de clases de equivalencia del teorema 1.1.1 bajo el isomorfismo obvio. De hecho, si G', G'' son grupos con la presentación (1.11) bajo las aplicaciones

$$a \to g', b \to h', c \to k', \dots$$

y

$$a \to g'', b \to h'', c \to k'', \dots$$

respectivamente, entonces un isomorfismo entre ellos viene dado explícitamente por

$$W(g', h', k', \dots) \to W(g'', h'', k'', \dots).$$

Notar que, ciertamente, todo elemento de G' está definido por una palabra W en los generadores. □

Observación 1.1.4 Si $\mathcal{P}$ y $\mathcal{P}'$ son dos presentaciones para un grupo G entonces G es isomorfo a $G(\mathcal{P})$ y a $G(\mathcal{P}')$, luego existe un isomorfismo $\varphi_{\mathcal{P},\mathcal{P}'} : G(\mathcal{P}) \to G(\mathcal{P}')$. Este isomorfismo hace corresponder a cada generador en $\mathcal{P}$ una palabra en los generadores de $\mathcal{P}'$. Y su isomorfismo inverso asocia a cada generador de $\mathcal{P}'$ una palabra en los generadores de $\mathcal{P}$. Nótese que aquí estamos identificando, por brevedad, la clase de una palabra con la palabra.

Corolario 1.1.5 Si $g'', h'', k'', \dots$ son elementos de un grupo G'' tales que

$$P(g'', h'', k'', \dots), Q(g'', h'', k'', \dots), R(g'', h'', k'', \dots), \dots \tag{1.15}$$

son el elemento neutro en G'', entonces existe un homomorfismo del grupo de clases de equivalencia G del teorema 1.1.1 (y, por tanto, de cualquier grupo con la presentación (1.11)) en G''.

Demostración: La aplicación

$$\{W(a, b, c, \dots)\} \to W(g'', h'', k'', \dots) \tag{1.16}$$

es un homomorfismo de G en G''.

Como cada elemento de (1.15) es el neutro en G'', si $W_1(a, b, c, \dots)$ se puede transformar en $W_2(a, b, c, \dots)$ mediante 1 y 2, entonces $W_1(g'', h'', k'', \dots)$ y $W_2(g'', h'', k'', \dots)$ son el mismo elemento en G''. Por tanto, la aplicación (1.16) está bien definida. Es homomorfismo por la misma razón por la que (1.14) es homomorfismo. □

Corolario 1.1.6 Si G tiene la presentación

$$\langle a, b, c, \dots ; P, Q, R, \dots \rangle$$

y G' tiene la presentación

$$\langle a, b, c, \dots ; P, Q, R, \dots, S, T, \dots \rangle$$

entonces G' es imagen homomorfa de G bajo el homomorfismo obvio.

Demostración: Supongamos $a, b, c, \ldots$ definen $g', h', k', \ldots$ respectivamente en G'. Como $P, Q, R, \ldots$ son relatores, definen el neutro en G', es decir,

$$P(g', h', k', \ldots), Q(g', h', k', \ldots), R(g', h', k', \ldots), \ldots$$

son el neutro de G'. De donde se sigue el resultado por el corolario 1.1.5. □

Para terminar esta sección, vamos a probar un resultado que necesitaremos en el capítulo 3 cuando estudiemos grupos presentados con una única relación.

Lema 1.1.7 Sea $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq \ldots$ una sucesión creciente de conjuntos de símbolos y sea $T_1 \subseteq T_2 \subseteq \cdots \subseteq T_n \subseteq \ldots$ una sucesión creciente de conjuntos de palabras, donde T_n es un conjunto de palabras en los símbolos de S_n. Sea $G_n = \langle S_n; T_n \rangle$ y supongamos que para cada n, el subgrupo de G_n generado por los símbolos de S_{n-1} tiene la presentación $\langle S_{n-1}; T_{n-1} \rangle$ bajo la aplicación obvia. Entonces, si $S = \bigcup_{n=1}^{\infty} S_n$, $T = \bigcup_{n=1}^{\infty} T_n$ y $G = \langle S; T \rangle$, se tiene que el subgrupo de G generado por los símbolos de S_n es G_n, y por tanto, $G = \bigcup_{n=1}^{\infty} G_n$.

Demostración: Comencemos probando que el subgrupo de G generado por los símbolos de S_n es G_n. En primer lugar, consideremos el grupo de clases de equivalencia G_n y, para cada clase de equivalencia $\mathcal{C}_i^{(n)}$ seleccionemos una palabra $W_i^{(n)} \in \mathcal{C}_i^{(n)}$ de tal modo que $\{W_i^{(n-1)}\}_{i \in I_{n-1}} \subseteq \{W_i^{(n)}\}_{i \in I_n}$. Es decir, selecciono una palabra de cada clase de equivalencia de tal forma que el conjunto de estos representantes contenga un sistema de representantes de las clases de equivalencia de G_{n-1}. Esto lo podemos hacer pues si $W_i^{(n-1)}$ es un representante de $\mathcal{C}_i^{(n-1)} \in G_{n-1}$, entonces $W_i^{(n-1)}$ también lo puedo ver como una palabra en los símbolos de S_n y la tomo como representante de su clase en G_n. Además, dos representantes $W_{i_1}^{(n-1)} \neq W_{i_2}^{(n-1)}$ en G_{n-1} siguen representando clases distintas en G_n, pues si representasen la misma clase $\mathcal{C}_i^{(n)}$ en G_n, serían palabras equivalentes en G_n, luego también en G_{n-1} (pues G_{n-1} es, por hipótesis, subgrupo de G_n) lo que conduce a una contradicción.

Si denotamos $W_n := \{W_i^{(n)}\}_{i \in I_n}$ el conjunto de la palabras representantes para G_n entonces claramente W_n forma un grupo bajo el producto adecuado: el producto de dos representantes $W_i^{(n)}$ y $W_j^{(n)}$ es el representante $W_k^{(n)}$ si y sólo si la yuxtaposición de $W_i^{(n)}$ y $W_j^{(n)}$ pertenece a $\mathcal{C}_k^{(n)}$. Además, por como hemos tomado los representantes y por lo anterior, W_{n-1} es un subgrupo de W_n. También es claro que $W_n \cong G_n$.

Si $W = \bigcup_{n=1}^{\infty} W_n$, entonces S es un conjunto de símbolos generadores para W bajo la aplicación obvia pues todo $g \in W$ pertenece a algún W_n, luego es un representante $W_i^{(n)}$ de una clase de G_n, lo que implica que es una palabra en los símbolos de $S_n \subseteq S$.

Además, los elementos de T son relatores de W pues si $U \in T$ entonces por definición $U \in T_n$ para algún n, de donde U define el neutro en $G_n \cong W_n \leq W$, luego U también define el neutro en W.

Si una palabra U en los símbolos de S es un relator en W, es una palabra en los símbolos de algún S_n que define el neutro en W, luego también define el neutro en el subgrupo $W_n \cong G_n$, luego U es un relator en G_n lo que implica que es derivable de las palabras en T_n y, por tanto, de las palabras en T.

Hemos probado que W tiene la presentación $\langle S; T\rangle$, y como $G_n \cong W_n \leq W \cong G$ se tiene la primera parte del resultado.

Probar ahora que $G = \bigcup_{n=1}^{\infty} G_n$ es inmediato pues por lo anterior $\bigcup_{n=1}^{\infty} G_n \subseteq G$. Y, para ver el otro contenido, dado $g \in G$ puedo representar g por una palabra $W(a_\nu)$ en los símbolos de S. Como sólo pueden intervenir en W una cantidad finita de símbolos de S existirá un n tal que todos ellos pertenezcan a S_n. Por tanto, g pertenecerá al subgrupo de G generado por los símbolos de S_n que, por lo anterior, es G_n. □

1.2. Las transformaciones de Tietze.

Un grupo puede tener muchas presentaciones. Por ejemplo, el grupo simétrico de grado 3, S_3, tiene la presentación

$$\langle a, b; a^3, b^2, ab = ba^2\rangle$$

bajo la aplicación $a \to (1, 2, 3)$, $b \to (1, 2)$. Pero también tiene la presentación

$$\langle a, b; a^3, b^2, ab = ba^{-1}\rangle$$

bajo la misma aplicación. Más aun, S_3 también tiene la presentación,

$$\langle c, d; c^2, d^2, (cd)^3\rangle$$

bajo la aplicación $c \to (1, 3)$, $d \to (2, 3)$.

Esto nos lleva a preguntarnos si existe algún método para transformar una presentación en otra. Las transformaciones de Tietze dan respuesta a esta pregunta. Dada una presentación de un grupo G

$$\langle a, b, c, \ldots; P, Q, R, \ldots\rangle, \tag{1.17}$$

cualquier otra presentación se puede obtener de ella aplicando reiteradamente las siguientes tranformaciones (llamadas transformaciones de Tietze):

(T1) Si las palabras $S, T, \ldots$ son derivables de $P, Q, R, \ldots$ entonces añadir $S, T, \ldots$ al conjunto de relatores en (1.17).

(T2) Si alguno de los relatores $S, T, \ldots$ de entre los que aparecen en la presentación (1.17) es derivable a partir de los otros, eliminar $S, T, \ldots$ de la presentación.

(T3) Si $K, M, \ldots$ son palabras en $a, b, c, \ldots$, añadir los símbolos $x, y, \ldots$ a los símbolos generadores en (1.17) y añadir las relaciones $x = K$, $y = M$, $\ldots$ al conjunto de relaciones de (1.17).

(T4) Si alguna de las relaciones que aparecen en (1.17) es de la forma $p = V, q = W, \ldots$ donde $p, q, \ldots$ son generadores en (1.17) y $V, W, \ldots$ son palabras en las que no aparecen los genradores $p, q, \ldots$, entonces eliminar $p, q, \ldots$ de los generadores, eliminar $p = V, q = W, \ldots$ de las relaciones y sustituir $p, q, \ldots$ por $V, W, \ldots$ respectivamente, en las demás relaciones de (1.17).

Una transformación de Tietze se dirá elemental si sólo involucra la inserción o eliminación de un único relator, o la inserción o eliminación de un generador y la correspondiente relación.

Aplicar una transformación de Tietze a una presentación no cambia el grupo definido por esa presentación. Si (1.17) es una presentación de G bajo la aplicación $a \to g, b \to h, c \to k, \ldots$, entonces aplicar (T1) o (T2) a (1.17) proporciona una presentación de G bajo la misma aplicación. Aplicar (T3) a (1.17) proporciona una presentación de G bajo la aplicación

$$a \to g, b \to h, c \to k, \ldots, x \to K(g, h, k, \ldots), y \to M(g, h, k, \ldots), \ldots \tag{1.18}$$

puesto que si $N(a, b, c, \ldots, x, y, \ldots)$ es un relator en G bajo la aplicación (1.18), entonces usando las relaciones $x = K$, $y = M$, $\ldots$, la palabra N se puede transformar en una palabra en la que sólo aparecen los símbolos $a, b, c, \ldots$ que es un relator bajo la aplicación $a \to g, b \to h, c \to k, \ldots$, y por tanto se puede derivar de $P, Q, R, \ldots$, luego $P, Q, R, \ldots, x = K, y = M, \ldots$ es un conjunto completo de relaciones para G bajo (1.18). Finalmente, aplicar (T4) a (1.17) proporciona una presentación de G bajo la restricción de la aplicación $a \to g, b \to h, c \to k, \ldots$ a los generadores de (1.17) que permanecen en la nueva presentación, ya que usando (T3) para insertar los generadores eliminados y sus correspondientes relaciones llegamos de nuevo a (1.17) (tras reemplazar $V, W, \ldots$ por $p, q, \ldots$ donde sea necesario usando (T1) y (T2)) y, puesto que (T3) no cambia el grupo definido por la presentación, tampoco lo hace (T4).

Por otra parte, la transformación inversa de una transformación de Tietze es una secuencia de transformaciones de Tietze. De hecho, la transformación inversa de una transformación (T1) es una transformación (T2), y viceversa. La transformación inversa de una transformación (T3) es una transformación (T4); y la transformación inversa de (T4) es una transformación (T3) seguida de una (T1) y después una (T2).

Hemos visto que aplicar transformaciones de Tietze a una presentación no cambia el grupo definido por la presentación. Más aun, se puede probar que si tenemos un grupo dado por

una determinada presentación, cualquier otra presentación para ese grupo se puede obtener de la que teníamos aplicando reiteradamente transformaciones de Tietze, como probaremos a continuación.

Teorema 1.2.1 Dadas dos presentaciones de un grupo G,

$$\langle a_1, a_2, \dots ; R_1(a_\nu), R_2(a_\nu), \dots \rangle, \tag{1.19}$$

y

$$\langle b_1, b_2, \dots ; S_1(b_\mu), S_2(b_\mu), \dots \rangle, \tag{1.20}$$

entonces (1.20) se puede obtener a partir de (1.19) mediante aplicación reiterada de transformaciones de Tietze.

Demostración: Supongamos que (1.19) es una presentación de G bajo la aplicación

$$a_1 \to g_1, a_2 \to g_2, \dots$$

y que (1.20) lo es bajo la aplicación

$$b_1 \to h_1, b_2 \to h_2, \dots$$

Como $g_1, g_2, \dots$ son elementos generadores de G, podemos expresar $h_1, h_2, \dots$ en términos de $g_1, g_2, \dots$

$$h_1 = B_1(g_1, g_2, \dots), \quad h_2 = B_2(g_1, g_2, \dots), \dots$$

Aplicando una transformación (T3), añadimos los nuevos símbolos $b_1, b_2, \dots$ a los símbolos generadores de (1.19), y añadimos las relaciones

$$b_1 = B_1(a_1, a_2, \dots), \quad b_2 = B_2(a_1, a_2, \dots), \dots$$

obteniendo la presentación

$$\langle a_1, a_2, \dots, b_1, b_2, \dots ; R_1(a_\nu), R_2(a_\nu), \dots b_1 = B_1(a_\nu), b_2 = B_2(a_\nu), \dots \rangle \tag{1.21}$$

De hecho, G está presentado por (1.21) bajo la aplicación

$$a_1 \to g_1, a_2 \to g_2, \dots, b_1 \to h_1, b_2 \to h_2, \dots \tag{1.22}$$

Puesto que $S_1(b_1, b_2, \dots), S_2(b_1, b_2, \dots), \dots$ son relatores bajo $b_1 \to h_1, b_2 \to h_2, \dots$, también lo son bajo (1.22), de modo que mediante una transformación (T1), podemos añadir estos relatores a la presentación dada por (1.21), obteniendo:

$$\langle a_1, a_2, \dots, b_1, b_2, \dots ; R_1(a_\nu), R_2(a_\nu), \dots b_1 = B_1(a_\nu), b_2 = B_2(a_\nu), \dots, S_1(b_\mu), S_2(b_\mu), \dots \rangle \tag{1.23}$$

que es una presentación de G bajo (1.22).

Como $h_1, h_2, \ldots$ son elementos generadores de G, podemos expresar $g_1, g_2, \ldots$ en términos de $h_1, h_2, \ldots$

$$g_1 = A_1(h_1, h_2, \ldots), \quad g_2 = A_2(h_1, h_2, \ldots), \ldots$$

Así, bajo la aplicación (1.22) tenemos que

$$a_1 = A_1(b_1, b_2, \ldots), \quad a_2 = A_2(b_1, b_2, \ldots), \ldots$$

son relaciones y, por tanto, derivables a partir de las relaciones en (1.23), luego aplicando (T1) podemos añadir estas relaciones a las relaciones de (1.23), obteniendo la presentación

$$\langle a_1, a_2, \ldots, b_1, b_2, \ldots; R_1(a_\nu), R_2(a_\nu), \ldots b_1 = B_1(a_\nu), b_2 = B_2(a_\nu),$$

$$\ldots, S_1(b_\mu), S_2(b_\mu), \ldots, a_1 = A_1(b_\mu), a_2 = A_2(b_\mu), \ldots \rangle \tag{1.24}$$

Observemos que (1.24) es simétrica, luego también podemos obtener (1.24) a partir de (1.20) mediante transformaciones de Tietze, de modo que aplicando las inversas de dichas transformaciones de Tietze podemos obtener (1.20) a partir de (1.24). Pero la transformación inversa de una tranformación de Tietze es una secuencia de transformaciones de Tietze, y por tanto podemos obtener (1.20) a partir de (1.19) mediante transformaciones de Tietze. □

Corolario 1.2.2 Si las presentaciones (1.19) y (1.20) del teorema 1.2.1 son finitas, entonces (1.19) se puede transformar en (1.20) mediante una secuencia finita de transformaciones elementales de Tietze.

Demostración: Si las presentaciones (1.19) y (1.20) son finitas, entonces los generadores y las relaciones que se añaden en el teorema para obtener (1.24) son una cantidad finita, y se pueden añadir de uno en uno mediante transformaciones elementales de Tietze. De manera análoga, (1.20) se puede obtener de (1.24) mediante un número finito de transformaciones elementales de Tietze. □

1.3. Grupos libres.

El objetivo de esta sección es introducir el concepto de grupo libre.

Definición 1.3.1 El grupo libre F_n en n generadores libres $x_1, \ldots, x_n$ es el grupo con generadores $x_1, \ldots, x_n$ y donde el vacío forma un conjunto completo de relaciones. Es decir, $F_n = \langle x_1, \ldots, x_n \rangle$.

Del corolario 1.1.6 se sigue que cualquier grupo G con n generadores es imagen homomorfa de F_n.

Una palabra en los símbolos $x_1, \ldots, x_n$ se dice reducida si en ella los símbolos $x_\nu^\epsilon, x_\nu^{-\epsilon}$ $(\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$ no aparecen consecutivos. Por ejemplo, la palabra $x_1^2 x_3^{-1}$ es reducida pero la palabra $x_1^3 x_2^{-2} x_2^4$ no lo es.

Una palabra se dice cíclicamente reducida si es reducida y no le ocurre que empieza por x_ν^ϵ y termina por $x_\nu^{-\epsilon}$ $(\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$, equivalentemente, una palabra se dice cíclicamente reducida si ella y todas sus permutaciones cíclicas son reducidas. Por ejemplo, la palabra $x_1^2 x_3^{-1}$ es cíclicamente reducida pero la palabra $x_1^2 x_3^{-1} x_1^{-1}$ no lo es.

Dos palabras $W_1(x_\nu)$ y $W_2(x_\nu)$ se dicen libremente iguales (y se denota $W_1 \approx W_2$) si determinan el mismo elemento de F_n, el grupo libre en $x_1, \ldots, x_n$, es decir, si W_1 se puede transformar en W_2 mediante inserción y eliminación de relatores triviales. Por ejemplo, $x_1 x_2^2 x_2^{-1} x_3^2 x_3^{-2} x_1^{-1} \approx x_1 x_2 x_1^{-1}$.

Claramente, cualquier palabra es libremente igual a una palabra reducida (basta eliminar relatores triviales). Sin embargo, la eliminación de relatores triviales puede llevarse a cabo de diversas maneras, por lo que no resulta obvio que la palabra reducida que se obtiene será siempre la misma, independientemente del procedimiento que se utilice. Esto se establece en el siguiente teorema.

Teorema 1.3.2 Todo elemento del grupo libre F_n en los generadores libres $x_1, \ldots, x_n$ está definido por una única palabra reducida, es decir, toda palabra en $x_1, \ldots, x_n$ es libremente igual a una única palabra reducida.

Demostración: Sea ρ el siguiente proceso para reducir libremente una palabra:

$\rho(1) = 1$, $\rho(x_\nu^\epsilon) = x_\nu^\epsilon$ $(\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$

y si $\rho(U) = x_{\mu_1}^{\eta_1} \ldots x_{\mu_q}^{\eta_q}$ $(\eta_i = \pm 1; \mu_i = 1, 2, \ldots, n)$ entonces

$$\rho(U x_\nu^\epsilon) = \begin{cases} x_{\mu_1}^{\eta_1} \ldots x_{\mu_q}^{\eta_q} x_\nu^\epsilon & \text{si } \mu_q \neq \nu \text{ o } \eta_q \neq -\epsilon \\ x_{\mu_1}^{\eta_1} \ldots x_{\mu_{q-1}}^{\eta_{q-1}} & \text{si } \mu_q = \nu \text{ y } \eta_q = -\epsilon \end{cases}$$

Entonces ρ verifica las siguientes propiedades:

1. $\rho(W)$ es reducida
2. $\rho(W) \approx W$
3. Si V es reducida entonces $\rho(V) = V$
4. $\rho(W_1 \cdot W_2) = \rho(\rho(W_1) \cdot W_2)$
5. $\rho(W x_\nu^\epsilon x_\nu^{-\epsilon}) = \rho(W), (\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$
6. $\rho(W_1 x_\nu^\epsilon x_\nu^{-\epsilon} W_2) = \rho(W_1 W_2), (\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$

Las propiedades 1, 2 y 5 se siguen de la definición de ρ por inducción en la longitud de W, la propiedad 3 se sigue por inducción en la longitud de V, mientras que 4 se sigue por inducción en la longitud de W_2. La propiedad 6 es consecuencia de 4 y 5.

Probaremos ahora que si dos palabras son libremente iguales, el proceso ρ aplicado sobre cada una de ellas da el mismo resultado. En efecto, si $U \approx T$ entonces existen palabras $U_1, \ldots, U_k$ tales que $U_1 = U, U_k = T$ y U_{i+1} se obtenga de U_i por inserción o eliminación de un único relator de la forma $x_\nu^\epsilon x_\nu^{-\epsilon}, (\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$. Entonces, por 6, $\rho(U_{i+1}) = \rho(U_i)$, luego $\rho(U) = \rho(T)$.

Finalmente, veremos que cualquier forma de reducir libremente una palabra U da como resultado $\rho(U)$. Si $U \approx V$ con V reducida, entonces por lo anterior y 3, se obtiene que $\rho(U) = \rho(V) = V$. Por tanto, toda palabra U es libremente igual a una única palabra reducida: $\rho(U)$. □

Corolario 1.3.3 Si F_n es el grupo libre en los generadores libres $x_1, \ldots, x_n$, entonces todo elemento no trivial tiene orden infinito.

Demostración: Sea $W = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_p}^{\epsilon_p}$ $(\epsilon_i = \pm 1; \nu_i = 1, 2, \ldots, n)$ una palabra reducida que define un elemento de F_n distinto del neutro. Si W es también cíclicamente reducida, entonces $\nu_1 \neq \nu_p$ ó $\epsilon_1 \neq -\epsilon_p$. Por tanto, si k es un entero positivo,

$$W^k = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_p}^{\epsilon_p} x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_p}^{\epsilon_p} \ldots x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_p}^{\epsilon_p}$$

donde el lado derecho de esta igualdad está formado por k factores, cada uno de ellos igual a W. Necesariamente W^k es entonces reducida y no es la palabra vacía. Por tanto, W^k no puede definir el elemento neutro ya que la palabra vacía define el neutro y en virtud del teorema 1.3.2 no hay ninguna otra palabra reducida que pueda hacerlo. En consecuencia, W tiene orden infinito.

Por otra parte, si W no es cíclicamente reducida, entonces podemos expresar W de la forma:

$$W = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_r}^{\epsilon_r} x_{\mu_1}^{\eta_1} \ldots x_{\mu_q}^{\eta_q} x_{\nu_r}^{-\epsilon_r} \ldots x_{\nu_1}^{-\epsilon_1}$$

donde $\mu_1 \neq \mu_q$ ó $\eta_1 \neq -\eta_q$ $(\epsilon_i, \eta_j = \pm 1; \nu_i, \mu_j = 1, 2, \ldots, n)$, luego $W = UVU^{-1}$ con $U = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_r}^{\epsilon_r}$, $V = x_{\mu_1}^{\eta_1} \ldots x_{\mu_q}^{\eta_q}$ y V es cíclicamente reducida y no vacía. Como V es cíclicamente reducida, V define (por el caso anterior) un elemento de F_n de orden infinito. Por tanto W, que define un conjugado de este elemento, también define un elemento de orden infinito. □

El teorema 1.3.2 nos permite dar otra definición de grupo libre, pues podemos definir el grupo libre F_n como el conjunto de palabras reducidas en $x_1, \ldots, x_n$ con el producto de palabras definido mediante la yuxtaposición y posterior reducción hasta lograr una palabra reducida.

Del mismo modo que hemos introducido un método para reducir libremente una palabra, daremos ahora un procedimiento σ que asocia a cada palabra una palabra cíclicamente reducida. Hay que tener en cuenta que ρ transformaba cada palabra en otra reducida que definía

el mismo elemento; sin embargo, $\sigma(W)$ y W no definirán necesariamente el mismo elemento sino elementos conjugados.

Definimos σ para palabras reducidas de la siguiente manera:

$\sigma(1) = 1$, $\sigma(x_\nu^\epsilon) = x_\nu^\epsilon$ $(\epsilon = \pm 1; \nu = 1, 2, \ldots, n)$

$\sigma(x_\nu^\epsilon U x_\mu^\eta) = x_\nu^\epsilon U x_\mu^\eta$ si $\nu \neq \mu$ ó $\epsilon \neq -\eta$

$\sigma(x_\nu^\epsilon U x_\mu^\eta) = \sigma(U)$ si $\nu = \mu$ y $\epsilon = -\eta$

donde $\epsilon, \eta = \pm 1; \nu, \mu = 1, 2, \ldots, n$. Finalmente, para una palabra cualquiera (no necesariamente reducida) σ se define del siguiente modo: $\sigma(W) = \sigma(\rho(W))$.

Por ejemplo, $\sigma(x_1 x_2 x_3 x_3^{-1} x_2 x_1 x_2^{-1} x_1^{-1}) = \sigma(x_1 x_2^2 x_1 x_2^{-1} x_1^{-1}) = \sigma(x_2^2 x_1 x_2^{-1}) = \sigma(x_2 x_1) = x_2 x_1$

A partir de la definición de σ se obtiene por inducción en la longitud de W que $\sigma(W)$ es cíclicamente reducida y que W y $\sigma(W)$ definen elementos conjugados de F_n.

Teorema 1.3.4 Si F_n es el grupo libre en los generadores libres $x_1, \ldots, x_n$, entonces $W_1(x_\nu)$ y $W_2(x_\nu)$ definen elementos conjugados de F_n si y sólo si $\sigma(W_1)$ es una permutación cíclica de $\sigma(W_2)$.

Demostración: Supongamos primero que $\sigma(W_2)$ es una permutación cíclica de $\sigma(W_1)$.

$$\sigma(W_1) = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_s}^{\epsilon_s} x_{\nu_{s+1}}^{\epsilon_{s+1}} \ldots x_{\nu_p}^{\epsilon_p}$$

$$\sigma(W_2) = x_{\nu_{s+1}}^{\epsilon_{s+1}} \ldots x_{\nu_p}^{\epsilon_p} x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_s}^{\epsilon_s}$$

donde $\epsilon_i = \pm 1$, $\nu_i = 1, \ldots, n$. Entonces $\sigma(W_1) \approx K \sigma(W_2) K^{-1}$ donde $K = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_s}^{\epsilon_s}$. Como $\sigma(W_1)$ y W_1 y también $\sigma(W_2)$ y W_2 definen elementos conjugados de F_n, se sigue que W_1 y W_2 definen elementos conjugados de F_n.

Supongamos ahora que W_1 y W_2 definen elementos conjugados de F_n, es decir, $W_1 \approx T W_2 T^{-1}$. Veamos que $\sigma(W_1)$ y $\sigma(W_2)$ son permutaciones cíclicas la una de la otra. Como $\rho(W_1) = \rho(T W_2 T^{-1})$, se sigue que

$$\sigma(W_1) = \sigma(\rho(W_1)) = \sigma(\rho(T W_2 T^{-1})) = \sigma(T W_2 T^{-1})$$

luego basta probar que $\sigma(T W_2 T^{-1})$ es una permutación cíclica de $\sigma(W_2)$. Lo haremos por inducción en la longitud de T.

Si $T = x_\nu^\epsilon$ con $\epsilon = \pm 1$, $\nu = 1, \ldots, n$, debemos comparar $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon})$ con $\sigma(W_2)$. Ahora bien, $\sigma(W_2) = \sigma(\rho(W_2))$, y además, $x_\nu^\epsilon W_2 x_\nu^{-\epsilon} \approx x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}$, de donde $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon}) = \sigma(\rho(x_\nu^\epsilon W_2 x_\nu^{-\epsilon})) = \sigma(\rho(x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}))$. Supongamos que $\rho(W_2) = x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_r}^{\epsilon_r}$ con $\epsilon_i = \pm 1$, $\nu_i = 1, \ldots, n$, entonces para calcular $\rho(x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}) = \rho(x_\nu^\epsilon x_{\nu_1}^{\epsilon_1} \ldots x_{\nu_r}^{\epsilon_r} x_\nu^{-\epsilon})$ vamos a considerar cuatro casos.

Caso 1: No tiene lugar ninguna eliminación de relatores triviales, es decir, $\nu \neq \nu_1$ o $\epsilon \neq -\epsilon_1$, y $\nu \neq \nu_r$ o $\epsilon \neq \epsilon_r$. Entonces $\rho(x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}) = x_\nu^\epsilon x_{\nu_1}^{\epsilon_1} \dots x_{\nu_r}^{\epsilon_r} x_\nu^{-\epsilon}$. Por tanto, $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon}) = \sigma(x_\nu^\epsilon x_{\nu_1}^{\epsilon_1} \dots x_{\nu_r}^{\epsilon_r} x_\nu^{-\epsilon}) = \sigma(x_{\nu_1}^{\epsilon_1} \dots x_{\nu_r}^{\epsilon_r}) = \sigma(\rho(W_2)) = \sigma(W_2)$.

Caso 2: Hay eliminación de relatores triviales al principio y final de la palabra, es decir, $\nu = \nu_1 = \nu_r$, $\epsilon = -\epsilon_1 = \epsilon_r$. Entonces $\rho(x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}) = x_{\nu_2}^{\epsilon_2} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}}$.

Así, en este caso, $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon}) = \sigma(x_{\nu_2}^{\epsilon_2} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}})$. Pero, por otra parte, $\sigma(W_2) = \sigma(\rho(W_2)) = \sigma(x_{\nu_1}^{\epsilon_1} x_{\nu_2}^{\epsilon_2} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}} x_{\nu_1}^{-\epsilon_1}) = \sigma(x_{\nu_2}^{\epsilon_2} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}})$, luego también en este caso se cumple que $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon}) = \sigma(W_2)$.

Caso 3: Sólo se produce cancelación en el extremo izquierdo, es decir, $\nu = \nu_1$ y $\epsilon = -\epsilon_1$, pero $\nu \neq \nu_r$ o $\epsilon \neq \epsilon_r$. Entonces $\rho(x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}) = x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1}$. Como $x_{\nu_1}^{\epsilon_1} x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r}$ y $x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1}$ son ambas reducidas, son las dos cíclicamente reducidas. Por tanto,

$$\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon}) = \sigma(x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1}) = x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1}$$

$$\sigma(W_2) = \sigma(\rho(W_2)) = \sigma(x_{\nu_1}^{\epsilon_1} x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r}) = x_{\nu_1}^{\epsilon_1} x_{\nu_2}^{\epsilon_2} \dots x_{\nu_r}^{\epsilon_r}$$

En este caso, $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon})$ es una permutación cíclica de $\sigma(W_2)$.

Caso 4: Sólo se produce cancelación en el extremo derecho, es decir, $\nu \neq \nu_1$ o $\epsilon \neq -\epsilon_1$, pero $\nu = \nu_r$ y $\epsilon = \epsilon_r$. Entonces $\rho(x_\nu^\epsilon \rho(W_2) x_\nu^{-\epsilon}) = x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}}$. Así,

$$\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon}) = \sigma(x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}}) = x_{\nu_r}^{\epsilon_r} x_{\nu_1}^{\epsilon_1} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}}$$

que es una permutación cíclica de

$$\sigma(W_2) = \sigma(\rho(W_2)) = \sigma(x_{\nu_1}^{\epsilon_1} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}} x_{\nu_r}^{\epsilon_r}) = x_{\nu_1}^{\epsilon_1} \dots x_{\nu_{r-1}}^{\epsilon_{r-1}} x_{\nu_r}^{\epsilon_r}$$

Por tanto, en cada uno de los cuatro casos $\sigma(x_\nu^\epsilon W_2 x_\nu^{-\epsilon})$ es una permutación cíclica de $\sigma(W_2)$. Esto prueba que $\sigma(T W_2 T^{-1})$ es una permutación cíclica de $\sigma(W_2)$ cuando T tiene longitud 1.

Supongámoslo probado para longitud n y supongamos que T tiene longitud $n+1$. T será de la forma $T = x_\nu^\epsilon K$ con K de longitud n. Por hipótesis de inducción, $\sigma(K W_2 K^{-1})$ es una permutación cíclica de $\sigma(W_2)$. Pero por el caso $n = 1$, $\sigma(x_\nu^\epsilon K W_2 K^{-1} x_\nu^{-\epsilon})$ es una permutación cíclica de $\sigma(K W_2 K^{-1})$, luego también es una permutación cíclica de $\sigma(W_2)$. □

1.4. Los problemas de Dehn.

Hemos probado que cualquier presentación que podamos imaginar, sin importar cuántas ni cuán complicadas puedan ser las relaciones, define un único grupo salvo isomorfismo. No obstante, no es sencillo en general conocer propiedades de dicho grupo, por ejemplo, si es finito, abeliano, ...

En realidad, ni siquiera es fácil en general saber cuándo dos palabras definen el mismo elemento o, formulando el problema de manera equivalente, cuándo una palabra define el elemento neutro. Estos dos problemas son, ciertamente, equivalentes, pues W_1 define el mismo elemento que W_2 si y sólo si $W_1 W_2^{-1}$ define el elemento neutro.

Éste es uno de los tres problemas que se conocen con el nombre de problemas de Dehn, y que se plantean, para un grupo G definido por medio de una presentación, de la siguiente manera:

- Problema de la palabra: Dada una palabra cualquiera W en los generadores, decidir en un número finito de pasos si W define el elemento neutro de G o no.
- Problema de la conjugación: Dadas dos palabras cualesquiera W_1 y W_2 en los generadores, decidir en un número finito de pasos, si W_1 y W_2 definen elementos conjugados en G o no.
- Problema del isomorfismo: Dado un grupo G' cualquiera definido por medio de otra presentación, decidir en un número finito de pasos, si G es isomorfo a G' o no.

El problema de la palabra ha sido resuelto para ciertos tipos de presentaciones, por ejemplo, presentaciones en las que aparece un único relator (ver sección 3.2) o ninguno (ver sección 1.3) o presentaciones construidas de manera sencilla a partir de presentaciones para las que el problema de la palabra es resoluble (ver sección 2.1).

Hay que destacar que la solución a los problemas de Dehn está basada siempre en una presentación específica del grupo. Sin embargo, es habitual hablar de los problemas de Dehn para un grupo, sin especificar qué presentación concreta del grupo se está considerando, entendiendo que se toma una presentación "estándar" para el grupo, por ejemplo, el grupo libre en n generadores tiene la presentación "estándar" $\langle a_1, \ldots, a_n \rangle$. Por ello, cuando hablemos, por ejemplo, del problema de la palabra para grupos libres o para grupos dados por una única relación, estaremos sobreentendiendo que el grupo está presentado en términos de generadores libres o en términos de generadores y una única relación, respectivamente.

Para grupos libres (presentados mediante generadores libres) se conoce la solución al problema de la palabra gracias al teorema 1.3.2. De hecho:

Corolario 1.4.1 Si F_n es el grupo libre en los generadores libres $x_1, \ldots, x_n$, entonces el problema de la palabra tiene solución.

Demostración: Para decidir si una palabra dada $W(x_1, \ldots, x_n)$ define el neutro de F_n basta reducir libremente W usando ρ. W define la identidad de F_n si y sólo si $\rho(W)$ es la palabra vacía. □

Es decir, si F_n es el grupo libre en los generadores libres $x_1, \ldots, x_n$, la palabra $x_1 x_2^3 x_2^{-2}$ no define el elemento neutro pues si la reducimos libremente obtenemos $x_1 x_2$, que no es la palabra vacía. En cambio, la palabra $x_1^{-2} x_2 x_2^{-1} x_1^2$ sí define el neutro de F_n pues al reducirla libremente obtenermos la palabra vacía. De este modo, una palabra que ya es reducida definirá el neutro si y sólo si es la palabra vacía.

En este caso, no solamente hemos resuelto el problema de la palabra para grupos libres dados por generadores libres sino que la solución que hemos obtenido es particularmente sencilla.

Sin embargo, existen grupos finitamente presentados para los que no existe un procedimiento general y efectivo para decidir si una palabra cualquiera W en los generadores representa el elemento neutro del grupo o no. De hecho, el problema de la palabra adquirió fama cuando Novikov y, de forma independiente, Boone y Britton probaron que no es resoluble en general. Primero Rabin, y después Baumslag, Boone y B. H. Neumann, utilizaron el descubrimiento de Novikov para probar que prácticamente todos los problemas relativos a grupos finitamente presentados no son resolubles en general, incluyendo los problemas de decidir si un grupo en trivial, finito, libre, nilpotente o simple.

La solución al problema de la palabra para una presentación finita de un grupo G nos proporciona una forma canónica de expresar los elementos de G. (Formalmente, una forma canónica es una aplicación F del conjunto de las palabras en los generadores en sí mismo cumpliendo que dos palabras son equivalentes si y sólo si sus imágenes por F coinciden). Es decir, la solución al problema de la palabra en grupos finitamente presentados nos permite seleccionar un único representante para cada clase de equivalencia de palabras. También nos permite dar la tabla de multiplicación de estos representantes, es decir, podemos ver G de la manera usual: como un conjunto de elementos distintos y su tabla de multiplicación. Supongamos que tenemos un grupo G con la presentación finita

$$\langle a_1, a_2, \ldots, a_n; R_1, R_2, \ldots, R_m \rangle \tag{1.25}$$

y definimos una relación de orden $<$ en el conjunto de palabras en los símbolos $a_1, a_2, \ldots, a_n$ de la siguiente manera:

Si $L(W_1) < L(W_2)$ entonces $W_1 < W_2$

Si $L(W_1) = L(W_2)$ entonces se toma el convenio

$$a_1 < a_1^{-1} < a_2 < a_2^{-1} < \ldots < a_n < a_n^{-1}$$

y se ordenan W_1 y W_2 de acuerdo al primer término en que difieran según lo anterior.

Así, por ejemplo,

$$1 < a_1 < a_2 a_n < a_2 a_n^{-1} < a_1^3$$

Dada una palabra W, es claro que sólo hay una cantidad finita de palabras que la preceden, pues éstas han de tener longitud menor o igual que $L(W)$ y sólo hay una cantidad finita de generadores en (1.25). Por tanto, cualquier conjunto no vacío de palabras tiene una palabra "menor". Tomemos como sistema de representantes S el conjunto de palabras "menores", una por cada clase de equivalencia.

Si el problema de la palabra es resoluble para (1.25), podemos encontrar de forma constructiva el representante de cualquier palabra W. Para ello, primero enumeramos todas las palabras W_i que preceden W (y que serán una cantidad finita). Usemos la solución al problema de la palabra para ver cuáles de estos W_i definen el mismo elemento que W, y finalmente seleccionemos el menor de tales W_i.

Además, dados dos representantes U, V en S, para encontrar el producto de U y V en S sólo hay que encontrar el representante de UV en S según el método anterior. Por tanto, S forma, con este producto, un grupo isomorfo a G, lo que nos permite ver G como un conjunto de representantes canónicos bajo esta regla de multiplicación.

Recíprocamente, dado (1.25), si podemos obtener un conjunto de palabras S tal que toda palabra sea equivalente a una de las de S y ningún par de palabras en S sean equivalentes, y si tenemos un procedimiento constructivo para decidir en un número finito de pasos cuál es la palabra de S equivalente a una palabra dada W, entonces el problema de la palabra en (1.25) es resoluble. Dada una palabra W, basta calcular en un número finito de pasos la palabra en S equivalente a W y la palabra en S equivalente a la palabra vacía. Entonces W define el neutro en G si y sólo si ambas palabras de S coinciden.

El problema de la conjugación es aún más difícil que el problema de la palabra. De hecho, incluye al problema de la palabra como caso particular, pues resolver el problema de la conjugación tomando una de las palabras igual a la palabra vacía es precisamente resolver el problema de la palabra. Por tanto, los grupos para los que está resuelto el problema de la conjugación son grupos para los que también está resuelto el problema de la palabra, por ejemplo grupos libres presentados en términos de generadores libres (ver sección 1.3). En cambio, hay algunos tipos de presentaciones para las que se ha resuelto el problema de la palabra pero no el de la conjugación, por ejemplo presentaciones en las que aparece una única relación.

Hasta el momento, se ha podido resolver el problema de la conjugación para grupos libres dados por generadores libres. La solución está recogida en el teorema 1.3.4 que nos dice que dos palabras en los generadores libres $x_1, \ldots, x_n$ definen elementos conjugados en F_n si y sólo si sus correspondientes reducciones cíclicas son permutaciones cíclicas la una de la otra. Por ejemplo, las palabras $W_1 = x_1x_2x_3x_3^{-1}x_2x_1x_2^{-1}x_1^{-1}$ y $W_2 = x_1x_2$ definen elementos conjugados en F_n pues $\sigma(W_1) = x_2x_1$ es una permutación cíclica de $\sigma(W_2) = x_1x_2$.

Hay que destacar que las soluciones que hemos dado a los problemas de la palabra y de la conjugación para grupos libres son válidas solamente cuando el grupo libre está presentado en términos de generadores libres. Ciertamente, un grupo libre se puede presentar también usando un conjuto completo de relaciones no vacío, por ejemplo el grupo $\langle a, b, c; ab^{-2}\rangle$ es un grupo libre en los generadores libres b y c (basta usar una transformación de Tietze T4).

El problema del isomorfismo es el más difícil de los tres problemas de Dehn. De hecho, ni siquiera existe un procedimiento general y efectivo para decidir si un grupo finitamente presentado es trivial. El problema del isomorfismo sí se puede resolver en algunos casos especiales. Por ejemplo, si las presentaciones de G y G' carecen de relaciones, o si una de las presentaciones no incluye relaciones y la otra sólo incluye una única relación, entonces el problema del isomorfismo se puede resolver. No obstante, si las dos presentaciones incluyen un único relator cada una, entonces la solución al problema es desconocida, pudiendo incluso el problema no ser resoluble.

Si bien en un principio se podría pensar que el teorema 1.2.1 proporciona una solución al problema del isomorfismo, ésto no es cierto pues dicho teorema no da ningún procedimiento constructivo para decidir en un número finito de pasos si una presentación se puede obtener a partir de otra mediante transformaciones de Tietze, simplemente afirma que cualquier presentación de G se puede obtener mediante transformaciones de Tietze a partir de cualquier otra presentación de G.

1.5. Grupos cociente.

En esta sección estudiaremos cómo dar una presentación de un cociente G/N si tenemos una presentación $\langle a, b, c, \dots ; P, Q, R, \dots \rangle$ de G.

Diremos que N es el subgrupo normal de G generado por $g, h, \dots$ si es el menor subgrupo normal de G que contiene a $g, h, \dots$ o, equivalentemente, si es la intersección de todos los subgrupos normales de G que contienen a $g, h, \dots$. También se dice que N es la clausura normal de $\{g, h, \dots\}$ en G. Esta definición es equivalente a decir que N es el subgrupo de G generado por $g, h, \dots$ y todos sus conjugados.

Supongamos G dado por la presentación

$$\langle a, b, c, \dots ; P, Q, R, \dots \rangle \tag{1.26}$$

Para dar una presentación de G/N supondremos N expresado como subgrupo normal generado por ciertas palabras $S(a, b, c, \dots), T(a, b, c, \dots), \dots$ (o mejor dicho, por los elementos de G definidos por estas palabras). Se tiene entonces el siguiente resultado:

Teorema 1.5.1 Supongamos que G está presentado por (1.26) bajo la aplicación

$$a \to g, b \to h, c \to k, \dots \tag{1.27}$$

y sea N el subgrupo normal de G generado por $S(g,h,k,\dots), T(g,h,k,\dots), \dots$ Entonces el grupo cociente G/N tiene la presentación

$$\langle a, b, c, \dots ; P, Q, R, \dots, S, T, \dots \rangle \tag{1.28}$$

bajo la aplicación

$$a \to gN, b \to hN, c \to kN, \dots \tag{1.29}$$

Demostración: Bajo la aplicación (1.29), la palabra $W(a,b,c,\dots)$ define el elemento $W(gN, hN, kN, \dots) = W(g,h,k,\dots)N$. Como (1.26) es una presentación de G y N es el subgrupo normal generado por $S(g,h,k,\dots), T(g,h,k,\dots), \dots$, los elementos de G definidos por $P, Q, R, \dots, S, T, \dots$ pertenecen todos a N. Por tanto, $P, Q, R, \dots, S, T, \dots$ son relatores en G/N bajo (1.29), de modo que por el corolario 1.1.6, (1.29) induce un homomorfismo de (1.28) en G/N.

Como G está generado por $g, h, k, \dots$, G/N está generado por $gN, hN, kN, \dots$ y por tanto, el homomorfismo inducido por (1.29) es suprayectivo.

Para ver que es inyectivo, supongamos que $W(a,b,c,\dots)$ define el neutro en G/N bajo (1.29). Entonces $W(g,h,k,\dots)$ pertenece a N. Como N es el subgrupo normal de G generado por $S, T, \dots$

$$W(g,h,k,\dots) = U_1 V_1 U_1^{-1} \cdot \dots \cdot U_r V_r U_r^{-1}$$

donde los U_i son elementos de G y cada V_i es una de las siguientes palabras: $S, S^{-1}, T, T^{-1}, \dots$. Por tanto,

$$W(a,b,c,\dots) \sim U_1 V_1 U_1^{-1} \cdot \dots \cdot U_r V_r U_r^{-1}$$

con respecto a la aplicación (1.27) de G. Por tanto, $W(a,b,c,\dots)$ se puede transformar en $U_1 V_1 U_1^{-1} \cdot \dots \cdot U_r V_r U_r^{-1}$ mediante inserciones y eliminaciones de $P, Q, R, \dots$ y de relatores triviales. Pero $U_1 V_1 U_1^{-1} \cdot \dots \cdot U_r V_r U_r^{-1}$ se puede transformar en la palabra vacía mediante inserciones y eliminaciones de $S, T, \dots$ y de relatores triviales. De este modo, $W(a,b,c,\dots) \sim 1$ en la presentación (1.28) y por tanto, el homomorfismo inducido por (1.29) es inyectivo y en consecuencia hemos visto que es un isomorfismo de (1.28) en G/N. □

1.6. Una aproximación alternativa al concepto de presentación de un grupo.

El teorema 1.5.1 tiene como corolario inmediato el siguiente resultado:

Corolario 1.6.1 Si F es el grupo libre en $a, b, c, \dots$ y N es el subgrupo normal de F generado por $P(a, b, c, \dots), Q(a, b, c, \dots), R(a, b, c, \dots), \dots$, entonces

$$F/N = \langle a, b, c, \dots; P, Q, R, \dots \rangle \tag{1.30}$$

□

Este resultado nos proporciona una manera alternativa de definir el concepto de presentación de un grupo. De hecho, definiendo primero grupo libre podemos tomar (1.30) como definición de la presentación (1.26).

En la presente sección, se introducirá esta aproximación alternativa a los conceptos de grupo libre y presentación de un grupo. Comenzaremos definiendo grupo libre sin apoyarnos en presentaciones de grupos.

Definición 1.6.2 Dado un conjunto X, un grupo libre sobre X es un par (F, i) donde F es un grupo e $i : X \to F$ es una aplicación tal que para todo grupo G y toda aplicación $f : X \to G$ existe un único homomorfismo de grupos $\overline{f} : F \to G$ tal que $f = \overline{f} \circ i$.

Con la anterior definición no es claro que exista grupo libre sobre cualquier conjunto X. Daremos un esquema de la demostración de existencia.

Si $X = \emptyset$ entonces F es el grupo trivial. Si $X \neq \emptyset$ elegiremos un conjunto X' disjunto y biyectivo con X. Elegimos una biyección $X \to X'$ y denotaremos la imagen de $x \in X$ por x^{-1}. Como antes, decimos que una palabra es una secuencia finita $a_1 a_2 \dots a_n$ donde $a_i \in X \cup X'$ y la palabra vacía la denotamos por 1. Una palabra se dirá reducida si para todo $x \in X \cup X'$ se cumple que x y x^{-1} no aparecen consecutivamente.

En particular, la palabra vacía 1 es reducida. Toda palabra no vacía y reducida es de la forma $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ con $n \geq 1$, $x_1, \dots, x_n \in X$, $\epsilon_i = \pm 1$. Denotemos $F(X)$ el conjunto de todas las palabras reducidas en X. Podemos ver $X \subseteq F(X)$ y tenemos la aplicación $i : X \to F$ dada por $x \to x^1 = x$.

Dos palabras reducidas $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$, $y_1^{\eta_1} \dots y_m^{\eta_m}$ son iguales si y sólo si $n = m$, $x_i = y_i$, $\epsilon_i = \eta_i$ para todo i.

Ciertamente, la idea de palabra reducida es la misma que la introducida en la sección 1.3.

Definimos ahora una ley en $F(X)$. Dadas dos palabras reducidas el producto de ambas vendrá dado por la yuxtaposición transformada por ρ para obtener una nueva palabra reducida. (Ver la definición de ρ en la sección 1.3).

Se puede probar que $F(X)$ con el producto que hemos definido es un grupo y además verifica la propiedad de grupo libre sobre X. Luego siempre existe grupo libre sobre cualquier conjunto. El conjunto X se dice sistema de generadores libres de $F(X)$.

Además, como consecuencia de la definición de grupo libre se obtiene también su unicidad salvo isomorfismo.

Se puede probar que todo grupo G es imagen homomorfa de un grupo libre sobre un conjunto X que genere G. Por tanto,$G \cong F/N$ donde $G = \langle X \rangle$, F es el grupo libre sobre X y N es el núcleo del epimorfismo de F en G que sabemos que existe. Luego, para determinar G salvo isomorfismo sólo necesitamos especificar X, F y N. Pero F está determinado por X salvo isomorfismo. Y N está determinado por cualquier subconjunto que lo genere como subgrupo normal de F. Así, si $P, Q, R, \dots$ son palabras en $X = \{a, b, c, \dots\}$ que generan N como subgrupo normal de F, entonces diremos que $\langle a, b, c, \dots ; P, Q, R, \dots \rangle$ es una presentación de G, donde eso significará que G es isomorfo al cociente del grupo libre en $\{a, b, c, \dots\}$ sobre el subgrupo normal generado por las palabras $P, Q, R, \dots$. Esto nos da una manera alternativa de llegar al mismo concepto de presentación de un grupo que ya habíamos definido.

Por último, se puede probar que si X, Y son conjuntos entonces $F(X) \cong F(Y)$ si y sólo si X e Y tienen el mismo cardinal. Como consecuencia de ello podemos definir el rango de un grupo libre F como el cardinal de cualquier sistema de generadores libres de F. Así, dos grupos libres son isomorfos si y sólo si tienen el mismo rango. Esto resuelve el problema del isomorfismo para grupos libres siempre y cuando estén presentados en términos de generadores libres: bastará comprobar que los conjuntos de generadores libres tengan el mismo cardinal.

1.7. Presentaciones de subgrupos.

Sea

$$G = \langle a_1, \dots, a_n ; R_\mu(a_\nu), \dots \rangle \tag{1.31}$$

En la sección 1.5 estudiamos cómo presentar un cociente G/N de G. En esta sección veremos cómo presentar un subgrupo H de G. Para presentar un cociente se necesitaban palabras en los a_ν que generasen N como subgrupo normal de G. Para presentar H requeriremos palabras en los a_ν que generen H, y también un proceso que nos permita "reescribir" una palabra en los a_ν que pertenezca a H en términos de los generadores de H.

Formalmente, si H está generado por las palabras $J_i(a_\nu)$, un proceso de reescritura para H (con respecto a los generadores $J_i(a_\nu)$) es una aplicación

$$\tau : U(a_\nu) \to V(s_i) \tag{1.32}$$

de palabras $U(a_\nu)$ que definen elementos de H en palabras en los símbolos s_i de tal manera que las palabras $U(a_\nu)$ y $V(J_i(a_\nu))$ definen el mismo elemento de H. El siguiente teorema

establece cómo presentar un subgrupo H de G usando los símbolos generadores s_i para los elementos generadores $J_i(a_\nu)$.

Teorema 1.7.1 Sea H un subgrupo del grupo G presentado en (1.31). Si $J_i(a_\nu)$ son generadores de H y τ es un proceso de reescritura para H (con respecto a los generadores $J_i(a_\nu)$), entonces una presentación de H bajo la aplicación $s_i \to J_i(a_\nu)$ se obtiene usando los símbolos s_i como símbolos generadores y las siguientes ecuaciones como conjunto completo de relaciones:

$$s_i = \tau(J_i(a_\nu)) \tag{1.33}$$

$$\tau(U) = \tau(U^*) \tag{1.34}$$

donde $U(a_\nu)$ y $U^*(a_\nu)$ son palabras libremente iguales que definen elementos de H.

$$\tau(U_1 \cdot U_2) = \tau(U_1)\tau(U_2) \tag{1.35}$$

donde $U_1(a_\nu)$ y $U_2(a_\nu)$ definen elementos de H

$$\tau(W R_\mu W^{-1}) = 1 \tag{1.36}$$

donde $R_\mu(a_\nu)$ es uno de los relatores que aparecen en la presentación (1.31) y W es cualquier palabra en los a_ν.

Se puede simplificar la presentación del teorema 1.7.1, eligiendo adecuadamente los generadores y el proceso de reescritura. Tomaremos un transversal a derecha de G módulo H en el que la clase H esté representada por la palabra vacía y denotaremos $\overline{W}(a_\nu)$ el representante de la clase de $W(a_\nu)$ en el transversal elegido.

Teorema 1.7.2 Usando la notación anterior, H está generado por las palabras

$$K a_\nu \cdot \overline{K a_\nu}^{-1} \tag{1.37}$$

donde K recorre los elementos del transversal y a_ν recorre los generadores de G.

Si bien, en general, un subgrupo de un grupo finitamente generado no es finitamente generado, gracias al teorema anterior podemos dar una condición suficiente para que ésto ocurra.

Corolario 1.7.3 Si G es finitamente generado y H es un subgrupo de índice finito, entonces H es finitamente generado.

Demostración: Si G tiene n generadores y H tiene índice j, en (1.37) hay a lo sumo nj generadores para H. □

Corolario 1.7.4 Si introducimos el símbolo generador s_{K,a_ν} para el elemento de H definido por la palabra $Ka_\nu\overline{Ka_\nu}^{-1}$ donde K recorre los elementos del transversal y a_ν recorre los generadores de G y definimos la aplicación τ que lleva una palabra U de la forma $a_{\nu_1}^{\epsilon_1}\dots a_{\nu_r}^{\epsilon_r}(\epsilon_i=\pm 1)$ definiendo un elemento de H a la palabra

$$\tau(U)=s_{K_1,a_{\nu_1}}^{\epsilon_1}s_{K_2,a_{\nu_2}}^{\epsilon_2}\dots s_{K_r,a_{\nu_r}}^{\epsilon_r} \tag{1.38}$$

donde K_j es el representante de la clase del segmento inicial de U que precede a a_{ν_j} si $\epsilon_j=1$, y K_j es el representante de la clase del segmento inicial de U hasta $a_{\nu_j}^{-1}$ incluido si $\epsilon_j=-1$, entonces τ es un proceso de reescritura para H.

Demostración: Para probar que τ es un proceso de reescritura, debemos probar que si $s_{K_j,a_{\nu_j}}$ es reemplazado por $K_ja_{\nu_j}\overline{K_ja_{\nu_j}}^{-1}$ en (1.38) se obtiene una palabra en los a_ν que define el mismo elemento de H que $U(a_\nu)$.

Si denotamos W_j al segmento inicial de U que precede a $a_{\nu_j}^{\epsilon_j}$, entonces

$$K_j=\overline{W_j}\text{ si }\epsilon_j=1$$

y

$$K_j=\overline{W_ja_{\nu_j}^{-1}}\text{ si }\epsilon_j=-1$$

por definición de K_j. Por tanto, en cualquier caso, $s_{K_j,a_{\nu_j}}^{\epsilon_j}$ es reemplazado por $\overline{W_j}a_{\nu_j}^{\epsilon_j}\overline{W_ja_{\nu_j}^{\epsilon_j}}^{-1}$. Pero entonces (1.38) se convierte en

$$\overline{W_1}a_{\nu_1}^{\epsilon_1}\overline{W_1a_{\nu_1}^{\epsilon_1}}^{-1}\cdot\overline{W_2}a_{\nu_2}^{\epsilon_2}\overline{W_2a_{\nu_2}^{\epsilon_2}}^{-1}\dots\overline{W_r}a_{\nu_r}^{\epsilon_r}\overline{W_ra_{\nu_r}^{\epsilon_r}}^{-1},$$

que define el mismo elemento que $U(a_\nu)$. □

Un proceso de reescritura τ obtenido a partir de una función de clases a derecha se dice proceso de reescritura de Reidemeister. Como ejemplo de reescritura con un proceso de Reidemeister, supongamos que $a_1^2a_2^{-1}a_3$ define un elemento de H. Entonces

$$\tau(a_1a_1a_2^{-1}a_3)=s_{\overline{1},a_1}s_{\overline{a_1},a_1}s^{-1}_{\overline{a_1^2a_2^{-1}},a_2}s_{\overline{a_1^2a_2^{-1}},a_3}$$

Obsérvese que el cálculo de $\tau(U)$ se puede llevar a cabo reemplazando cada símbolo a_ν^ϵ por el s-símbolo adecuado s_{K,a_ν}^ϵ.

Usando un proceso de reescritura de Reidemeister, la presentación del teorema 1.7.1 se puede simplificar en gran medida.

Teorema 1.7.5 Sea τ el proceso de reescritura de Reidemeister dado por (1.38) para un subgrupo H de un grupo G. Si G tiene la presentación (1.31), entonces H tiene la presentación

$$\langle s_{K,a_\nu},\dots;s_{K,a_\nu}=\tau(Ka_\nu\overline{Ka_\nu}^{-1}),\dots,\tau(KR_\mu K^{-1}),\dots\rangle \tag{1.39}$$

bajo la aplicación $s_{K,a_\nu} \to Ka_\nu\overline{Ka_\nu}^{-1}$ donde K pertenece al transversal elegido, a_ν es uno de los generadores de (1.31) y R_μ una de las relaciones en la presentación (1.31).

A partir del teorema 1.7.5 se obtiene de forma inmediata el siguiente corolario:

Corolario 1.7.6 Si G es finitamente presentado y H es un subgrupo de índice finito, entonces H es finitamente presentado. □

La presentación lograda en 1.7.5 se puede simplificar aún más tomando un tipo especial de transversales a derecha. Diremos que un transversal a derecha es de Schreier (o que es un sistema de representantes de Schreier) si todo segmento inicial de un elemento del transversal vuelve a pertenecer al transversal. Un proceso de reescritura de Reidemeister que usa un sistema de Schreier se dice proceso de reescritura de Reidemeister-Schreier. Lo primero que haremos será garantizar que siempre existe sistema de Schreier. Es más, en el siguiente lema encontraremos, para cualquier grupo G y cualquier subgrupo H de G, un sistema de Schreier minimal, es decir, un sistema de Schreier donde cada representante tiene una longitud que no excede a la de ninguna de las palabras de su clase. No todo sistema de Schreier es minimal.

Lema 1.7.7 Sea G un grupo con la presentación (1.31) y sea H un subgrupo de G. Entonces existe algún sistema de representantes de Schreier de G módulo H.

Demostración: En esta demostración usaremos el concepto de longitud de una clase, que definiremos como la menor de las longitudes de los elementos de la clase.

Elegimos la palabra vacía como representante de H, la clase de longitud cero. Si S_1 es una clase de longitud uno, elegimos cualquier palabra de longitud 1 en S_1 como representante. Si S_2 tiene longitud dos, seleccionemos una palabra b_1b_2 de longitud dos en S_2 (b_1 y b_2 son los generadores en (1.31) o sus inversos). Pero $\overline{b_1}b_2$ está en S_2 pues su representante es el mismo que el de b_1b_2, y como $\overline{b_1}$ tiene longitud a lo sumo uno, $\overline{b_1}b_2$ tiene longitud dos, de modo que elegimos $\overline{b_1}b_2$ como representante de S_2. En general, suponiendo que hemos elegido representantes para todas las clases de longitud menor que r, si S_r es una clase de longitud r y $b_1 \dots b_r$ es una palabra en S_r, elegimos $\overline{b_1 \dots b_{r-1}}b_r$ (que tiene longitud r) como representante de S_r. Por construcción se cumple que si eliminamos el último símbolo de un representante obtenemos otro representante, lo que garantiza que cualquier segmento inicial de un representante es un representante. □

Usando un proceso de reescritura de Reidemeister-Schreier, se pueden simplificar las relaciones (1.33) de la presentación de H.

Teorema 1.7.8 Sea G un grupo con la presentación (1.31) y sea H un subgrupo de G. Si τ es un proceso de reescritura de Reidemeister-Schreier. entonces H tiene la presentación

$$\langle s_{K,a_\nu}, \dots ; s_{M,a_\lambda}, \dots , \tau(KR_\mu K^{-1}), \dots \rangle \tag{1.40}$$

donde K es un representante de Schreier, a_ν es uno de los generadores de (1.31) y R_μ una de las relaciones en la presentación (1.31), y M es un representante de Schreier y a_λ un generador tales que

$$Ma_\lambda \approx \overline{Ma_\lambda} \tag{1.41}$$

Corolario 1.7.9 Un subgrupo de un grupo libre es libre.

Demostración: Si G es un grupo libre, se puede presentar con un conjunto vacío de relaciones. Por tanto, los relatores que aparecen en la presentación (1.40) serán solamente algunos de los generadores del subgrupo. Usando una transformación de Tietze para eliminar los generadores que aparecen como relatores, junto con el correspondiente relator, resulta una presentación con un conjunto completo de relaciones que es vacío. Por tanto, el subgrupo es libre. □

Veamos ahora un ejemplo ilustrativo que muestre cómo el uso de representantes de Schreier simplifica la presentación de subgrupos. Tomemos $G = \langle x, y; x^2, y^3 \rangle$ y $H = G'$. El conjunto $T_1 = \{1, x, y, xy, y^2, yxy\}$ es un transversal a derecha de G módulo H, pero no es de Schreier puesto que yx es un segmento inicial de yxy que no pertenece a T_1. Vamos a indicar cómo aplicar los resultados de esta sección para obtener una presentación de H.

De acuerdo con el teorema 1.7.5, una presentación de H viene dada por los generadores $s_{1,x}, s_{1,y}, s_{x,x}, s_{x,y}, s_{y,x}, s_{y,y}, s_{xy,x}, s_{xy,y}, s_{y^2,x}, s_{y^2,y}, s_{yxy,x}, s_{yxy,y}$ y por las relaciones que calcularemos a continuación:

Puesto que $\tau(1x\overline{1x}^{-1}) = \tau(xx^{-1}) = s_{1,x}s^{-1}_{\overline{xx^{-1}},x} = s_{1,x}s^{-1}_{1,x}$, se tiene que $s_{1,x}s^{-1}_{1,x} = s_{1,x}$ es una relación en H.

Del mismo modo, como $\tau(1y\overline{1y}^{-1}) = \tau(yy^{-1}) = s_{1,y}s^{-1}_{\overline{yy^{-1}},y} = s_{1,y}s^{-1}_{1,y}$, se tiene que $s_{1,y}s^{-1}_{1,y} = s_{1,y}$ es una relación en H.

Análogamente $\tau(xx\overline{x}\overline{x}^{-1}) = \tau(x^2) = s_{1,x}s_{x,x}$ da lugar a la relación $s_{1,x}s_{x,x} = s_{x,x}$,
$\tau(xy\overline{xy}^{-1}) = \tau(xyy^{-1}x^{-1}) = s_{1,x}s_{x,y}s^{-1}_{x,y}s^{-1}_{1,x}$ da lugar a la relación $s_{1,x}s_{x,y}s^{-1}_{x,y}s^{-1}_{1,x} = s_{x,y}$,
$\tau(yx\overline{yx}^{-1}) = \tau(yxy^{-1}x^{-1}) = s_{1,y}s_{y,x}s^{-1}_{x,y}s^{-1}_{1,x}$ da lugar a la relación $s_{1,y}s_{y,x}s^{-1}_{x,y}s^{-1}_{1,x} = s_{y,x}$,
y procediendo del mismo modo se obtienen 19 relaciones más de este tipo, a las que hay que añadir otras 24 relaciones, de las cuales escribiremos parte a continuación. Éstas últimas 24 relaciones se obtienen sabiendo que:
$\tau(1x^21^{-1}) = \tau(x^2) = s_{1,x}s_{x,x}$,
$\tau(1y^31^{-1}) = \tau(y^3) = s_{1,y}s_{y,y}s_{y^2,y}$,

$\tau(xx^2x^{-1}) = s_{1,x}s_{x,x}s_{x^2,x}s_{1,x}^{-1}$,
$\tau(xy^3x^{-1}) = s_{1,x}s_{x,y}s_{xy,x}s_{yxy,y}s_{1,x}^{-1}$,
...

De aquí se obtienen, como aunciábamos, las relaciones

$$s_{1,x}s_{x,x} = 1, s_{1,y}s_{y,y}s_{y^2,y} = 1, s_{1,x}s_{x,x}s_{x^2,x}s_{1,x}^{-1} = 1, s_{1,x}s_{x,y}s_{xy,x}s_{yxy,y}s_{1,x}^{-1} = 1, \ldots$$

Esto nos conduce a una presentación de H con 12 generadores y 48 relaciones, que se puede simplificar en gran medida, hasta tal punto que probaremos que H es un grupo libre en dos generadores.

Si utilizamos un sistema de representantes de Schreier, por ejemplo $T_2 = \{1, x, y, xy, y^2, xy^2\}$, se obtiene una presentación más sencilla para H. En este caso, de acuerdo con el teorema 1.7.8, los generadores son $s_{1,x}, s_{1,y}, s_{x,x}, s_{x,y}, s_{y,x}, s_{y,y}, s_{xy,x}, s_{xy,y}, s_{y^2,x}, s_{y^2,y}, s_{xy^2,x}, s_{xy^2,y}$.

El primer, segundo, cuarto, sexto y octavo s-símbolos tienen la propiedad 1.41, luego son relatores. Los restantes relatores de la presentación son los siguientes (omitimos cualquier s-símbolo que ya sepamos que es relator):
$\tau(1x^21^{-1}) = \tau(x^2) = s_{x,x}$
$\tau(xx^2x^{-1}) \approx \tau(x^2)$
$\tau(yx^2y^{-1}) = s_{y,x}s_{xy,x}$
$\tau(xyx^2y^{-1}x^{-1}) = s_{xy,x}s_{y,x}$
$\tau(y^2x^2y^{-2}) = s_{y^2,x}s_{xy^2,x}$
$\tau(xy^2x^2y^{-2}x^{-1}) = s_{xy^2,x}s_{y^2,x}$
$\tau(1y^31^{-1}) = \tau(y^3) = s_{y^2,y}$
$\tau(xy^3x^{-1} = s_{xy^2,y}$
$\tau(yy^3y^{-1}) \approx \tau(y^3)$
$\tau(xyy^3y^{-1}x^{-1}) \approx \tau(xy^3x^{-1})$
$\tau(y^2y^3y^{-2}) \approx \tau(y^3)$
$\tau(xy^2y^3y^{-2}x^{-1}) \approx \tau(xy^3x^{-1})$

De estos relatores se deduce que $s_{xy,x} = s_{y,x}^{-1}$ y $s_{xy^2,x} = s_{y^2,x}^{-1}$. Aplicando transformaciones de Tietze, se pueden eliminar todos los generadores excepto $s_{y,x}$ y $s_{y^2,x}$, y todos lo relatores, de modo que H es el grupo libre en dos generadores.

Capítulo 2

Producto libre y producto amalgamado de grupos.

2.1. Producto libre de grupos.

En el capítulo anterior hemos introducido los problemas de Dehn y los hemos estudiado en el caso de grupos libres presentados en términos de generadores libres. A lo largo de este segundo capítulo introduciremos ciertas construcciones de grupos que aparecen de modo natural en áreas como la topología, y estudiaremos el problema de la palabra y de la conjugación para estos grupos. En concreto, las construcciones que manejaremos serán el producto libre de grupos y el producto amalgamado. Dedicaremos una sección a cada uno de ellos, comenzando por el producto libre que se define del siguiente modo:

Definición 2.1.1 El producto libre $A * B$ de los grupos

$$A = \langle a_1, \ldots, a_n; R_1(a_\nu), \ldots, R_p(a_\nu) \rangle \tag{2.1}$$

y

$$B = \langle b_1, \ldots, b_m; S_1(b_\mu), \ldots, S_q(b_\mu) \rangle \tag{2.2}$$

es el grupo

$$A * B = \langle a_1, \ldots, a_n, b_1, \ldots, b_m; R_1(a_\nu), \ldots, R_p(a_\nu), S_1(b_\mu), \ldots, S_q(b_\mu) \rangle \tag{2.3}$$

Se dice que A y B son los factores libres de $A * B$.

Esta definición de producto libre se basa en una presentación concreta de los factores, por lo que no está claro en principio que el producto libre no dependa de la presentación que se considere para los factores. Por eso, lo primero que haremos antes de continuar es comprobar que, en efecto, no depende y por tanto el producto libre de dos grupos está bien definido.

Teorema 2.1.2 El producto libre $A * B$ está unívocamente determinado por los grupos A y B. Además, $A * B$ está generado por dos subgrupos $\overline{A}, \overline{B}$ que son isomorfos a A, B respectivamente y que cumplen $\overline{A} \cap \overline{B} = 1$.

Demostración: Supongamos que A y B tienen las presentaciones $\mathcal{P}_1$ y $\mathcal{P}_2$ dadas en (2.1) y (2.2), y también las presentaciones $\mathcal{P}_1'$ y $\mathcal{P}_2'$ siguientes:

$$A \cong \langle a_1', \dots, a_s'; R_1'(a_\sigma'), \dots \rangle \tag{2.4}$$

$$B \cong \langle b_1', \dots, b_t'; S_1'(b_\tau'), \dots \rangle \tag{2.5}$$

Veamos entonces que la presentación $\mathcal{P}$ dada en (2.3) y la presentación

$$\langle a_1', \dots, a_s', b_1', \dots, b_t'; R_1'(a_\sigma'), \dots, S_1'(b_\tau'), \dots \rangle \tag{2.6}$$

definen el mismo grupo salvo isomorfismo.

Los isomorfismos $\varphi_{\mathcal{P}_!,\mathcal{P}_1'}$ y $\varphi_{\mathcal{P}_2,\mathcal{P}_2'}$ (ver 1.1.4) definen de forma natural un homomorfismo entre $G(\mathcal{P})$ y $G(\mathcal{P}')$ porque los relatores de la presentación (2.3) tienen por imagen relatores en el grupo (2.6), aunque no sean necesariamente los que aparecen en la presentación (2.6). Este homomorfismo tiene inverso, que viene determinado por los inversos de $\varphi_{\mathcal{P}_!,\mathcal{P}_1'}$ y $\varphi_{\mathcal{P}_2,\mathcal{P}_2'}$. Por tanto, $A * B$ está unívocamente determinado, salvo isomorfismo, por A y B.

Sea $\overline{A}$ el subgrupo de (2.3) generado por $a_1, \dots, a_n$ y sea $\overline{B}$ el subgrupo de (2.3) generado por $b_1, \dots, b_m$. Claramente $A * B$ está generado por $\overline{A}$ y $\overline{B}$. Además, la aplicación $a_\nu \to a_\nu$ de (2.1) en (2.3) es un homomorfismo de A en $A * B$ cuya imagen es $\overline{A}$. El homomorfismo de $A * B$ en A dado por $a_\nu \to a_\nu$, $b_\mu \to 1$ lleva $\overline{A}$ sobre A y es el inverso del homomorfismo anterior. Por tanto $\overline{A} \cong A$, y análogamente $\overline{B} \cong B$.

Por último, si $g \in \overline{A} \cap \overline{B}$ entonces el homomorfismo de $A * B$ en A dado por $a_\nu \to a_\nu$, $b_\mu \to 1$ lleva g a 1 pues $g \in \overline{B}$. Pero la restricción de este homomorfismo a $\overline{A}$ es inyectiva, de modo que $g = 1$. Por tanto, $\overline{A} \cap \overline{B} = 1$. □

Puesto que $\overline{A} \cong A$, $\overline{B} \cong B$, se suele identificar $\overline{A}$ con A y $\overline{B}$ con B y considerar A, B como subgrupos de $A * B$.

El producto libre de A y B cumple la siguiente propiedad: existen homomorfismos $\tau_A : A \to A * B, \tau_B : B \to A * B$ tales que para cualquier grupo G y para cualesquiera homomorfismos $\alpha : A \to G, \beta : B \to G$ existe un único homomorfismo $\gamma : A * B \to G$ cumpliendo $\alpha = \gamma \circ \tau_A$ y $\beta = \gamma \circ \tau_B$.

Ciertamente, si tomamos como τ_A y τ_B los homomorfismos inducidos por las incluciones de los generadores de A y B, respectivamente, en $A * B$, se tiene que para cualesquiera homomorfismos α, β de A y B, respectivamente, en un grupo G, la aplicación γ dada por $\gamma(a_\nu) = \alpha(a_\nu), \gamma(b_\mu) = \beta(b_\mu)$ define un homomorfismo de $A * B$ en G y es claro que es el único que verifica $\alpha = \gamma \circ \tau_A$ y $\beta = \gamma \circ \tau_B$.

Una vez definido el producto libre de grupos, nos centraremos en estudiar el problema de la palabra y de la conjugación para esta construcción.

Definición 2.1.3 Si $g \neq 1$ está en $A * B$ y es tal que $g \in A$ ó $g \in B$, entonces el factor libre que contiene a g se denotará $F(g)$. Obviamente, $F(g)$ será A ó B. Si W es una palabra únicamente en los símbolos a_ν, diremos entonces que $F(W) = A$. Análogamente, $F(W) = B$ si W es una palabra sólo en los símbolos b_μ. Esta notación la usaremos también cuando W sea un relator, siempre que W no sea la palabra vacía.

Para grupos libres obtuvimos una forma canónica de escribir los elementos: todo elemento estaba definido por una única palabra reducida. Gracias a esta forma de representar los elementos logramos una solución sencilla al problema de la palabra para grupos libres. En lo que sigue, el objetivo será resolver el problema de la palabra para productos libres de grupos, y para ello comenzaremos buscando una forma adecuada de representar los elementos de $A * B$. El papel que las palabras reducidas jugaban en los grupos libres lo desempeñarán aquí las secuencias reducidas.

Definición 2.1.4 Una secuencia de elementos $g_1, \ldots, g_n \in A * B$ se dice reducida si $g_i \neq 1$ para todo $i = 1, \ldots, n$, g_i pertenece a $A \cup B$ para todo $i = 1, \ldots, n$ y $F(g_i) \neq F(g_{i+1})$ para todo $i = 1, \ldots, n-1$.

Por ejemplo, tomemos $A = \langle a; a^3 \rangle$, $B = \langle b; b^4 \rangle$. Entonces los elementos de A son $1, a, a^2$, los de B son $1, b, b^2, b^3$ y $A * B = \langle a, b; a^3, b^4 \rangle$. La secuencia b^2, a, b^3, a^2 es reducida; sin embargo, la secuencia $a^2, 1, b$ no lo es pues el segundo término es 1, y tampoco lo es la secuencia b, a, a^2 pues a y a^2 son términos consecutivos que pertenecen al mismo factor libre.

Recordemos que la longitud de una palabra es el número de símbolos que intervienen en ella. A partir de ahora, para trabajar con productos libres, nos será útil considerar otra longitud, que para evitar confusiones llamaremos longitud silábica.

Definición 2.1.5 Sea $W(a_\nu, b_\mu)$ una palabra en $a_1, \ldots, a_n, b_1, \ldots, b_m$. Si $W = W_1 \ldots W_r$ donde cada W_i es una palabra sólo en los a_ν o sólo en los $b\mu$, ningún W_i es la palabra vacía (aunque W_i pueda definir el neutro de $A * B$), y W_i y W_{i+1} no están las dos en el mismo factor libre de $A * B$, entonces diremos que la longitud silábica $\lambda(W)$ de W en A y B es r y que $W_1, \ldots, W_r$ son las sílabas de W.

Para evitar confusiones, a la longitud que mide el número de símbolos en la palabra la llamaremos en adelante longitud en las letras. Veamos un ejemplo que ilustre la diferencia entre ambas longitudes:

Si $A = \langle a_1, a_2, a_3; a_1^2 a_2^3 a_3^2 \rangle$ y $B = \langle b_1, b_2; b_1^2 b_2^2 \rangle$ entonces obtenemos que

$$A * B = \langle a_1, a_2, a_3, b_1, b_2; a_1^2 a_2^3 a_3^2, b_1^2 b_2^2 \rangle.$$

Y si consideramos la palabra $W = a_1 a_2^{-1} b_2^2 a_3^3$ observamos que tiene longitud en las letras igual a 7 y longitud silábica igual a 3, donde las sílabas son $W_1 = a_1 a_2^{-1}, W_2 = b_2^2, W_3 = a_3^3$.

Entenderemos por longitud silábica de un elemento $g \in A * B$ la menor de las longitudes silábicas de todas las palabras que definen g. De este modo, el elemento neutro 1 de $A * B$ tiene longitud silábica 0, cualquier elemento $g \neq 1$ que pertenezca a un factor libre tiene longitud silábica 1 y cualquier elemento que no esté ni en A ni en B tiene longitud silábica mayor o igual que 2.

Ahora ya estamos en condiciones de enunciar y demostrar el teorema que nos proporcione la forma canónica de representar los elementos de $A * B$.

Teorema 2.1.6 Todo elemento $g \in A*B$ se puede expresar de forma única como un producto

$$g = g_1 \dots g_r \tag{2.7}$$

donde $g_1, \dots, g_r$ es una secuencia reducida.

Demostración: Como $A*B$ está generado por A y B, todo elemento g se puede expresar como un producto $h_1 \dots h_n$, donde h_i pertenece a A o a B. Sea $g_1 \dots g_r$ un producto de esa forma que exprese g con el menor número r de términos. Entonces $g_1, \dots, g_r$ es una secuencia reducida, ya que si $g_i = 1$ entonces $g_1 \dots g_{i-1} g_{i+1} \dots g_r$ sería un producto que expresa g con menos de r términos; y si g_i y g_{i+1} perteneciesen al mismo factor libre entonces $g_1 \dots g_{i-1}(g_i g_{i+1}) \dots g_r$ sería un producto que expresa g con menos de r términos. Por tanto g se puede expresar en la forma (2.7).

Falta probar la unicidad. Para ello vamos a introducir un proceso concreto ρ para "reducir" una palabra a una secuencia reducida. La forma reducida $\rho(g_1, \dots, g_n)$ de una secuencia de elementos $g_1, \dots, g_n$ donde g_i está en A o en B (no necesariamente de forma alternada) se define de la siguiente manera:

$$\rho(\text{secuencia vacía}) = \text{secuencia vacía}$$

$$\rho(g_1) = \begin{cases} \text{secuencia vacía} & \text{si } g_1 = 1 \\ g_1 & \text{si } g_1 \neq 1 \end{cases}$$

Si $\rho(g_1, \dots, g_n) = h_1, \dots, h_r$ entonces:

$$\rho(g_1, \dots, g_n, g_{n+1}) = \begin{cases} h_1, \dots, h_r & \text{si } g_{n+1} = 1 \\ h_1, \dots, h_{r-1} & \text{si } g_{n+1} = h_r^{-1} \\ h_1, \dots, h_r \cdot g_{n+1} & \text{si } g_{n+1} \neq h_r^{-1} \text{ pero } F(g_{n+1}) = F(h_r) \\ h_1, \dots, h_r, g_{n+1} & \text{si } F(g_{n+1}) \neq F(h_r) \end{cases}$$

Por último, ρ se define para palabras de la siguiente manera: si $W_1, \ldots, W_n$ son las sílabas de W y g_i es el elemento de $A \cup B$ definido por W_i, entonces $\rho(W_1 \ldots W_n) = \rho(g_1, \ldots, g_n)$.

Se cumplen las siguientes propiedades:

1. $\rho(g_1, \ldots, g_n)$ es una secuencia reducida de longitud a lo sumo n.
2. Si $\rho(g_1, \ldots, g_n) = h_1, \ldots, h_r$ entonces $g_1 \ldots g_n = h_1 \ldots h_r$.
3. Si $g_1, \ldots, g_n$ es una secuencia reducida, entonces $\rho(g_1, \ldots, g_n) = g_1, \ldots, g_n$.
4. $\rho(g_1, \ldots, g_k, g_{k+1}, \ldots, g_n) = \rho(\rho(g_1, \ldots, g_k), g_{k+1}, \ldots, g_n)$.
5. $\rho(g_1, \ldots, g_n, 1) = \rho(g_1, \ldots, g_n)$.
6. $\rho(g_1, \ldots, g_i, 1, g_{i+1}, \ldots, g_n) = \rho(g_1, \ldots, g_i, g_{i+1}, \ldots, g_n)$.
7. Si $F(g_n) = F(g_{n+1})$, entonces $\rho(g_1, \ldots, g_n, g_{n+1}) = \rho(g_1, \ldots, g_n \cdot g_{n+1})$.
8. Si $F(g_i) = F(g_{i+1})$, entonces $\rho(g_1, \ldots, g_i, 1, g_{i+1}, \ldots, g_n) = \rho(g_1, \ldots, g_i \cdot g_{i+1}, \ldots, g_n)$

Usaremos estas propiedades,que se obtienen mediante inducción, para probar el teorema. Supongamos que $g_1, \ldots, g_r$ y $h_1, \ldots, h_s$ son secuencias reducidas cumpliendo $g_1 \ldots g_r = h_1 \ldots h_s$. Los g_i, h_j están definidos por palabras de una sílaba U_i, V_j, respectivamente. $U = U_1 \ldots U_r$ y $V = V_1 \ldots V_s$ son palabras en los símbolos a_ν, b_μ que definen el mismo elemento de $A * B$. Por tanto, podemos obtener V a partir de U mediante inserciones y eliminaciones de los relatores $R(a_\nu), R(a_\nu)^{-1}, \ldots, S(b_\mu), S(b_\mu)^{-1}, \ldots$ o de relatores triviales $a_\nu^\epsilon a_\nu^{-\epsilon}$, $b_\mu^\epsilon b_\mu^{-\epsilon}$ ($\epsilon = \pm 1$).

Probaremos que ρ de una palabra no varía por inserción o eliminación de relatores de una sílaba. Una vez hayamos probado esto, tendremos que, puesto que podemos obtener V a partir de U mediante inserciones y eliminaciones de relatores de una sílaba, $\rho(U) = \rho(V)$. Pero $\rho(U_1 \ldots U_r) = \rho(g_1, \ldots, g_r) = g_1, \ldots, g_r$ y $\rho(V_1 \ldots V_s) = \rho(h_1, \ldots, h_s) = h_1, \ldots, h_s$ por la propiedad 3. Por tanto, $g_1, \ldots, g_r = h_1, \ldots, h_s$ y el teorema estaría probado.

Es decir, sólo resta probar que ρ de una palabra no varía por inserción o eliminación de relatores de una sílaba. Basta considerar el caso de la inserción, puesto que si Y se obtiene de X eliminando un relator de una sílaba, X se obtiene de Y insertándolo.

Sea $X = X_1 \ldots X_n$ una palabra en los símbolos a_ν, b_μ, donde $X_1, \ldots, X_n$ son las sílabas de X y k_i es el elemento de $A * B$ definido por X_i. Si Y se obtiene a partir de X por inserción de un relator P de una sílaba, se pueden dar las siguientes posibilidades: o bien P se inserta al principio o al final de X, o bien entre sílabas consecutivas X_i, X_{i+1} de X, o bien en medio de una sílaba X_i.

Si P tiene a su derecha o a su izquierda una sílaba de X que está en el mismo factor libre que P o si P se inserta en medio de una sílaba que está en su mismo factor libre, entonces la secuencia de elementos definidos por las sílabas de Y es la misma que la secuencia de elementos definidos por las sílabas de X. Por tanto, $\rho(Y) = \rho(k_1, \ldots, k_n) = \rho(X)$.

Las posibilidades restantes son que P se inserte antes de X_1 y $F(X_1) \neq F(P)$, o que se

inserte después de X_n y $F(X_n) \neq F(P)$ o bien que $X_i = X_i' X_i''$ con $F(X_i) \neq F(P)$ y P se inserte antes de X_i''. En cada uno de estos tres casos tenemos lo siguiente:

$\rho(Y) = \rho(PX_1 \dots X_n) = \rho(1, k_1, \dots, k_n) = \rho(k_1, \dots, k_n) = \rho(X)$ por la propiedad 6.

$\rho(Y) = \rho(X_1 \dots X_n P) = \rho(k_1, \dots, k_n, 1) = \rho(k_1, \dots, k_n) = \rho(X)$ por la propiedad 6.

$\rho(Y) = \rho(X_1 \dots X_i' P X_i'' \dots X_n) = \rho(k_1, \dots, k_i', 1, k_i'', \dots, k_n) = \rho(k_1, \dots, k_i' \cdot k_i'', \dots, k_n) = \rho(k_1, \dots, k_i, \dots, k_n) = \rho(X)$ por la propiedad 8.

Esto finaliza la demostración. □

El teorema anterior nos dice que para resolver el problema de la palabra en un producto libre $A*B$ es necesario saber resolver el problema de la palabra en A y en B. Ciertamente, dada una palabra W que representa un elemento de $A * B$, para saber si representa el elemento neutro necesitamos ver si la secuencia reducida $\rho(W)$ es vacía, para lo que, debido a la definición de ρ necesitamos ver si las sílabas de W definen el elemento neutro en los factores libres, es decir, necesitamos resolver el problema de la palabra en A y en B.

Veremos en el siguiente corolario que las propiedades que hemos visto que verifica el producto libre, en realidad lo caracterizan.

Corolario 2.1.7 Sean A, B subgrupos de un grupo G tales que $A \cap B = 1$ y supongamos que todo elemento de G se puede escribir de forma única como un producto $g_1 \dots g_r$ donde $(g_1, \dots, g_r)$ es una secuencia reducida. Entonces G es el producto libre de A y B.

Demostración: Sea $A = \langle a_1, \dots, a_n; R(a_\nu), \dots \rangle$ y $B = \langle b_1, \dots, b_m; S(b_\mu), \dots \rangle$. Entonces $a_1, \dots, a_n, b_1, \dots, b_m$ generan G pues por hipótesis todo elemento de G es producto de elementos en A y en B; y $R(a_\nu), \dots, S(b_\mu), \dots$ son relatores en G pues definen el neutro en los subgrupos A y B, respectivamente, luego también en G. Para probar que $G = A * B$, basta ver que todo relator $W(a_\nu, b_\mu)$ se puede derivar a partir de $R(a_\nu), \dots, S(b_\mu), \dots$. Sea $W = W_1 \dots W_r$ donde W_i son las sílabas de W. Usaremos inducción en la longitud silábica de W. Si $r = 0$, W es derivable de $R(a_\nu), \dots, S(b_\mu), \dots$.

Supongamos que cualquier relator con menos de r sílabas es derivable de las palabras $R(a_\nu), \dots, S(b_\mu), \dots$ y consideremos un relator de G, $W_1 \dots W_r$, de r sílabas. Sea g_i el elemento de G definido por W_i. Si $g_i \neq 1$ para todo i, entonces $(g_1, \dots, g_r)$ es una secuencia reducida con $r \geq 1$, luego por la unicidad no puede definir el neutro. Por tanto, $g_i = 1$ para algún i. Pero entonces W_i es un relator en A ó B, y por tanto, derivable de las relaciones $R(a_\nu), \dots$ o de las relaciones $S(b_\mu), \dots$. Consideremos ahora $W_1 \dots W_{i-1} W_{i+1} \dots W_r$, que ha de ser un relator y, por hipótesis de inducción, derivable de las relaciones $R(a_\nu), \dots, S(b_\mu), \dots$. Por tanto, cualquier relator en G es derivable de $R(a_\nu), \dots, S(b_\mu), \dots$. □

Corolario 2.1.8 Sea $G = A * B$ y sean C y D subgrupos de A y B, respectivamente. Si H es el subgrupo de G generado por C y D entonces $H = C * D$.

Demostración: Puesto que C y D generan H, cada elemento de H es un producto $h_1 \dots h_s$ donde cada h_i pertenece a C ó a D y se puede comprobar, del mismo modo que en la demostración de 2.1.6, que todo elemento de H se puede expresar como una secuencia reducida $(g_1 \dots g_r)$ en $C * D$, que por tanto, es también una secuencia reducida en $A * B$. Luego, la representación de un elemento de H como producto de una secuencia reducida en $C * D$ es única. Además, $C \cap D \subseteq A \cap B = 1$, luego por el corolario 2.1.7, $H = C * D$. □

Corolario 2.1.9 Si $(g_1, \dots, g_r)$ es una secuencia reducida en $A*B$, entonces $\lambda(g_1 \dots g_r) = r$.

Demostración: Si $W(a_\nu, b_\mu)$ define $g_1 \dots g_r$, entonces la secuencia $\rho(W(a_\nu, b_\mu))$ no tiene más términos que el número de sílabas en $W(a_\nu, b_\mu)$ (por la propiedad 1 de ρ). Pero si U_i es una palabra de una sílaba definiendo g_i, entonces

$$\rho(U_1, \dots, U_r) = \rho(g_1, \dots, g_r) = (g_1, \dots, g_r)$$

Como $U_1 \dots U_r$ y W definen el mismo elemento de $A * B$, $\rho(W) = \rho(U_1 \dots U_r)$ y por tanto, $\lambda(W) \geq r$. Luego r es la menor longitud silábica de una palabra que defina $g_1 \dots g_r$. □

Corolario 2.1.10 Un elemento de orden finito en $A * B$ es un conjugado de un elemento de orden finito en A ó en B.

Demostración: Sea g un elemento de orden finito en $A * B$. Usemos inducción en la longitud silábica de g. Si la longitud silábica de g es cero o uno, la afirmación es trivialmente cierta.

Si $g = g_1 \dots g_r$ es la forma reducida de g en $A * B$ y g_1, g_r pertenecen a factores libres diferentes, entonces para todo entero positivo k se tiene que

$$g^k = g_1 \dots g_r g_1 \dots g_r \dots g_1 \dots g_r$$

es la forma reducida de g^k en $A * B$. Luego en este caso, g no puede tener orden finito. Esto significa que g_1, g_r pertenecen al mismo factor libre, luego

$$g_1^{-1} g g_1 = g_2 \dots g_{r-1}(g_r g_1)$$

tiene menor longitud silábica que g y también es de orden finito. Por la hipótesis de inducción, $g_1^{-1} g g_1$ es conjugado de algún elemento en un factor libre, luego también lo es g. □

Corolario 2.1.11 Si A y B son grupos no triviales, entonces $A * B$ contiene algún elemento de orden infinito.

Demostración: Basta tomar $1 \neq x \in A, 1 \neq y \in B$ y considerar $g = xy \in A * B$. Para todo entero positivo k, $g^k = xyxy \dots xy$ es la forma reducida de g^k, luego es distinto de 1. Así, g tiene orden infinito. □

Corolario 2.1.12 Si $g \in A * B$ y $a, gag^{-1} \in A$, $a \neq 1$ entonces $g \in A$. En particular, $g \notin A \Rightarrow gAg^{-1} \cap A = 1$.

Demostración: Usaremos inducción en la longitud silábica de g. Si $\lambda(g) = 0$, se cumple trivialmente. Supongamos que $g = g_1 \dots g_r$ con $r \geq 1$ es la forma reducida de g en $A * B$. Si $g_r \notin A$, entonces

$$gag^{-1} = g_1 \dots g_r a g_r^{-1} \dots g_1^{-1}$$

es la forma reducida de gag^{-1} y tiene longitud silábica estrictamente mayor que 1, luego $gag^{-1} \notin A$, contrariamente a la hipótesis. Así, necesariamente, $g_r \in A$ y $g_r a g_r^{-1} \in A$ y es distinto de 1. Como

$$(g_1 \dots g_{r-1})(g_r a g_r^{-1})(g_1 \dots g_{r-1})^{-1} \in A$$

entonces, por la hipótesis de inducción, $g_1 \dots g_{r-1} \in A$, luego $g = g_1 \dots g_r \in A$. □

Corolario 2.1.13 Si $A \neq 1, B \neq 1$ entonces $Z(A * B) = 1$.

Demostración: Sea $g \in Z(A * B)$. Como $A \neq 1$ existe $1 \neq a \in A$, y por el corolario 2.1.12, $g \in A$ pues $gag^{-1} = a \in A$ ya que $g \in Z(A * B)$. El resultado del corolario 2.1.12 es igualmente válido sustituyendo A por B, de modo que por un razonamiento análogo $g \in B$. Luego $g \in A \cap B = 1$. □

Corolario 2.1.14 Sean u, v elementos no triviales de $A * B$ que conmutan. Entonces o bien u y v están en el mismo conjugado de un factor libre, o bien u y v son potencias de un mismo elemento w.

Demostración: Si uno de los elementos, por ejemplo v, está en el conjugado de algún factor libre, por ejemplo, gAg^{-1}, entonces $g^{-1}vg \in A$ y es distinto de 1 pues $v \neq 1$. Como $u^{-1}vu = v$, se tiene $(g^{-1}ug)^{-1} \cdot g^{-1}vg \cdot g^{-1}ug = g^{-1}vg$ que está en A. Por tanto, por el corolario 2.1.12, $g^{-1}ug \in A$, luego $u, v \in gAg^{-1}$.

Por tanto, sólo nos falta probar que si dos elementos de $A * B$ conmutan y ninguno está en el conjugado de un factor libre, entonces son potencias de un mismo elemento. Supongamos que esta afirmación es falsa y tomemos u, v tales que v tenga la menor longitud silábica posible de entre todos los elementos para los que existe otro de tal manera que se incumpla la anterior afirmación. Y sea u un elemento de longitud silábica mínima de entre los que incumplen la afirmación anterior para un v de tal longitud. Claramente, $\lambda(v) \leq \lambda(u)$. Sea $u = g_1 \dots g_r$, $v = h_1 \dots h_s$ las formas reducidas de u, v en $A * B$, entonces $r \geq s$. Si h_1, h_s pertenecen al mismo factor libre, entonces $h_1^{-1}vh_1 = h_2 \dots h_{s-1}(h_s h_1)$ tiene menor longitud silábica que v y conmuta con $h_1^{-1}uh_1$; además, ni $h_1^{-1}vh_1$ ni $h_1^{-1}uh_1$ pertenece al conjugado de un factor libre pues ni u ni v pertenecen. Por tanto, $h_1^{-1}vh_1$, $h_1^{-1}uh_1$ han de ser potencias de un mismo elemento w, es decir, $h_1^{-1}vh_1 = w^k$, $h_1^{-1}uh_1 = w^p$, pero entonces $v = (h_1 w h_1^{-1})^k, u =$

$(h_1 w h_1^{-1})^p$ también son potencias de un mismo elemento. Por como habíamos elegido v, u esto no es posible.

Supongamos ahora que h_1, h_s no pertenecen al mismo factor libre. Si además h_1, g_r no están en el mismo factor libre, entonces $uv = g_1 g_2 \dots g_r h_1 h_2 \dots h_s$ es la forma reducida de uv en $A * B$. Por tanto, $\lambda(uv) = r + s$, luego $vu = h_1 h_2 \dots h_s g_1 g_2 \dots g_r$ es la forma reducida de vu en $A * B$. Por unicidad de la forma reducida de $uv = vu$ en $A * B$, debe ocurrir que $r > s$ y $uv^{-1} = g_1 g_2 \dots g_{r-s}$ pues, de lo contrario, $u = v$ lo que no puede ser pues estamos suponiendo que u, v no son potencias de un mismo elemento. Como u conmuta con v, uv^{-1} también conmuta con v. Si uv^{-1} estuviese en el conjugado de un factor libre, también v lo estaría, por la primera parte de la demostración. Luego uv^{-1}, v conmutan y ninguno está en el conjugado de un factor libre, y $\lambda(uv^{-1}) < \lambda(u)$, luego, por como hemos elegido u se sigue que $v = w^k$, $uv^{-1} = w^p$. Pero entonces $u = uv^{-1}v = w^{p+k}$, de donde u, v serían potencias de un mismo elemento, contrariamente a nuestra hipótesis. Luego ha de ocurrir que h_s^{-1}, g_r no estén en el mismo factor libre. Pero en este caso, el razonamiento anterior aplicado a u, v^{-1} en lugar de u, v prueba que u, v^{-1} (y por tanto u, v) son potencias de un mismo elemento. De modo que, en cualquier caso llegamos a contradicción. □

Para estudiar el problema de la conjugación en productos libres se usa la siguiente definición:

Definición 2.1.15 Una secuencia reducida de elementos $g_1, \dots, g_r \in A * B$ se dice cíclicamente reducida si g_1 y g_r pertenecen a factores libres diferentes.

Teorema 2.1.16 Todo elemento $g \in A * B$ es conjugado de un elemento $g_1 \dots g_r$ donde la secuencia $g_1, \dots, g_r$ es cíclicamente reducida. Además, si $g_1, \dots, g_r$ y $h_1, \dots, h_s$ son secuencias cíclicamente reducidas tales que $g_1 \dots g_r$ y $h_1 \dots h_s$ son conjugados en $A * B$ y $r \neq 1$ entonces las secuencias $g_1, \dots, g_r$ y $h_1, \dots, h_s$ son permutaciones cíclicas la una de la otra; si $r = 1$ entonces $s = 1$ y g_1 y h_1 son conjugados en algún factor libre.

2.2. Producto amalgamado de grupos

El grupo $\langle a, b; a^4, b^6 \rangle$ es claramente el producto libre de $\langle a, a^4 \rangle$ y $\langle b, b^6 \rangle$. Pero el grupo

$$\langle a, b; a^4, b^6, a^2 = b^3 \rangle \tag{2.8}$$

no es un producto libre de grupos (no triviales). En efecto, un producto libre de grupos (no triviales) tiene centro trivial, sin embargo el grupo (2.8) no tiene centro trivial pues a^2 está en el centro y no es el elemento neutro. Claramente a^2 está en el centro de (2.8) pues conmuta

con a y también con b pues a^2 es una potencia de b. Para ver que a^2 no es el elemento neutro basta tomar la aplicación de (2.8) en $\langle x; x^{12}\rangle$ dada por $a \to x^3$, $b \to x^2$, que es un homomorfismo. Bajo dicho homomorfismo, a^2 va en x^6, que es distinto del neutro, luego también a^2 es distinto del neutro. Así, (2.8) no es un producto libre; sin embargo, grupos con una presentación como la de (2.8) reciben un nombre especial y serán estudiados en esta sección.

Definición 2.2.1 Si

$$G = \langle a_1, \ldots, a_n, b_1, \ldots, b_m; R(a_\nu), \ldots, S(b_\mu), \ldots, U_1(a_\nu) = V_1(b_\mu), \ldots, U_q(a_\nu) = V_q(b_\mu)\rangle \tag{2.9}$$

y A' es el subgrupo de G generado por $a_1, \ldots, a_n$,
B' es el subgrupo de G generado por $b_1, \ldots, b_m$,
H' es el subgrupo de A' generado por $U_1(a_\nu), \ldots, U_q(a_\nu)$,
K' es el subgrupo de B' generado por $V_1(b_\mu), \ldots, V_q(b_\mu)$,
entonces G se dice producto libre de A' y B' con los subgrupos H' y K' amalgamados bajo la aplicación $U_i(a_\nu) \to V_i(b_\mu)$.

Ejemplo 2.2.2 Consideremos de nuevo el grupo (2.8). Sabemos, a partir de la presentación, que $a^4 = b^6 = 1$. Si además consideramos el homomorfismo de (2.8) en $\langle x; x^{12}\rangle$ dado por $a \to x^3$, $b \to x^2$, entonces podemos concluir que los elementos a, a^2, b, b^2, b^3 son no triviales pues sus imágenes son no triviales, de donde a tiene orden 4 y b orden 6, lo que nos dice que (2.8) es producto libre de $A' = \langle a; a^4\rangle$ y $B' = \langle b; b^6\rangle$ con los subgrupos H' (subgrupo cíclico de A' de orden 2) y K' (subgrupo cíclico de B' de orden 2) amalgamados bajo la aplicación $a^2 \to b^3$.

Ejemplo 2.2.3 Tomemos ahora el grupo $G = \langle c, d; c^8, d^{10}, c^2 = d^5\rangle$. Entonces G es producto libre de C' (subgrupo generado por c) y D' (subgrupo generado por d) con los subgrupos L' y M' generados por c^2 y d^5, respectivamente, amalgamados bajo la aplicación $c^2 \to b^5$.

Sin embargo, C' no tiene la presentación $\langle c; c^8\rangle$ pues de las relaciones se deduce $c^4 = d^{10} = 1$, lo que implica que c tiene orden divisor de 4.

Es más, la aplicación de G en $\langle x; x^{20}\rangle$ dada por $c \to x^5$, $d \to x^2$ es un homomorfismo que nos permite concluir que el orden de c es exactamente 4 y el orden de d es exactamente 10. Luego G es producto libre de un grupo cíclico C' de orden 4 y un grupo cíclico D' de orden 10 con los subgrupos cíclicos L' y M' de orden 2 amalgamados bajo la aplicación $c^2 \to d^5$.

A la vista de los dos ejemplos anteriores se plantea de forma natural una pregunta:
¿Bajo qué condiciones A' y B' tienen las presentaciones naturales $\langle a_1, \ldots, a_n; R(a_\nu), \ldots\rangle$ y

$\langle b_1, \ldots, b_m; S(b_\mu), \ldots \rangle$, *respectivamente?*

A esta pregunta respondemos en el siguiente teorema.

Teorema 2.2.4 Sean

$$A = \langle a_1, \ldots, a_n; R(a_\nu), \ldots \rangle,$$

$$B = \langle b_1, \ldots, b_m; S(b_\mu), \ldots \rangle,$$

$$G = \langle a_1, \ldots, a_n, b_1, \ldots, b_m; R(a_\nu), \ldots, S(b_\mu), \ldots, U_1(a_\nu) = V_1(b_\mu), \ldots, U_q(a_\nu) = V_q(b_\mu) \rangle.$$

Si A' es el subgrupo de G generado por $a_1, \ldots, a_n$ y B' es el subgrupo de G generado por $b_1, \ldots, b_m$, entonces $A \cong A'$ bajo la aplicación $a_\nu \to a_\nu$ y $B \cong B'$ bajo $b_\mu \to b_\mu$ si y sólo si la aplicación $U_i(a_\nu) \to V_i(b_\mu)$ induce un isomorfismo φ entre el subgrupo H de A generado por los $U_i(a_\nu)$ y el subgrupo K de B generado por los $V_i(b_\mu)$.

Demostración: Supongamos primero que $A \cong A'$ bajo la aplicación $a_\nu \to a_\nu$ y $B \cong B'$ bajo $b_\mu \to b_\mu$. Si H' y K' son los subgrupos de G generados por los $U_i(a_\nu)$ y los $V_i(b_\mu)$, respectivamente, entonces $H \cong H'$ bajo $U_i(a_\nu) \to U_i(a_\nu)$ y $K \cong K'$ bajo $V_i(b_\mu) \to V_i(b_\mu)$. Como $U_i(a_\nu) \to V_i(b_\mu)$ es el isomorfismo identidad de H' en K', se sigue que $U_i(a_\nu) \to V_i(b_\mu)$ induce un isomorfismo φ de H en K.

Recíprocamente, supongamos que la aplicación $U_i(a_\nu) \to V_i(b_\mu)$ induce un isomorfismo φ de H en K. Claramente, las aplicaciones $a_\nu \to a_\nu$ y $b_\mu \to b_\mu$ inducen homomorfismos de A en A' y de B en B', respectivamente. Para ver que estos homomorfismos son de hecho isomorfismos necesitaremos resolver el problema de la palabra para G. Por esta razón, pospondremos el final de la demostración hasta que hayamos resuelto el problema de la palabra para G bajo la hipótesis de que $U_i(a_\nu) \to V_i(b_\mu)$ induce un isomorfismo de H en K.

Vamos a considerar ahora un ejemplo orientado a intuir la solución al problema de la palabra para productos amalgamados. Sean

$$G = \langle a, b; a^{12}, b^{15}, a^4 = b^5 \rangle$$

$$A = \langle a; a^{12} \rangle, \ B = \langle b; b^{15} \rangle$$

Entonces H y K son grupos cíclicos de orden 3 y $a^4 \to b^5$ define un isomorfismo entre H y K. Considerando el homomorfismo de G en $\langle x; x^{60} \rangle$ que lleva a en x^5 y b en x^4, es fácil concluir de forma análoga a ocasiones anteriores que $A \cong A'$ y $B \cong B'$.

Para intuir cómo resolver el problema de la palabra para G vamos a reducir una palabra concreta, por ejemplo:

$$a^{15} b^{-21} a^{32} b^{42} a^{-19}. \tag{2.10}$$

Usando las dos primeras relaciones de G podemos reducir los exponentes de a módulo 12 y los exponentes de b módulo 15, de manera que la palabra (2.10) representa el mismo elemento de G que $a^3b^9a^8b^{12}a^5$. Ahora bien, usando la relación $a^4 = b^5$ podemos simplificar aún más:

$$a^3b^9a^8b^{12}a^5 = a^3b^9a^8b^{12}(a^4 \cdot a) = a^3b^9a^8b^{12}(b^5 \cdot a) = a^3b^9a^8 \cdot b^{17} \cdot a =$$

$$= a^3b^9a^8 \cdot (b^{15} \cdot b^2) \cdot a = a^3b^9a^8 \cdot (1 \cdot b^2) \cdot a = a^3b^9 \cdot a^8 \cdot b^2a = a^3b^9 \cdot b^{10} \cdot b^2a =$$

$$= a^3 \cdot b^{21} \cdot a = a^3 \cdot b^6 \cdot a = a^3(b^5 \cdot b)a = a^3(a^4 \cdot b)a = a^7 \cdot ba = (a^4 \cdot a^3)ba = a^4 \cdot a^3ba$$

De manera similar, podemos probar que cualquier palabra $W(a, b)$ se puede reducir a una palabra de la forma

$$a^{4k}a^{\alpha_1}b^{\beta_1} \cdots a^{\alpha_r}b^{\beta_r} \tag{2.11}$$

donde $k = 0, 1, 2$, $\alpha_i = 0, 1, 2, 3$, $\beta_i = 0, 1, 2, 3, 4$, y $\alpha_i \neq 0$ si $i \neq 1$ y $\beta_j \neq 0$ si $j \neq r$.

Para probar que dos palabras distintas de la forma (2.11) no pueden definir el mismo elemento de G, basta usar el homomorfismo de G en $\langle a, b; a^4, b^5\rangle$ dado por $a \to a$, $b \to b$, y el homomorfismo de G en $\langle x; x^{60}\rangle$ dado por $a \to x^5$, $b \to x^4$.

¿Cuál es la generalización adecuada de este ejemplo concreto? El factor a^{4k} que aparece en (2.11) define un elemento genérico de H, a^{α_i} puede ser igual a $1, a, a^2$ ó a^3 según el valor de α_i, es decir, a^{α_i} es uno de los representantes de las clases de A módulo H. Del mismo modo, b^{β_i} puede ser igual a $1, b, b^2, b^3$ ó b^4 según el valor de β_i, es decir, b^{β_i} es uno de los representantes de las clases de B módulo K. Por tanto, todo elemento de G se puede expresar de forma única como un producto de un elemento de H y representantes de las clases de A módulo H y B módulo K alternativamente. Esto sugiere la siguiente generalización:

Teorema 2.2.5 Sean

$$A = \langle a_1, \ldots, a_n; R(a_\nu), \ldots\rangle,$$

$$B = \langle b_1, \ldots, b_m; S(b_\mu), \ldots\rangle,$$

(donde $A \cap B = 1$) y sea

$$G = \langle a_1, \ldots, a_n, b_1, \ldots, b_m; R(a_\nu), \ldots, S(b_\mu), \ldots, U_1(a_\nu) = V_1(b_\mu), \ldots, U_q(a_\nu) = V_q(b_\mu)\rangle.$$

Supongamos que la aplicación $U_i(a_\nu) \to V_i(b_\mu)$ induce un isomorfismo φ entre el subgrupo H de A generado por los $U_i(a_\nu)$ y el subgrupo K de B generado por los $V_i(b_\mu)$ y supongamos seleccionados un transversal a derecha de A módulo H y un transversal a derecha de B módulo K concretos. Entonces a cada elemento $g \in G$ le podemos asociar una única secuencia

$$(h, c_1, c_2, \ldots, c_r) \tag{2.12}$$

tal que

i) h es un elemento de H (puede ser que $h = 1$)

ii) c_i pertenece a uno de los dos tranversales seleccionados

iii) $c_i \neq 1$

iv) c_i y c_{i+1} no están ambos en A ni están ambos en B

v) si h', c_i' son los elementos de G que corresponden a h, c_i bajo los homomorfismos de A en G y de B en G dados por $a_\nu \to a_\nu$ y $b_\mu \to b_\mu$, respectivamente, entonces $g = h'c_1'c_2' \dots c_r'$.

Demostración: Para probar este teorema, introduzcamos un proceso concreto ρ para reducir una palabra en los símbolos a_ν y b_μ a una secuencia de la forma (2.12). Comenzaremos definiendo cómo actúa ρ sobre una secuencia de elementos que pertenecen a A y a B.

$$\rho(\text{secuencia vacía}) = 1, \text{ el elemento neutro de } H$$

$$\rho(g_1) = \begin{cases} g_1 & \text{si } g_1 \in H \\ \varphi^{-1}(g_1) & \text{si } g_1 \in K \\ (h, \overline{g_1}) & \text{donde } h = g_1\overline{g_1}^{-1} \text{ si } g_1 \in A,\ g_1 \notin H \\ (h, \overline{g_1}) & \text{donde } h = \varphi^{-1}(g_1\overline{g_1}^{-1}) \text{ si } g_1 \in B,\ g_1 \notin K \end{cases}$$

donde $\overline{d}$ es el representante de la clase de d en A módulo H o en B módulo K. Si $\rho(g_2, \dots, g_r) = (p, c_2, c_3, \dots, c_s)$, entonces $\rho(g_1, g_2, \dots, g_r) =$

$$= \begin{cases} (g_1 \cdot p, c_2, c_3, \dots, c_s) & \text{si } g_1 \in H \\ (\varphi^{-1}(g_1) \cdot p, c_2, c_3, \dots, c_s) & \text{si } g_1 \in K \\ (h, \overline{g_1p}, c_2, c_3, \dots, c_s) & \text{con } h = (g_1p) \cdot (\overline{g_1p})^{-1} \text{ si } g_1 \in A,\ g_1 \notin H, c_2 \notin A \\ (h, \overline{g_1\varphi(p)}, c_2, c_3, \dots, c_s) & \text{con } h = \varphi^{-1}(g_1\varphi(p) \cdot \overline{g_1\varphi(p)}^{-1}) \text{ si } g_1 \in B,\ g_1 \notin K, c_2 \notin B \\ (g_1pc_2, c_3, \dots, c_s) & \text{si } g_1 \in A,\ g_1 \notin H, c_2 \in A, g_1pc_2 \in H \\ (\varphi^{-1}(g_1\varphi(p)c_2), c_3, \dots, c_s) & \text{si } g_1 \in B,\ g_1 \notin K, c_2 \in B, g_1\varphi(p)c_2 \in K \\ (h, \overline{g_1pc_2}, c_3, \dots, c_s) & \text{con } h = (g_1pc_2) \cdot (\overline{g_1pc_2})^{-1} \\ & \text{si } g_1 \in A,\ g_1 \notin H, c_2 \in A, g_1pc_2 \notin H \\ (h, \overline{g_1\varphi(p)c_2}, c_3, \dots, c_s) & \text{con } h = \varphi^{-1}((g_1\varphi(p)c_2) \cdot (\overline{g_1\varphi(p)c_2})^{-1}) \\ & \text{si } g_1 \in B,\ g_1 \notin K, c_2 \in B, g_1pc_2 \notin K \end{cases}$$

Finalmente, si $W(a_\nu, b_\mu) = W_1 \cdot \dots \cdot W_r$ donde $W_1, \dots, W_r$ son las sílabas de W y g_i es el elemento de A o B definido por W_i, entonces definimos $\rho(W(a_\nu, b_\mu)) = \rho(W_1 \dots W_r) = \rho(g_1, \dots, g_r)$.

Hemos obtenido una expresión complicada para ρ debido, en parte, a que todavía no hemos probado el teorema (2.2.4), de modo que no podemos considerar A y B como subgrupos de G, luego no podemos multiplicar elementos de A y K, o de B y H, sino que debemos usar φ^{-1} y φ.

Usando la definición de ρ podemos probar que $\rho(g_1, g_2, \dots, g_r)$ es una secuencia reducida con las propiedades i) a iv). Además, podemos probar que ρ satisface:

vi) $\rho(1, g_1, \ldots, g_r) = \rho(g_1, g_2, \ldots, g_r)$ y, de forma más general, usando inducción en s:

$$\rho(g_1, g_2, \ldots, g_s, 1, g_{s+1}, \ldots, g_r) = \rho(g_1, g_2, \ldots, g_s, g_{s+1}, \ldots, g_r)$$

vii) si $c_1, \ldots, c_r$ son representantes de clases de A módulo H y de B módulo K alternativamente, $c_i \neq 1$, entonces

$$\rho(c_1, c_2, \ldots, c_r) = (1, c_1, c_2, \ldots, c_r)$$

viii) $\rho(\rho(g_1, g_2, \ldots, g_r)) = \rho(g_1, g_2, \ldots, g_r)$

ix) $\rho(g_1, g_2, \ldots, g_s, g_{s+1}, \ldots, g_r) = \rho(g_1, g_2, \ldots, g_s, \rho(g_{s+1}, \ldots, g_r))$ por inducción en s.

x) si $\rho(g_1, g_2, \ldots, g_r) = (h, c_1, c_2, \ldots, c_s)$, entonces $g_1' g_2' \ldots g_r' = h' c_1' c_2' \ldots c_r'$ en G.

xi) $\rho(g_1, g_2, \ldots, g_s, k, g_{s+1}, \ldots, g_r) = \rho(g_1, g_2, \ldots, g_s, \varphi^{-1}(k), g_{s+1}, \ldots, g_r)$ donde $k \in K$, y $\rho(g_1, g_2, \ldots, g_s, h, g_{s+1}, \ldots, g_r) = \rho(g_1, g_2, \ldots, g_s, \varphi(h), g_{s+1}, \ldots, g_r)$ donde $h \in H$

xii) si g_s y g_{s+1} están ambos en A o están ambos en B, entonces $\rho(g_1, g_2, \ldots, g_s, g_{s+1}, \ldots, g_r)$ $= \rho(g_1, g_2, \ldots, g_s \cdot g_{s+1}, \ldots, g_r)$.

Como en el caso del producto libre, esta última propiedad es la más difícil de probar.

Probaremos ahora que si $W(a_\nu, b_\mu)$ y $T(a_\nu, b_\mu)$ definen el mismo elemento de G, entonces $\rho(W) = \rho(T)$. Como podemos transformar W en T mediante inserción y eliminación de relatores de una sílaba $a_\nu^\epsilon a_\nu^{-\epsilon}$, $b_\mu^\epsilon b_\mu^{-\epsilon}$ ($\epsilon = \pm 1$), $R(a_\nu), \ldots, S(b_\mu), \ldots$, o relatores de dos sílabas $U_i(a_\nu)V_i(b_\mu)^{-1}$, basta considerar el caso en que T se obtiene de W por inserción de uno de estos relatores.

Si $\rho(W) = \rho(g_1, \ldots, g_r)$ y T se obtiene de W por inserción de un relator de una sílaba, la situación es la misma que en el caso del producto libre, es decir, $\rho(T)$ es o bien

$$\rho(g_1, \ldots, g_r) = \rho(W)$$

ó

$$\rho(T) = \rho(g_1, \ldots, g_s, 1, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s, g_{s+1}, \ldots, g_r) = \rho(W)$$

ó

$$\rho(T) = \rho(g_1, \ldots, g_s^*, 1, g_s^{**}, g_{s+1}, \ldots, g_r)$$

donde $g_s = g_s^* \cdot g_s^{**}$ y por tanto en este caso

$$\rho(T) = \rho(g_1, \ldots, g_s^*, g_s^{**}, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s^* \cdot g_s^{**}, g_{s+1}, \ldots, g_r) = \rho(W)$$

Si T se obtiene de W por inserción de un relator de dos sílabas $U_i V_i^{-1}$, sean u y v los elementos de H y K definidos por U_i y V_i, respectivamente. Entonces $\varphi(u) = v$. Además, o bien

$$\rho(T) = \rho(g_1, \ldots, g_s, u, v^{-1}, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s, \varphi(u), v^{-1}, g_{s+1}, \ldots, g_r) =$$

$$= \rho(g_1, \ldots, g_s, \varphi(u)v^{-1}, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s, 1, g_{s+1}, \ldots, g_r) = \rho(W)$$

o bien

$$\rho(T) = \rho(g_1, \ldots, g_s \cdot u, v^{-1}, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s, u, v^{-1}, g_{s+1}, \ldots, g_r) = \rho(W)$$

o bien

$$\rho(T) = \rho(g_1, \ldots, g_s \cdot u, v^{-1} \cdot g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s, u, v^{-1}, g_{s+1}, \ldots, g_r) = \rho(W)$$

o bien

$$\rho(T) = \rho(g_1, \ldots, g_s^* \cdot u, v^{-1}, g_s^{**}, g_{s+1}, \ldots, g_r)$$

donde $g_s = g_s^* \cdot g_s^{**}$ y por tanto,

$$\rho(T) = \rho(g_1, \ldots, g_s^*, u, v^{-1}, g_s^{**}, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s^*, 1, g_s^{**}, g_{s+1}, \ldots, g_r) = \rho(W)$$

o bien, por último

$$\rho(T) = \rho(g_1, \ldots, g_s^*, u, v^{-1} \cdot g_s^{**}, g_{s+1}, \ldots, g_r) = \rho(g_1, \ldots, g_s^*, u, v^{-1}, g_s^{**}, g_{s+1}, \ldots, g_r) = \rho(W)$$

Por tanto, si W y T definen el mismo elemento de G, $\rho(W) = \rho(T)$. En consecuencia, podemos definir $\rho(g)$ para un elemento cualquiera $g \in G$ como ρ de cualquier palabra en a_ν y b_μ que defina g. Probaremos ahora que $\rho(g)$ es una secuencia reducida de la forma (2.12) que satisface v). Sea $W(a_\nu, b_\mu) = W_1 \ldots W_r$ una palabra que define g donde W_i son las sílabas de W. Si g_i es el elemento de A o de B definido por W_i, entonces $g = g_1' g_2' \ldots g_r'$ y

$$\rho(g) = \rho(W) = \rho(g_1, \ldots, g_r) = (h, c_1, c_2, \ldots, c_s)$$

Pero tenemos que $g_1' g_2' \ldots g_r' = h' c_1' \ldots c_s'$, luego $\rho(g)$ satisface las propiedades i) a v). Para probar que ninguna otra secuencia puede satisfacer las propiedades i) a v), supongamos que $(p, d_1, d_2, \ldots, d_t)$ las satisface. Entonces, si P, D_i son las palabras en los símbolos a_ν o b_μ que definen p, d_i en A o B, respectivamente, $Q = PD_1 \ldots D_t$ es una palabra que define g en G. Por tanto, $\rho(g) = \rho(Q) = \rho(PD_1 \ldots D_t)$. Pero las sílabas de Q son o $P, D_1, \ldots, D_t$ o $PD_1, D_2, \ldots, D_t$. Por tanto, $\rho(Q) = \rho(p, d_1, d_2, \ldots, d_t)$ o $\rho(pd_1, d_2, \ldots, d_t) = \rho(p, d_1, d_2, \ldots, d_t)$. Como $(p, d_1, d_2, \ldots, d_t)$ es una secuencia reducida,

$$\rho(g) = \rho(Q) = (p, d_1, d_2, \ldots, d_t)$$

De este modo, $\rho(g)$ es la única secuencia que satisface las propiedades i) a v). □

Estamos ahora en condiciones de completar la demostración del teorema 2.2.4. Tenemos que probar que los homomorfismos de A y B en G dados por $a_\nu \to a_\nu$ y $b_\mu \to b_\mu$ son inyectivos.

Si g_1 es un elemento de $A \cup B$, entonces g_1' es su imagen en G. Además, si W es una palabra en los símbolos a_ν ó b_μ que defina g_1', entonces $\rho(g_1') = \rho(W) = \rho(g_1)$. Por tanto, si g_1 y g_2 son elementos ambos en A o ambos en B y $g_1' = g_2'$, entonces $\rho(g_1) = \rho(g_1') = \rho(g_2') = \rho(g_2)$. Probaremos que g_1 ha de ser g_2.

Supongamos que $g_1 \in A$, entonces

$$\rho(g_1) = \begin{cases} g_1 & \text{si } g_1 \in H \\ (h, \overline{g_1}) & \text{donde } h = g_1\overline{g_1}^{-1} \text{ si } g_1 \in A,\ g_1 \notin H \end{cases}$$

En cualquiera de los dos casos, el producto de los términos de $\rho(g_1)$ es g_1. Por tanto, si $\rho(g_1) = \rho(g_2)$, tenemos que $g_1 = g_2$. Por otra parte, si $g_1 \in B$, entonces

$$\rho(g_1) = \begin{cases} \varphi^{-1}(g_1) & \text{si } g_1 \in K \\ (h, \overline{g_1}) & \text{donde } h = \varphi^{-1}(g_1\overline{g_1}^{-1}) \text{ si } g_1 \in B,\ g_1 \notin K \end{cases}$$

En cualquiera de los dos casos, el producto de los términos de $\rho(g_1)$ es g_1 si el término de H es reemplazado por su imagen bajo φ. Por tanto, si $\rho(g_1) = \rho(g_2)$, tenemos que $g_1 = g_2$. □

Corolario 2.2.6 Sea G como en el teorema 2.2.5. Si seleccionamos un transversal a derecha para A' módulo H' y un transversal a derecha para B' módulo K', entonces todo elemento g de G se puede expresar de forma única como un producto $h'c_1'c_2'\ldots c_q'$ donde $h' \in H'$, $c_i' \neq 1$, los c_i' pertenecen al transversal de A' módulo H' o al transversal de B' módulo K', y c_i', c_{i+1}' no están ambos en A' ni ambos en B'.

Demostración: Si h, c_i son los elementos de H, A ó B que se corresponden con h', c_i', entonces $\rho(h'c_1'c_2'\ldots c_q') = (h, c_1, c_2, \ldots, c_q)$ y basta aplicar el teorema 2.2.5 para concluir. □

Corolario 2.2.7 Sea G como en el teorema 2.2.5. Si un elemento $g \in G$ es un producto $g = g_1'g_2'\ldots g_r'$ donde $g_i' \notin H'$, $g_i' \in A'$ ó B' y g_i', g_{i+1}' no están ambos en A' ni ambos en B', y si $\rho(g) = (h, c_1, c_2, \ldots, c_q)$, entonces $q = r$ y g_i' y c_i' están ambos en A' o en B'. Además, si $g_k', g_{k+1}', \ldots, g_r'$ pertenecen a los transversales fijados, entonces $c_k' = g_k', c_{k+1}' = g_{k+1}', \ldots, c_r' = g_r'$.

Demostración: Probaremos el resultado por inducción en r. Si $r = 1$ y $g_1' \in A'$ entonces $\rho(g_1') = \rho(g_1) = (h, \overline{g_1})$ donde $h = g_1\overline{g_1}^{-1}$; análogamente, si $g_1' \in B'$ entonces $\rho(g_1') = \rho(g_1) = (h, \overline{g_1})$ donde $h = \varphi^{-1}(g_1\overline{g_1}^{-1})$. Por tanto, si g_1' es un representante, $c_1' = g_1'$ y tenemos el resultado en cualquiera de los dos casos. Supongamos el resultado cierto para r y consideremos $\rho(g_1'g_2'\ldots g_r'g_{r+1}') = \rho(g_1, g_2, \ldots, g_r, g_{r+1})$. Para calcular esto primero debemos calcular $\rho(g_2, \ldots, g_{r+1})$ que, por hipótesis de inducción, es igual a $(h, c_2, \ldots, c_{r+1})$, donde c_i y g_i están ambos en A o ambos en B. Por tanto, g_1 y c_2 no están ambos en A ni ambos en B. Si $g_1 \in A$, entonces $\rho(g_1, g_2, \ldots, g_r, g_{r+1}) = (p, c_1, c_2, \ldots, c_{r+1})$ con $c_1 = \overline{g_1h}$ y $p =$

$g_1 h \cdot \overline{g_1 h}^{-1}$; si $g_1 \in B$ entonces $\rho(g_1, g_2, \ldots, g_r, g_{r+1}) = (p, c_1, c_2, \ldots, c_{r+1})$ con $c_1 = \overline{g_1 \varphi(h)}$ y $p = \varphi^{-1}(g_1 \varphi(h) \cdot \overline{g_1 \varphi(h)}^{-1})$.

Si además $g'_k, \ldots, g'_{r+1}$ son representantes y $k \geq 2$, tenemos el resultado por hipótesis de inducción. Si $g'_1, \ldots, g'_{r+1}$ son todos representantes, por hipótesis de inducción se tiene que $g'_2 = c'_2, \ldots, g'_{r+1} = c'_{r+1}$. Como $\rho(g'_2 \ldots g'_{r+1}) = (h, c_2, \ldots, c_{r+1})$, $c'_2 \ldots c'_{r+1} = g'_2 \ldots g'_{r+1} = h' c'_2 \ldots c'_{r+1}$ y $h' = 1$. Por tanto, $c_1 = \overline{g_1 h} = \overline{g_1} = g_1$, luego $c'_1 = g'_1$, y tenemos el resultado. □

Gracias al corolario anterior podemos definir la longitud en los representantes de un elemento $g \in G$:

Definición 2.2.8 Si $g = h' c'_1 \ldots c'_q$ como en los corolarios anteriores, entonces $h' c'_1 \ldots c'_q$ se denomina forma reducida de g en G, y q se dice longitud de g en los representantes. Por el corolario anterior, q es independiente de los sistemas de representantes elegidos para A' mod H' y B' mod K'.

Corolario 2.2.9 Si G es como en el teorema 2.2.5, entonces $A' \cap B' = H'$.

Demostración: Supongamos que $g \in A' \cap B'$, entonces hay una palabra $W(a_\nu)$ y otra palabra $T(b_\mu)$ que definen g, luego $\rho(g) = \rho(W(a_\nu)) = \rho(T(b_\mu))$. Pero si $W(a_\nu) \notin H$, entonces ocurriría que $\rho(W(a_\nu)) = (h, c)$ con c el representante de $W(a_\nu)$ en A mod H. Del mismo modo, si $T(b_\mu) \notin K$, entonces ocurriría que $\rho(T(b_\mu)) = (h_1, c_1)$ con c_1 el representante de $T(b_\mu)$ en B mod K. Como $\rho(W(a_\nu)) = \rho(T(b_\mu))$, se tendría que $c = c_1$, lo que es imposible pues $A \cap B = 1$. Así, $W(a_\nu) \in H$ o $T(b_\mu) \in K$. En cualquier caso, $g \in H' = K'$, luego $A' \cap B' \subseteq H'$. Como $H' = K'$, se tiene el otro contenido y por tanto la igualdad. □

Es interesante remarcar que, aunque $A \cap B = 1$, acabamos de probar que $A' \cap B' = H'$, por lo que debemos ser cuidadosos a la hora de identificar los grupos isomorfos A, A' y B, B'. Sin embargo, seguiremos identificándolos cuando no cause confusión. Así la definición 2.2.1 se puede reformular:

Definición 2.2.10 Si A, B, H, K, φ y G son como en el teorema 2.2.5, diremos que G es el producto libre de A y B con los subgrupos H y K amalgamados bajo φ, y lo denotaremos $G = *(A, B, H, K, \varphi)$. Abreviadamente, también lo llamaremos producto libre de A y B con subgrupo amalgamado H, y diremos que A y B son los factores de la amalgama.

Notemos que esta definición de $G = *(A, B, H, K, \varphi)$ involucra presentaciones concretas de A y B y generadores concretos de H (los generadores de K están determinados por los de H y por φ), sin embargo el grupo G depende sólo de los grupos A, B, H y de la aplicación φ, lo que se puede establecer de manera formal en la siguiente proposición.

Proposición 2.2.11 Supongamos que A tiene las presentaciones $\mathcal{P}_1$ y $\mathcal{P}_1'$ siguientes:

$$\langle a_1, \dots, a_n; R(a_\nu), \dots \rangle \tag{2.13}$$

y

$$\langle c_1, \dots, c_k; P(c_\kappa), \dots \rangle \tag{2.14}$$

y que B tiene las presentaciones $\mathcal{P}_2$ y $\mathcal{P}_2'$ siguientes:

$$\langle b_1, \dots, b_m; S(b_\mu), \dots \rangle \tag{2.15}$$

y

$$\langle d_1, \dots, d_l; Q(d_\lambda), \dots \rangle \tag{2.16}$$

Y supongamos que el subgrupo H de A está generado por $U_1(a_\nu), \dots$ y también por $T_1(c_\kappa), \dots,$ y que el subgrupo K de B está generado por $\varphi(U_1(a_\nu)) = V_1(b_\mu), \dots$ y también por $\varphi(T_1(c_\kappa)) = W_1(d_\lambda), \dots,$ donde φ es un isomorfismo entre H y K.

Entonces los isomorfismos $\varphi_{\mathcal{P}_1,\mathcal{P}_1'}$ y $\varphi_{\mathcal{P}_2,\mathcal{P}_2'}$ (ver 1.1.4) se pueden extender a un isomorfismo entre

$$\langle a_1, \dots, a_n, b_1, \dots, b_m; R(a_\nu), \dots, S(b_\mu), \dots, U_1(a_\nu) = V_1(b_\mu), \dots \rangle \tag{2.17}$$

y

$$\langle c_1, \dots, c_k, d_1, \dots, d_l; P(c_\kappa), \dots, Q(d_\lambda), \dots, T_1(c_\kappa) = W_1(d_\lambda), \dots \rangle \tag{2.18}$$

Proposición 2.2.12 Sea $G = *(A, B, H, K, \varphi)$, entonces cualquier elemento de G de orden finito está en un conjugado de A ó de B.

Demostración: Sea g un elemento de orden finito que no está en un conjugado de A ó de B. Sea entonces $g = hc_1 \dots c_r$, $r \geq 2$ la forma reducida de g.

Caso 1: Si c_1 y c_r pertenecen a distintos factores de la amalgama, entonces

$$g^k = hc_1 \dots c_r \cdot hc_1 \dots c_r \cdot \dots \cdot hc_1 \dots c_r = (hc_1) \cdot c_2 \cdot \dots \cdot c_r \cdot (hc_1) \cdot c_2 \cdot \dots \cdot c_r \cdot \dots \cdot (hc_1) \cdot c_2 \cdot \dots \cdot c_r$$

tiene longitud kr en los representantes, luego no puede ser 1, lo que contradice que g tenga orden finito pues el razonamiento anterior es válido para todo entero positivo k.

Caso 2: Si c_1 y c_r pertenecen al mismo factor de la amalgama, tomemos g_1 el conjugado de g con menor longitud en los representantes. Como hemos supuesto que g tenía orden finito, g_1 también tiene orden finito. Además, g_1 ha de tener la forma reducida $pd_1 \dots d_q$ con $q \geq 2$, $p \in H$ y con d_1, d_q pertenecientes a distintos factores de la amalgama. El hecho de que $q \geq 2$ se debe a que g (y por tanto g_1) no pertenece a un conjugado de A o B. Y el hecho de que d_1, d_q pertenezcan a distintos factores de la amalgama, se debe que en caso contrario tendríamos que $d_q g_1 d_q^{-1} = (d_q p d_1) \cdot d_2 \cdot \dots \cdot d_{q-1}$ sería un conjugado de g con menor longitud en los representantes que g_1. Por el caso 1, g_1 no puede tener orden finito, luego tampoco g. □

El producto libre es una extensión del concepto de grupo libre, pues un grupo libre de rango n es un producto libre de n grupos cíclicos infinitos. A su vez, el producto amalgamado es una extensión del producto libre, ya que si el subgrupo amalgamado es el trivial se obtiene un producto libre. En este proceso, los resultados que se obtienen se vuelven cada vez más complejos. Como muestra de ello, veremos qué podemos decir de dos elementos que conmutan en un producto amalgamado. En un grupo libre ambos elementos deberán ser potencias de un mismo elemento, mientras que en un producto libre de grupos ambos estarán en el mismo conjugado en un factor libre o bien serán potencia de un mismo elemento. En el caso de productos amalgamados, las posibles situaciones que se pueden presentar son las siguientes:

Teorema 2.2.13 Sea $G = *(A, B, H, K, \varphi)$ y sean $x, y \in G$ tales que $xy = yx$. Entonces se cumple exactamente una de las siguientes alternativas:

- Alguno de los dos elementos pertenece a un conjugado de H
- Si x e y no están en ningún conjugado de H, pero x pertenece a un conjugado de un factor de la amalgama, entonces y está también en dicho conjugado
- Si x e y no están en ningún conjugado de un factor, entonces $x = ghg^{-1} \cdot \omega^j$, $y = gh'g^{-1} \cdot \omega^k$, donde $g, \omega \in G$, $h, h' \in H$, $ghg^{-1}, gh'g^{-1}, \omega$ conmutan dos a dos.

Corolario 2.2.14 El centro de $G = *(A, B, H, K, \varphi)$, si $A \neq H$ y$B \neq K$, es $H \cap Z(A) \cap Z(B)$.

Demostración: Como A y B generan G, $H \cap Z(A) \cap Z(B) \subseteq Z(G)$. Si $x \in Z(G)$ entonces $x \in H$ ya que si $x = hc_1 \dots c_r$ es la forma reducida de x y $r \geq 1$, entonces eligiendo un representante $c \neq 1$ perteneciente al factor A o B que no contiene a c_r, se tiene que $xc = hc_1 \dots c_r \cdot c$ es una forma reducida. Luego $cx = chc_1 \dots c_r$ debe tener longitud $r + 1$ en los representantes, de donde c y c_1 pertenecen a factores diferentes, luego por el corolario 2.2.7, cx termina en c_r. Esto contradice que $xc = cx$. Por tanto, $x \in H$. Y también se cumple $x \in Z(A)$ y $x \in Z(B)$ pues $x \in Z(G)$.

Notar que aquí se está identificando A' con A y B' con B y, por tanto, se consideran A y B como subgrupos de G. □

La creciente dificultad de algunos problemas cuando se plantean para grupos libres, productos libres y productos amalgamados puede observarse también en los problemas de la palabra y la conjugación.

El problema de la palabra para grupos libres tiene una solución extremadamente sencilla, mientras que para un producto libre $A * B$ requiere saber resolver el problema de la palabra para A y para B. En un producto amalgamado $G = *(A, B, H, K, \varphi)$, para resolver el problema de la palabra, debemos ser capaces de resolver el problema de la palabra generalizado

para A módulo H y para B módulo K, y debemos tener un método para calcular $\varphi(h)$ y $\varphi^{-1}(k)$ para $h \in H, k \in K$ (por ejemplo, un método para escribir h y k como palabras en $U_i(a_\nu)$ y $V_i(b_\mu)$, respectivamente, si φ viene dado por $U_i(a_\nu) \to V_i(b_\mu)$).

El problema de la conjugación para grupos libres se resuelve de forma sencilla sabiendo que dos elementos son conjugados si y sólo si, al reducirlos cíclicamente, uno es una permutación cíclica del otro. Para resolver el problema de la conjugación en un producto libre $A * B$ debemos ser capaces de resolverlo para A y para B (ver teorema 2.1.16). En cambio, para $G = *(A, B, H, K, \varphi)$, incluso si sabemos resolver el problema de la conjugación para A y B y sabemos resolver el problema de la palabra para G, la solución del problema de la conjugación para G es en general desconocida. Sin embargo, en algunos casos, el problema de la conjugación se puede resolver.

Diremos que un elemento $g \in G = *(A, B, H, K, \varphi)$, con forma reducida $g = hg_1 \dots g_r$, es cíclicamente reducido si g_1, g_r no pertenecen al mismo factor de la amalgama salvo en el caso $r = 1$. Si $g = p_1 \dots p_r$ con $r \geq 2$ y p_i, p_{i+1} pertenecen a factores distintos, entonces g es cíclicamente reducido si y sólo si p_1, p_r pertenecen a factores diferentes. Esto se debe a que si la forma reducida de g es $hg_1 \dots g_r$ entonces g_i está en el mismo factor que p_i por el corolario 2.2.7.

Teorema 2.2.15 Sea $G = *(A, B, H, K, \varphi)$. Entonces todo elemento de G es conjugado de un elemento de G cíclicamente reducido. Además, si $g \in G$ es un elemento cíclicamente reducido, entonces:

1. Si g es conjugado de un elemento $h \in H$ entonces g pertenece a algún factor y hay una secuencia de elementos $h, h_1, h_2, \dots, h_t, g$ tales que $h_i \in H$ y elementos consecutivos de la secuencia son conjugados en un factor.

2. Si g es conjugado de un elemento g' en un factor pero no en un conjugado de H, entonces g, g' pertenecen al mismo factor y son conjugados en ese factor.

3. Si g es conjugado de un elemento $p_1 \dots p_r$ con $r \geq 2$ y p_i, p_{i+1}, así como p_1, p_r pertenecen a factores distintos, entonces g se puede obtener permutando cíclicamente $p_1 \dots p_r$ y conjugando el resultado por un elemento de H.

Como aplicación del teorema anterior a una situación particular, obtenemos:

Corolario 2.2.16 Sea $G = *(A, B, H, K, \varphi)$ con H, K contenidos en $Z(A), Z(B)$, respectivamente. Entonces dos elementos de G son conjugados si y sólo si o bien al reducirlos cíclicamente pertenecen ambos al mismo factor y son conjugados en ese factor, o bien uno de

los elementos al reducirlo cíclicamente tiene la forma reducida $hg_1 \dots g_r$ y el otro elemento al reducirlo cíclicamente tiene la forma reducida $hg_s \dots g_r g_1 \dots g_{s-1}$.

Demostración: Como $H \subseteq Z(A)$ y $K \subseteq Z(B)$, entonces $H \subseteq Z(G)$. Por tanto, el único conjugado de un elemento $h \in H$ es el propio h. Sean $g, g' \in G$ cíclicamente reducidos y conjugados uno de otro en G. Si g' pertenece a un conjugado de H (es decir, a H), $g = g'$, luego g, g' están en el mismo factor y son conjugados en dicho factor. Si g' está en un factor pero no en un conjugado de H, entonces obtenemos el resultado por el caso 2 del teorema anterior. Por último, si g' tiene la forma reducida $hg_1 \dots g_r$ con $r \geq 2$. Entonces por el caso 3 del teorema anterior tomando $p_1 = hg_1$, $p_2 = g_2, \dots, p_r = g_r$ se tiene $g = k(g_s \dots g_r \cdot hg_1 \dots g_{s-1})k^{-1}$ donde $k \in H$. Como $H \subseteq Z(G)$, obtenemos $g = hg_s \dots g_r g_1 \dots g_{s-1}$. □

Capítulo 3

Grupos presentados con una única relación.

En este capítulo, aplicaremos la teoría de productos libres y amalgamados al estudio de grupos presentados con una única relación. En particular, en la segunda sección, resolveremos el problema de la palabra para tales grupos.

3.1. El teorema de la independencia. Consecuencias.

Comenzaremos con un importante teorema en el estudio de grupos presentados con una única relación, el teorema de la independencia.

Teorema 3.1.1 Sea $R(a_1, \ldots, a_n)$ una palabra cíclicamente reducida en $a_1, \ldots, a_n$ que involucra el símbolo a_n. Entonces el subgrupo de

$$G = \langle a_1, \ldots, a_n; R(a_1, \ldots, a_n) \rangle$$

generado por $a_1, \ldots, a_{n-1}$ está generado libremente por estos símbolos; en otras palabras, todo relator no trivial de G debe involucrar el símbolo a_n.

Demostración: Usaremos inducción en la longitud del relator R. Claramente, si la longitud de R es 1 o R involucra solo el símbolo a_n, entonces G es el producto libre del grupo libre en $a_1, \ldots, a_{n-1}$ y el grupo cíclico generado por a_n, luego se cumple el teorema.

Supongamos que el teorema se cumple para todos los grupos presentados con un único relator de longitud menor que r y supongamos que $R(a_1, \ldots, a_n)$ tiene longitud r.

Podemos suponer que R involucra al menos otro generador además de a_n, por ejemplo, a_1. Vamos primero a renombrar los generadores de tal manera que no necesitemos los subíndices, pues más adelante necesitaremos introducir subíndices con un significado diferente. En adelante, representaremos a_n por t, y $a_1, a_2, \ldots$ por $b, c, \ldots$.

Por supuesto, R no tiene que involucrar necesariamente todos los generadores de G. Los generadores de G que no aparecen en R generan libremente un subgrupo libre K de G, y se tiene que G es el producto libre de K y el grupo cuyos generadores son los de G que aparecen en R con el relator R como conjunto completo de relatores. Por tanto, para probar que los generadores de G distintos de t generan libremente un grupo libre, basta probar que los generadores de G distintos de t que aparecen en R generan libremente un grupo libre. En consecuencia, podemos suponer que todos los generadores de G aparecen en R. Denotaremos $\sigma_x(R)$ la suma de los exponentes en un simbolo x en la palabra R. Se dirá que $\sigma_x(R)$ es la suma de exponentes de R en x. Se nos presentan dos casos:

CASO 1: G tiene sólo dos generadores b y t. Hay dos posibilidades:

i) $\sigma_t(R) \neq 0$.

ii) $\sigma_t(R) = 0$.

CASO 2: G tiene al menos tres generadores b, c, t y se da una de las siguientes situaciones:

i) la suma de exponentes de R en algún generador distinto de t es 0.

ii) la suma de exponentes de R para cualquier generador distinto de t es no nula.

Para reflejar las técnicas que se utilizan en la demostración, desarrollaremos, por ejemplo, el caso 1.

CASO 1 i): En este caso, si b tuviese orden finito, existiría $k > 0$ tal que b^k pertenecería al subgrupo normal de F generado por R, con F el grupo libre generado por b, t, es decir,

$$b^k = \prod_i S_i R^{\epsilon_i} S_i^{-1}$$

Pero entonces

$$k = \sigma_b(b^k) = \sum_i \sigma_b(R^{\epsilon_i}) = \left(\sum_i \epsilon_i\right) \sigma_b(R)$$

$$0 = \sigma_t(b^k) = \sum_i \sigma_t(R^{\epsilon_i}) = \left(\sum_i \epsilon_i\right) \sigma_t(R)$$

Como $\sigma_t(R) \neq 0$, deducimos $\sum_i \epsilon_i = 0$, luego $k = 0$, de donde b tiene orden infinito en $\langle b, t; R(b,t)\rangle$ y genera libremente un grupo libre.

CASO 1 ii): En este caso, vamos a examinar el comportamiento de b en un subgrupo de $G = \langle b, t; R(b,t)\rangle$, en concreto, el subgrupo normal N de G generado por b. Vamos a obtener una presentación para N. Como representantes de Schreier de G módulo N elegimos $\{t^k / k \in \mathbb{Z}\}$. Una palabra $W(b,t)$ define un elemento de N si y solo si $\sigma_t(W) = 0$. En particular, $R(b,t)$ define una palabra de N. El representante $\overline{W}$ de una palabra W es t^k donde $k = \sigma_t(W)$. N está generado por los elementos b_k definidos de la siguiente manera:

$$b_k = t^k b t^{-k} = t^k \cdot b \cdot \overline{t^k b}^{-1}$$

Para cada palabra W que define un elemento de N, obtenemos una expresión $\tau(W)$ en términos de los b_k de la siguiente forma: cada símbolo b^ϵ ($\epsilon = \pm 1$) de W lo reemplazamos por b_s^ϵ donde s es la suma de los exponentes de los t-símbolos que aparecen antes del b^ϵ considerado. Por ejemplo,

$$\tau(t^{-1}btb^2tb^{-3}t^{-1}) = b_{-1}b_0^2b_1^{-3}$$

Si $R(b,t)$ es cíclicamente reducida como palabra en b, t, entonces $\tau(R)$ es una palabra cíclicamente reducida en los b_k.

Como t aparece en R pero no es reemplazado por ningún símbolo b_k al reescribir R como $\tau(R)$, la longitud de $\tau(R)$ como palabra en los símbolos b_k es menor que la longitud de R como palabra en b, t. Por tanto, podemos aplicar la hipótesis de inducción a $\tau(R)$ o cualquier palabra de su longitud. Sea

$$\tau(R) = P(\dots, b_k, \dots)$$

Entonces N está generado por los b_k y tiene como conjunto completo de relatores los siguientes:

$$P_m = \tau(t^m R t^{-m}) = P(\dots, b_{k+m}, \dots)$$

Por lo tanto,

$$N = \langle \dots, b_{-1}, b_0, b_1, \dots; \dots, P_{-1}, P_0, P_1, \dots \rangle \tag{3.1}$$

Para hacer más comprensible la demostración de que b_0 tiene orden infinito en N, ilustraremos primero la situación con un ejemplo concreto. Sea

$$G = \langle b, t; t^{-1}btb^2tb^{-3}t^{-1} \rangle$$

Entonces $\tau(R) = b_{-1}b_0^2b_1^{-3}$ y

$$N = \langle \dots, b_{-2}, b_{-1}, b_0, b_1, b_2, \dots; \dots, b_{-2}b_{-1}^2b_0^{-3}, b_{-1}b_0^2b_1^{-3}, b_0b_1^2b_2^{-3}, \dots \rangle$$

Ahora los grupos

$$N_m = \langle b_{-1+m}, b_m, b_{1+m}; b_{-1+m}b_m^2b_{1+m}^{-3} \rangle$$

pueden usarse para construir N de manera sencilla.

Como el relator en N_m tiene longitud menor que el relator en G, podemos aplicar la hipótesis de inducción a N_m, de modo que cualesquiera dos b-generadores de N_m generan libremente un grupo libre. Por tanto

$$N_{0,1} = \langle b_{-1}, b_0, b_1, b_2; b_{-1}b_0^2b_1^{-3}, b_0b_1^2b_2^{-3} \rangle$$

es el producto libre de N_0 y N_1 con el subgrupo libre de cada uno libremente generado por b_0, b_1 amalgamado bajo la aplicación identidad. Como $N_0 \subseteq N_{0,1}$, se sigue que b_{-1}, b_0 generan

libremente un grupo libre en $N_{0,1}$ y por tanto

$$N_{-1,1} = \langle b_{-2}, b_{-1}, b_0, b_1, b_2; b_{-2}b_{-1}^2 b_0^{-3}, b_{-1}b_0^2 b_1^{-3}, b_0 b_1^2 b_2^{-3} \rangle$$

es el producto libre de N_{-1} y $N_{0,1}$ con el subgrupo libre de cada uno libremente generado por b_{-1}, b_0 amalgamado bajo la aplicación identidad. Similarmente, como $N_1 \subseteq N_{0,1} \subseteq N_{-1,1}$, b_1, b_2 generan libremente un subgrupo libre de $N_{-1,1}$, y por tanto,

$$N_{-1,2} = \langle b_{-2}, b_{-1}, b_0, b_1, b_2, b_3; b_{-2}b_{-1}^2 b_0^{-3}, b_{-1}b_0^2 b_1^{-3}, b_0 b_1^2 b_2^{-3}, b_1 b_2^2 b_3^{-3} \rangle$$

es el producto libre de $N_{-1,1}$ y N_2 con el subgrupo libre de cada uno libremente generado por b_1, b_2 amalgamado bajo la aplicación identidad. Continuando de esta forma, obtenemos una cadena de grupos

$$N_0 \subseteq N_{0,1} \subseteq N_{-1,1} \subseteq N_{-1,2} \subseteq N_{-2,2} \subseteq \cdots \subseteq N_{-i+1,i} \subseteq N_{-i,i} \subseteq N_{-i,i+1} \subseteq \ldots$$

donde $N_{-i,i}$ es el producto libre de N_{-i} y $N_{-i+1,i}$ con un subgrupo libre amalgamado y $N_{-i,i+1}$ es el producto libre de $N_{-i,i}$ y N_{i+1} con un subgrupo libre amalgamado. Por el lema 1.1.7, N es la unión de esta cadena de grupos. Por tanto, $N_0 \subset N$ y como b_0 genera un grupo libre en N_0, b_0 genera un grupo libre en N. Como b_0 define el elemento b en $N \subseteq G$, se sigue que b genera un grupo libre en G.

Una vez visto este ejemplo concreto, volvamos ahora a la situación general en que N tiene la presentación (3.1). Como $\tau(R) = P(\ldots, b_k, \ldots)$ y t aparece en R pero tiene suma de exponentes 0 y R es cíclicamente reducida, P debe involucrar al menos dos b-símbolos distintos b_k y b_q $(k \neq q)$, puesto que si en R apareciera solamente una potencia de b entonces $R = t^\alpha b^\beta t^\gamma$ con α o γ no nulos y $\alpha + \gamma = 0$, lo que contradice el hecho de que R es cíclicamente reducida. Por tanto, al menos dos potencias de b aparecen en R separadas por una potencia de t, es decir, R contiene una subpalabra de la forma $b^\alpha t^\beta b^\gamma$ con $\alpha, \beta, \gamma \neq 0$. Si denotamos por k a la suma de exponentes de R en los símbolos t que preceden a b^α, entonces esta subpalabra es reemplazada por $b_k^\alpha b_{k+\beta}^\gamma$. Como $\tau(R) = P$ es cíclicamente reducida y $k + \beta \neq k$, tomando $q = k + \beta$, tenemos que b_k y b_q aparecen ambos en P.

Sea ahora μ el mínimo subíndice de b que aparece en P y sea M el máximo subíndice de b que aparece en P, entonces $\mu < M$ por lo anterior.

Para cada entero i definamos:

$$N_i = \langle b_{\mu+i}, b_{\mu+i+1}, \ldots, b_{M+i}; P_i \rangle \tag{3.2}$$

Como en el ejemplo, construimos ahora $N_{0,1}, N_{-1,1}, \ldots$:

$$N_{0,1} = \langle b_\mu, b_{\mu+1}, \ldots, b_M, b_{M+1}; P_0, P_1 \rangle$$

es el producto libre de N_0 y N_1, con el subgrupo libre en cada uno libremente generado por $b_{\mu+1}, \ldots, b_M$ amalgamado bajo la aplicación identidad. De forma similar, como $N_0 \subseteq N_{0,1}$ y $b_\mu, \ldots, b_{M-1}$ generan libremente un grupo libre en N_0,

$$N_{-1,1} = \langle b_{\mu-1}, b_\mu, b_{\mu+1}, \ldots, b_M, b_{M+1}; P_{-1}, P_0, P_1 \rangle$$

es el producto libre de N_{-1} y $N_{0,1}$ con el subgrupo libre en cada uno libremente generado por $b_\mu, \ldots, b_{M-1}$ amalgamado bajo la aplicación identidad. Continuando de esta manera, construimos una cadena de grupos

$$N_0 \subseteq N_{0,1} \subseteq N_{-1,1} \subseteq N_{-1,2} \subseteq \cdots \subseteq N_{-i+1,i} \subseteq N_{-i,i} \subseteq N_{-i,i+1} \subseteq \ldots \tag{3.3}$$

donde $N_{-i,i}$ es el producto libre de N_{-i} y $N_{-i+1,i}$ con un subgrupo libre amalgamado y $N_{-i,i+1}$ es el producto libre de $N_{-i,i}$ y N_{i+1} con un subgrupo libre amalgamado. Como antes, por el lema 1.1.7, N es la unión de esta cadena de grupos. Como cada N_i en (3.2) es un subgrupo de algún grupo en (3.3), cada N_i es un subgrupo de N. Como $\mu < M$, cualquier generador de N_i genera un grupo libre. Pero b_0 está en algún N_i y por tanto genera un grupo libre en N, luego b genera un grupo libre en G. □

El resultado anterior es cierto incluso si G tiene una cantidad infinita de generadores. En tal caso, R sólo puede involucrar un número finito de generadores de G.

Corolario 3.1.2 Todo grupo finitamente presentado con una única relación es un subgrupo de algún grupo presentado con dos generadores y una única relación.

Demostración: Supongamos que $H = \langle b_0, b_1, \ldots, b_n; P(\ldots, b_k, \ldots) \rangle$, donde P es cíclicamente reducida.

Si P involucra a todos los generadores de H, tomemos dos símbolos b, t y definamos $R(b,t) = P(\ldots, t^k b t^{-k}, \ldots)$, es decir, cada símbolo b_k lo sustituimos por $t^k b t^{-k}$. Entonces, como en el caso 1 ii) de la demostración del teorema anterior, el subgrupo normal N de $G = \langle b, t; R(b,t) \rangle$ generado por b tiene la presentación 3.1 y contiene a los N_i dados por 3.2 como subgrupos. En particular, cuando $i = 0$, $N_0 = H$. Luego H es un subgrupo de G.

Si P no involucra a todos los generadores de H, podemos usar transformaciones de Tietze y reemplazar uno de los generadores que aparecen en P por el producto de un nuevo generador y todos los generadores no involucrados en P. De esta manera, tendremos H dado por una presentación con una sola relación que involucra todos los generadores y podemos aplicar el caso anterior. □

Corolario 3.1.3 Si $E = \langle x, c, \ldots, t; R(x^\gamma, c, \ldots, t) \rangle$ con $\gamma \neq 0$, entonces el subgrupo G de E generado por $x^\gamma, c, \ldots, t$ tiene la presentación $G = \langle b, c, \ldots, t; R(b, c, \ldots, t) \rangle$ donde b corresponde a x^γ, c a c, $\ldots$, t a t.

Demostración: Si $R(b, c, \ldots, t)$ involucra sólo a b, entonces $R(x^\gamma, c, \ldots, t)$ involucraba sólo a x^γ, luego E es el producto libre del grupo cíclico generado por x y el grupo libre en los generadores $c, \ldots, t$, de donde se sigue (a partir de la teoría de productos libres) que G tiene la presentación del enunciado.

Si $R(b, c, \ldots, t)$ involucra a algún otro generador distinto de b, entonces b tiene orden infinito en $\langle b, c, \ldots, t; R(b, c, \ldots, t)\rangle$ por el teorema de la independencia. Por tanto,

$$\langle x, b, c, \ldots, t; bx^{-\gamma}, R(b, c, \ldots, t)\rangle \tag{3.4}$$

es el producto libre del grupo cíclico infinito en x y el grupo $\langle b, c, \ldots, t; R(b, c, \ldots, t)\rangle$ con los subgrupos cíclicos infinitos generados por x^γ y b, respectivamente, amalgamados bajo $x^\gamma \to b$. Mediante transformaciones de Tietze, podemos eliminar b de la presentación 3.4 y obtener $\langle x, c, \ldots, t; R(x^\gamma, c, \ldots, t)\rangle$ que es precisamente E. Por tanto, 3.4 también es una presentación de E, y el subgrupo generado por $b = x^\gamma, c, \ldots, t$ tiene la presentación del enunciado. □

Utilizando el teorema de la independencia y su método de demostración se puede probar el llamado teorema de la conjugación para grupos presentados con una única relación.

Teorema 3.1.4 Sea $G = \langle a_1, \ldots, a_n; R(a_1, \ldots, a_n)\rangle$ y $H = \langle a_1, \ldots, a_n; S(a_1, \ldots, a_n)\rangle$. Entonces G es isomorfo a H bajo la aplicación $a_\nu \to a_\nu$ si y sólo si $R(a_1, \ldots, a_n)$ y $S^\epsilon(a_1, \ldots, a_n)$ son conjugados en el grupo libre en $a_1, \ldots, a_n$, para $\epsilon = 1$ o $\epsilon = -1$.

Veamos una consecuencia del teorema anterior:

Corolario 3.1.5 Si $G = \langle a_1, \ldots, a_n; V^k(a_1, \ldots, a_n)\rangle$ con $k > 1$ y V palabra no vacía, entonces V define un elemento $v \in G$ de orden exactamente k.

Demostración: Podemos suponer que V es cíclicamente reducida pues si no lo fuese podríamos sustituir V por su reducción cíclica, que al ser conjugado de V tiene su mismo orden. Sea F el grupo libre en $a_1, \ldots, a_n$. Si denotamos por d el orden de v en G, sabemos que d divide a k. Además, V^d es relator en G, lo que implica que el elemento que V^d define en F pertenece al subgrupo normal de F generado por el elemento definido por V^k, donde F es el grupo libre en $a_1, \ldots, a_n$. Por tanto, el subgrupo normal de F generado por V^d (o, mejor dicho, por el elemento que esta palabra define en F) está contenido en el subgrupo normal de F generado por V^k. El otro contenido es trivialmente cierto, lo que implica que V^d y V^k determinan el mismo subgrupo normal de F y, por el teorema 3.1.4, V^d es conjugado en F de V^k o de V^{-k}. En cualquiera de los dos casos, ambas palabras son cíclicamente reducidas (por serlo V) y conjugadas, luego por 1.3.4, tienen la misma longitud, de donde $d = k$. □

Del teorema de la independencia y de su método de demostración obtenemos también la siguiente caracterización de los grupos presentados con una única relación que poseen elementos no triviales de orden finito.

Proposición 3.1.6 Si $G = \langle a_1, \ldots, a_n; R(a_1, \ldots, a_n)\rangle$, entonces G posee un elemento no trivial de orden finito si y sólo si R es la potencia k-ésima (con $k > 1$) de alguna palabra no vacía V en los generadores $a_1, \ldots, a_n$.

Demostración: La condición sobre R es suficiente, ya que entonces se tiene que

$$G = \langle a_1, \ldots, a_n; V^k\rangle$$

con V palabra no vacía y $k > 1$, lo que por el corolario anterior implica que G posee un elemento no trivial de orden finito: el elemento definido por V, que tiene orden k. Recíprocamente, supongamos que $G = \langle a_1, \ldots, a_n; R(a_1, \ldots, a_n)\rangle$ tiene un elemento no trivial de orden finito. Entonces R ha de tener como mínimo longitud 2 y, en caso de tener longitud exactamente 2 ha de involucrar un único generador. Si R sólo involucra un generador entonces el resultado es claro, independientemente de la longitud de R. Podemos, por tanto, suponer que R involucra más de un generador.

Por inducción supongamos que el resultado es cierto para cualquier grupo presentado con un único relator cuya longitud es menor que la de R. Podemos suponer que R es cíclicamente reducida.

Caso 1: Supongamos que $\sigma_t(R) = 0$ para algún generador t involucrado en R y supongamos que R involucra al menos otro generador b. Todo relator en G es un producto de conjugados de R y R^{-1} así que tiene suma nula en los exponentes de t. En particular, si U define un elemento no trivial de orden d finito en G, entonces $\sigma_t(U^d) = d\sigma_t(U) = 0$. Así U define un elemento en el subgrupo normal N de G generado por los generadores distintos de t. Si τ es el proceso de reescritura de Reidemeister-Schreier, usando $\{t^m\}$ como representantes, denotando por $b_m, c_m, \ldots$ a $t^m b t^{-m}, t^m c t^{-m}, \ldots$ y $P_m = \tau(t^m R t^{-m})$, para cualquier m entero, entonces se tiene

$$N = \langle \ldots, b_{-1}, b_0, b_1, \ldots, c_{-1}, c_0, c_1, \ldots; \ldots, P_{-1}, P_0, P_1, \ldots\rangle$$

y se pueden definir los grupos

$$N_i = \langle \ldots, c_{-1}, c_0, c_1, \ldots, b_{\mu+i}, \ldots, b_{M+i}; P_i\rangle \tag{3.5}$$

donde μ y M son los subíndices mínimo y máximo de b que aparecen en P_0. Procedemos como de costumbre para obtener la cadena de subgrupos

$$N_0 \subseteq N_{0,1} \subseteq N_{-1,1} \subseteq N_{-1,2} \subseteq \cdots \subseteq N_{-i+1,i} \subseteq N_{-i,i} \subseteq N_{-i,i+1} \subseteq \ldots \tag{3.6}$$

cuya unión es N. Como N tiene un elemento no trivial de orden finito, también lo tendrá uno de los grupos de la cadena, pero éstos se construyen como productos amalgamados, por lo que podemos aplicar 2.2.12 y concluir que uno de los grupos N_i en 3.5 tiene que tener un

elemento no trivial de orden finito. Como N_0 es isomorfo a N_i, lo mismo se cumple para N_0. Pero P_0 tiene longitud menor que R, luego por hipótesis de inducción

$$P_0(\dots, b_m, \dots, c_m, \dots) \approx W^k(\dots, b_m, \dots, c_m, \dots)$$

para algún $k > 1$. Entonces

$$R(b, c, \dots, t) \approx P_0(\dots, t^m b t^{-m}, \dots, t^m c t^{-m}, \dots) \approx$$

$$W^k(\dots, t^m b t^{-m}, \dots, t^m c t^{-m}, \dots) = V^k(b, c, \dots, t)$$

donde

$$V(b, c, \dots, t) = W(\dots, t^m b t^{-m}, \dots, t^m c t^{-m}, \dots)$$

Caso 2: Supongamos que la suma de exponentes es no nula para cualquier generador involucrado en $R(b, c, \dots, t)$. Consideramos el grupo

$$\langle x, c, \dots, t; R(x^\alpha, c, \dots, t)\rangle \tag{3.7}$$

donde $\alpha = \sigma_t(R)$. El grupo definido en 3.7 es el producto amalgamado de G y el grupo cíclico infinito generado por x con los subgrupos generados por x^α y b amalgamados bajo $x^\alpha \to b$. Como G tiene un elemento no trivial de orden finito, lo mismo ha de cumplirse para el grupo definido en 3.7. Aplicando transformaciones de Tietze, obtenemos que

$$\langle x, c, \dots, y; R(x^\alpha, c, \dots, y x^{-\beta})\rangle \tag{3.8}$$

es otra presentación para el grupo definido en 3.7, siendo $\beta = \sigma_b(R)$. La suma de los exponentes de x del relator en 3.8 es nula, de modo que consideramos el subgrupo normal del grupo definido en 3.8 generado por $c, \dots, y$. Tenemos, por el caso anterior, que $R(x^\alpha, c, \dots, y x^{-\beta}) = V^k(x, c, \dots, y)$ para algún $k > 1$ en el grupo libre en $x, c, \dots, y$. Haciendo $y = t x^\beta$, $R(x^\alpha, c, \dots, t) = S^k(x, c, \dots, t)$ en el grupo libre en $x, c, \dots, t$. Falta probar que $S(x, c, \dots, t)$ es una palabra de la forma $W(x^\alpha, c, \dots, t)$. Como $R(b, c, \dots, t)$ es cíclicamente reducida, también lo es $R(x^\alpha, c, \dots, t)$. Como podemos suponer que $S(x, c, \dots, t)$ es reducida, S debe ser cíclicamente reducida y un segmento inicial y final de $R(x^\alpha, c, \dots, t)$. Cualquier x^η que aparezca en S o bien rodeado de generadores distintos de x o bien al principio o bien al final de S debe tener η múltiplo de α. Es decir, $S(x, c, \dots, t) = W(x^\alpha, c, \dots, t)$. Por tanto, $R(x^\alpha, c, \dots, t) = W^k(x^\alpha, c, \dots, t)$ de donde $R(b, c, \dots, t) = W^k(b, c, \dots, t)$ en el grupo libre en $b, c, \dots, t$. □

Proposición 3.1.7 Si $G = \langle a_1, \dots, a_n; V^k(a_1, \dots, a_n)\rangle$ con $k > 1$ y $V(a_1, \dots, a_n)$ no es una verdadera potencia en el grupo libre en $a_1, \dots, a_n$, todo elemento de orden finito de G está definido por un conjugado de una potencia de V.

Demostración: De nuevo, usamos inducción en la longitud de V. Si V involucra sólo un generador (en particular, si tiene longitud uno), el resultado se sigue de 2.1.10. Supongamos que el resultado se verifica para todos lo grupos presentados con un único relator U^k donde U no es una verdadera potencia y tiene longitud menor que la de V. Podemos suponer que V es cíclicamente reducida, si no, sustituiríamos V por un conjugado suyo cíclicamente reducido de menor longitud y el resultado se cumpliría por hipótesis de inducción. Representamos $a_1, \ldots, a_n$ por $b, c, \ldots, t$.

Caso 1: Supongamos que la suma de los exponentes de alguno de los generadores involucrados en V es 0. Por ejemplo, $\sigma_t(V) = 0$. Sea b otro generador involucrado en V. Como V^k tiene suma en los exponentes cero en t, lo mismo ocurre con cualquier relator de G, luego todos los elementos de orden finito están en el subgrupo normal N de G generado por $b, c, \ldots$. Presentando N como en la demostración anterior, tenemos

$$N = \langle \ldots, b_{-1}, b_0, b_1, \ldots, c_{-1}, c_0, c_1, \ldots; \ldots, P_{-1}^k, P_0^k, P_1^k, \ldots \rangle$$

donde $P_i = \tau(t^i R t^{-i})$. Definiendo μ y M como los subíndices mínimo y máximo de b que aparecen en P_0, tenemos los grupos

$$N_i = \langle \ldots, c_{-1}, c_0, c_1, \ldots, b_{\mu+i}, \ldots, b_{M+i}; P_i^k \rangle$$

a partir de los cuales obtenemos la cadena de grupos

$$N_0 \subseteq N_{0,1} \subseteq N_{-1,1} \subseteq N_{-1,2} \subseteq \cdots \subseteq N_{-i+1,i} \subseteq N_{-i,i} \subseteq N_{-i,i+1} \subseteq \ldots$$

cuya unión es N. Todo elemento de orden finito de N está en uno de los grupos de la cadena, y por la forma en que éstos están construidos, es conjugado de un elemento de orden finito en alguno de los grupos N_i. Entonces, por una propiedad de τ,

$$t^i V(b, c, \ldots, t) t^{-i} \approx P_i(\ldots, t^m b t^{-m}, \ldots, t^m c t^{-m}, \ldots)$$

Por tanto, si V no es una verdadera potencia en el grupo libre en $b, c, \ldots, t$, tampoco lo puede ser P_i en el grupo libre en $\ldots, c_{-1}, c_0, c_1, \ldots, b_{\mu+i}, \ldots, b_{M+i}$. Luego, por hipótesis de inducción, los elementos de orden finito en N_i son conjugados de potencias de P_i. Pero en G el elemento definido por P_i es un conjugado de V, luego todo elemento de orden finito en G es un conjugado de una potencia de V.

Caso 2: Supongamos que V tiene suma en los exponentes no nula en todos los generadores que involucra. Sean $\alpha = \sigma_t(V)$ y $\beta = \sigma_b(V)$ y construyamos el grupo

$$\langle x, c, \ldots, t; V^k(x^\alpha, c, \ldots, t) \rangle \tag{3.9}$$

que, como antes, haciendo $t = yx^{-\beta}$ se puede escribir también:

$$\langle x, c, \ldots, y; V^k(x^\alpha, c, \ldots, yx^{-\beta})\rangle \tag{3.10}$$

Como $V(b, c, \ldots, t)$ es cíclicamente reducida, se puede probar que si $V(x^\alpha, c, \ldots, yx^{-\beta})$ es una verdadera potencia, entonces $V(x^\alpha, c, \ldots, t)$ es una verdadera potencia y también lo es $V(b, c, \ldots, t)$. Así, $V(x^\alpha, c, \ldots, yx^{-\beta})$ no es una verdadera potencia. Usando el método de demostración del caso anterior (pues ahora $\sigma_x(V) = 0$), tomando como N el subgrupo normal de 3.10 generado por $c, \ldots, y$, podemos ver que los elementos de 3.10 de orden finito son conjugados en 3.10 de potencias de $V(x^\alpha, c, \ldots, yx^{-\beta})$. Aplicando la transformación de Tietze $y = tx^\beta$ a 3.10, obtenemos que los elementos en 3.9 de orden finito son conjugados en 3.9 de potencias de $V(x^\alpha, c, \ldots, t)$. Por tanto, un elemento no trivial W de orden finito en G que está en el subgrupo de 3.9 generado por $x^\alpha, c, \ldots, t$ debe ser un conjugado de una potencia de $V(x^\alpha, c, \ldots, t)$. Por tanto, en 3.9,

$$W(x^\alpha, c, \ldots, t) = TV^q(x^\alpha, c, \ldots, t)T^{-1}$$

donde T es una palabra en $x, c, \ldots, t$. Debemos probar que T es en realidad una palabra en $x^\alpha, c, \ldots, t$, es decir, que T define un elemento de G.

El grupo 3.9 es el producto libre de X (el grupo cíclico infinito en x) y G con los subgrupos cíclicos infinitos H, K generados por x^α, b en X y G, respectivamente, amalgamados bajo $\varphi : x^\alpha \to b$. Como V^q tiene orden finito y H es cíclico infinito, V^q no está en un conjugado de H. Por tanto, el problema se reduce a probar que en $*(X, G, H, K, \varphi)$, que es el grupo definido en 3.9, si g y sgs^{-1} están en G y g no está en un conjugado de H, entonces s está en G.

Pero si s no estuviese en G, s tendría la forma $s_1 \ldots s_p$ donde los s_i se alternan en X y en G (en particular, no pertenecen a H ó K). Por tanto, s_p está en X ó s_p está en G y s_{p-1} está en X. Pero la longitud en los representantes de

$$sgs^{-1} = s_1 \ldots s_{p-1} s_p g s_p^{-1} s_{p-1}^{-1} \ldots s_1^{-1} = s_1 \ldots s_{p-1}(s_p g s_p^{-1}) s_{p-1}^{-1} \ldots s_1^{-1}$$

no puede ser uno si s_p está en X, o si s_p está en G y s_{p-1} está en X, luego sgs^{-1} no podría estar en G.

Por tanto, T define un elemento de G, de donde W (que es un elemento de orden finito en G) debe ser un conjugado de una potencia de V en G. □

Corolario 3.1.8 Supongamos que el grupo $G = \langle a_1, \ldots, a_n; V^k(a_1, \ldots, a_n)\rangle$ es isomorfo al grupo $H = \langle a_1, \ldots, a_n; U^k(a_1, \ldots, a_n)\rangle$. Entonces $K = \langle a_1, \ldots, a_n; V(a_1, \ldots, a_n)\rangle$ es isomorfo a $L = \langle a_1, \ldots, a_n; U(a_1, \ldots, a_n)\rangle$.

Demostración: Expresemos $V = W^r$ donde W ya no es una verdadera potencia. Entonces $G = \langle a_1, \ldots, a_n; W^{kr}(a_1, \ldots, a_n)\rangle$, de donde (por el corolario 3.1.5) W tiene orden kr en G. Como, por 3.1.7, cualquier otro elemento de orden finito en G es un conjugado de una potencia de W, kr es el máximo orden que puede tener un elemento de orden finito en G. Sea ahora $U = Y^s$, donde Y no es una verdadera potencia. Razonando como antes, Y tiene orden ks y además ks es el máximo orden que puede tener un elemento de orden finito en H. Como $G \cong H$, $kr = ks$, de donde $r = s$. Los elementos de G de orden divisor de k son exactamente los conjugados de potencias de $W^r = V$. Del mismo modo, en H los elementos de G de orden divisor de k son exactamente los conjugados de potencias de $Y^r = U$. Sea φ el isomorfismo entre G y H. Como V tiene orden divisor de k en G, $\varphi(V)$ tiene orden divisor de k en H, luego es un conjugado de una potencia de U. Del mismo modo, $\varphi^{-1}(U)$ es un conjugado de una potencia de V. Por tanto, el subgrupo normal N de G generado por V se corresponde por φ con el subgrupo normal M de H generado por U. Así, $G/N \cong H/M$. Como $G/N = K$ y $H/M = L$, se tiene que $K \cong L$. □

Corolario 3.1.9 Sean R y S pertenecientes al grupo libre F en $a_1, \ldots, a_n$. Si S^k pertenece al subgrupo normal de F generado por R^k, entonces S pertenece al subgrupo normal de F generado por R. Es decir, si S^k es derivable de R^k entonces S es derivable de R.

Demostración: Supongamos que expresamos $R = W^r$ donde W ya no es una verdadera potencia. En el grupo

$$G = \langle a_1, \ldots, a_n; R^k\rangle = \langle a_1, \ldots, a_n; W^{rk}\rangle,$$

S^k define la identidad, luego S tiene orden finito divisor de k en G y, razonando como en el teorema anterior, S ha de ser un conjugado de $(W^r)^t = R^t$ para cierto t. Como R^k es el relator en la presentación de G, la palabra S, como elemento del grupo libre F, ha de ser libremente igual al producto de un conjugado de R^t y conjugados de R^k y R^{-k}. Por tanto, S es un producto de conjugados de R y R^{-1}, de donde el resultado. □

3.2. El problema de la palabra para grupos presentados con una única relación.

Finalmente, nos centraremos en el problema de la palabra para grupos presentados con una única relación. La solución de este problema requerirá del siguiente lema auxiliar:

Lema 3.2.1 Sea $G = *(A_1, A_2, H_1, H_2, \varphi)$. Supongamos que tenemos un procedimiento para determinar si un elemento de A_i pertenece a H_i y, en caso afirmativo, para escribirlo como

elemento de H_i; y supongamos que φ y φ^{-1} se pueden calcular ambas mediante un procedimiento específico. Entonces podemos decidir si un elemento de G pertenece a A_i y, en caso afirmativo, podemos escribirlo como elemento de A_i.

Demostración: Sea g dado como un producto $g_1 g_2 \dots g_n$ donde los g_j son elementos que pertenecen alternativamente a los A_i's. Probaremos por inducción en n que podemos decidir si g está en A_i y, en caso afirmativo, escribirlo como un elemento de A_i.

Si $n = 1$ entonces $g = g_1$ pertenece o bien a A_1 o bien a A_2. Además, pertenecerá a los dos si y sólo si g_1 pertenece a A_1 y a H_1 ó g_1 pertenece a A_2 y a H_2. Como esto, por hipótesis, lo podemos determinar y φ se puede calcular mediante un procedimiento específico, podemos decidir si g_1 está en A_i y, en caso afirmativo, escribirlo como un elemento de A_i.

Supongamos que podemos tomar esta decisión para elementos definidos por palabras de longitud silábica aparente menor que n y supongamos que g tiene longitud silábica aparente n con $n > 1$ ($g = g_1 g_2 \dots g_n$). Si ninguno de los g_j está en H_1 ó H_2, entonces g tendrá longitud en los representantes $n > 1$, luego no puede estar en A_i. Supongamos que algún g_j pertenece a A_1 y a H_1 o pertenece a A_2 y a H_2. Supongamos, para fijar ideas, que g_j pertenece a A_1 y a H_1. Entonces $\varphi(g_j)$ está en A_2 y H_2. En G,

$$g = g_1 g_2 \dots g_{j-1} \varphi(g_j) g_{j+1} \dots g_n = g_1 g_2 \dots g_{j-2} (g_{j-1} \varphi(g_j) g_{j+1}) g_{j+2} \dots g_n$$

Como g_{j-1}, g_{j+1} están en A_2, g tiene longitud silábica aparente menor que n, luego por hipótesis de inducción podemos decidir si g está en A_i y, en caso afirmativo, escribirlo como un elemento de A_i. □

Ahora ya estamos en condiciones de resolver el problema de la palabra para grupos presentados con una única relación.

Teorema 3.2.2 Dado un grupo $G = \langle a_1, \dots, a_n; R(a_1, \dots, a_n) \rangle$ entonces el problema de la palabra para G es resoluble.

Demostración: Para resolver el problema de la palabra en un grupo presentado con una sola relación, lo que haremos será resolver el problema de la palabra extendido para dicho grupo. El problema de la palabra extendido es el problema de decidir, dado un subconjunto propio (posiblemente vacío) de los generadores, si un elemento se puede expresar en términos de solamente esos generadores y, en caso afirmativo, encontrar al menos una expresión del elemento en términos de dichos generadores. Este problema es más general que el problema de la palabra, pues el problema de la palabra se corresponde con el caso en que el subconjunto propio de generadores elegido es vacío.

Vamos a dividir la demostración en dos partes. En la primera reduciremos el problema que tenemos que resolver a un problema más sencillo, que abordaremos en la segunda parte.

Más concretamente, lo primero que haremos será probar que, para grupos presentados con una única relación, el problema de la palabra extendido se reduce a resolver el problema de decidir si un elemento (en un grupo presentado con una única relación que involucra a todos los generadores) se puede expresar sin que intervenga un determinado generador y, en caso afirmativo, encontrar al menos una expresión del elemento en esas condiciones. Es decir, veremos que el problema de la palabra extendido para grupos presentados con una única relación se puede reducir al problema de la palabra extendido para tales grupos cuando la relación involucra todos los generadores tomando subconjuntos de generadores propios maximales. La segunda parte de la demostración consistirá precisamente en probar que este último problema es resoluble.

Supongamos en primer lugar que $G = \langle a_1, \ldots, a_n; R(a_1, \ldots, a_n)\rangle$ y que R involucra a todos los generadores. Dado cualquier subconjunto propio de generadores $\{a_{i_1}, \ldots, a_{i_r}\}$, tomemos un generador que no pertenezca a dicho subconjunto, por ejemplo, supongamos que a_n no es uno de los a_{i_j}'s. Para decidir si un elemento g se puede expresar en términos de $a_{i_1}, \ldots, a_{i_r}$, primero veamos si g se puede expresar en términos de $a_1, \ldots, a_{n-1}$. Si es posible, expresemos g en términos de $a_1, \ldots, a_{n-1}$ y reduzcamos libremente la palabra resultante. Como por el teorema de la independencia, $a_1, \ldots, a_{n-1}$ generan libremente un subgrupo libre de G, g se puede expresar en términos de $a_{i_1}, \ldots, a_{i_r}$ si y sólo si la palabra reducida que representa g en términos de $a_1, \ldots, a_{n-1}$ sólo involucra $a_{i_1}, \ldots, a_{i_r}$. Por tanto, acabamos de ver que el problema de la palabra extendido para cualquier subconjunto propio de generadores se reduce a resolver el problema extendido de la palabra para subconjuntos propios maximales en el caso en que todos los generadores estén involucrados en la relación R.

Supongamos ahora que R no involucra a todos los generadores. Para fijar ideas, supongamos que $a_{k+1}, \ldots, a_n$ son los generadores que aparecen en R. Dentro de este caso vamos a estudiar por separado las dos posibles situaciones que se pueden presentar, por una parte el caso en que $a_{k+1}, \ldots, a_n$ pertenecen todos al subconjunto $\{a_{i_1}, \ldots, a_{i_r}\}$ para el cual deseamos resolver el problema de la palabra extendido; y, por otra parte, el caso en que alguno de los generadores $a_{k+1}, \ldots, a_n$ no pertenece a $\{a_{i_1}, \ldots, a_{i_r}\}$. En el primero de los casos, los generadores que no pertenecen a $\{a_{i_1}, \ldots, a_{i_r}\}$ serán algunos de entre los siguientes: $a_1, \ldots, a_k$; supongamos, en concreto, que son $a_1, \ldots, a_s$. Entonces G será el producto libre del grupo libre F es los generadores libres $a_1, \ldots, a_s$ y el grupo $G' = \langle a_{s+1}, \ldots, a_n; R(a_{k+1}, \ldots, a_n)\rangle$. Resolver, entonces, el problema de la palabra extendido para $\{a_{i_1}, \ldots, a_{i_r}\} = \{a_{s+1}, \ldots, a_n\}$ equivale a decidir si un elemento de $G = F * G'$ está en G'. Para ello, bastará aplicar el lema 3.2.1 tomando $A_1 = F, A_2 = G', H_1 = H_2 = 1, \varphi =$ identidad. Para poder aplicar el lema hemos de garantizar que se cumplen las hipótesis, lo que es cierto pues en este caso lo que necesitamos es poder resolver el problema de la palabra para F y para G'. Pero el problema

de la palabra para F es resoluble pues F es un grupo libre dado en términos de generadores libres; y como $G' = F' * G''$ con F' grupo libre en los generadores libres $a_{s+1}, \ldots, a_k$ y $G'' = \langle a_{k+1}, \ldots, a_n; R(a_{k+1}, \ldots, a_n)\rangle$, el problema de la palabra para G' se puede reducir al problema de la palabra para F' que es resoluble y al problema de la palabra para G'' que, por lo anteriormente razonado, se puede reducir al problema de la palabra extendido para subconjuntos propios maximales de generadores de G''.

Por último, para completar la primera parte de la demostración, supongamos que R involucra como antes a los generadores $a_{k+1}, \ldots, a_n$ pero alguno de ellos no pertenece a $\{a_{i_1}, \ldots, a_{i_r}\}$; por ejemplo, supongamos que a_n no pertenece a $\{a_{i_1}, \ldots, a_{i_r}\}$.

En este caso, $G = F * G'$ con F el grupo libre en los generadores libres $a_1, \ldots, a_k$ y $G' = \langle a_{k+1}, \ldots, a_n; R(a_{k+1}, \ldots, a_n)\rangle$. Además, $a_1, \ldots, a_{n-1}$ generan libremente un subgrupo libre de G. Para decidir si un elemento $g \in G = F * G'$ se puede expresar en términos de $a_1, \ldots, a_{n-1}$, primero escribimos g en la forma canónica respecto a $F * G'$, para lo cual sólo necesitamos resolver el problema de la palabra para F (grupo libre presentado en términos de generadores libres) y el problema de la palabra para G' (que se puede reducir al problema de la palabra extendido para subconjuntos propios maximales de G'). Es más, de esta manera podemos decidir si las sílabas de g que pertenecen a G' se pueden expresar sin que intervenga el generador a_n. Todo ello implica que podemos, en definitiva, decidir si g se puede expresar en términos de $a_1, \ldots, a_{n-1}$, es decir, si pertenece al subgrupo libre F' de G libremente generado por $a_1, \ldots, a_{n-1}$ (y, en caso afirmativo, encontrar una expresión para g en términos de $a_1, \ldots, a_{n-1}$). Como $a_{i_1}, \ldots, a_{i_r}$ pertenecen a $\{a_1, \ldots, a_{n-1}\}$, ahora resulta sencillo decidir si g se puede expresar como una palabra en $a_{i_1}, \ldots, a_{i_r}$: basta reducir libremente la palabra en $a_1, \ldots, a_{n-1}$ que representa a g. La respuesta será afirmativa si y sólo si en el resultado sólo intervienen los símbolos $a_{i_1}, \ldots, a_{i_r}$.

Esto completa la primera parte de la demostración. Supondremos entonces ya que en el grupo $G = \langle a_1, \ldots, a_n; R(a_1, \ldots, a_n)\rangle$ del enunciado la relación R involucra a todos los generadores. Y probaremos que el problema de la palabra extendido para subconjuntos propios maximales de generadores es resoluble. Lo haremos por inducción en la longitud de R. Si R tiene longitud 1 o involucra sólo un generador entonces G es cíclico (porque R involucra todos los generadores) y el problema es resoluble. Supongamos entonces que la afirmación se verifica para todos los grupos presentados con un solo relator de longitud menor que la de R y supongamos, además, que R involucra por lo menos dos generadores. Como ya es habitual, representaremos $a_1, \ldots, a_n$ por $b, c, \ldots, t$. Vamos a diferenciar dos casos:

Caso 1: Supongamos que $\sigma_t(R) = 0$ para algún generador t. Tomemos N el subgrupo normal de G generado por el resto de generadores, $b, c, \ldots$, y denotemos por τ el proceso de reescritura, y $b_k := t^k b t^{-k}, c_k := t^k c t^{-k}, \ldots$ Para ver que el problema de la palabra extendido

para subconjuntos maximales de generadores se puede reducir a estudiar N, supongamos primero que el conjunto propio maximal de generadores excluye t. Entonces tenemos que decidir si un elemento definido por una palabra W que involucra t se puede definir mediante otra palabra que involucre sólo los símbolos $b, c, \ldots$. Puesto que $\sigma_t(R) = 0$, si la respuesta es afirmativa también tendría que ocurrir que $\sigma_t(W) = 0$ pues la palabra en $b, c, \ldots$ que obtendríamos a partir de W se obtendría por inserción o eliminación de relatores triviales, R ó R^{-1}, luego no varía el exponente suma en t. Puesto que se tendría $\sigma_t(W) = 0$, W definiría un elemento de N, luego el problema extendido de la palabra se transforma en un problema de expresar un elemento de N en términos de $b_0, c_0, \ldots$, en caso de que sea posible.

Supongamos ahora que el generador de G excluido del subconjunto propio maximal es distinto de t, por ejemplo, supongamos que es b. Entonces W puede no definir un elemento de N. Pero si W se puede expresar en G sin utilizar b, lo mismo ocurre con $Wt^{-\alpha}$ siendo $\alpha = \sigma_t(W)$ (el recíproco también es cierto). Ahora bien, la palabra $Wt^{-\alpha}$ sí que define un elemento de N, por lo que el problema se reduce a expresar un elemento de N sin utilizar ningún b_k, en caso de que sea posible.

Permutando cíclicamente R, podemos suponer que R comienza con un b-símbolo. Por tanto, $\tau(R)$ involucra b_0, luego si definimos $\tau(t^i R t^{-i}) = P_i(\ldots, b_k, \ldots, c_k, \ldots)$, tenemos que b_0 aparece en P_0. Si además definimos μ, M como los subíndices k mínimo y máximo (respectivamente) tales que b_k aparece en P_0 y

$$N_i = \langle \ldots, c_k, \ldots, b_{\mu+i}, \ldots, b_{M+i}; P_i \rangle$$

tenemos que, tanto si es t como si es b el símbolo excluido del subconjunto maximal de generadores, lo que necesitamos es decidir si un elemento dado de N se puede expresar en términos de un subconjunto de los generadores de

$$N_0 = \langle \ldots, c_k, \ldots, b_\mu, \ldots, b_M; P_0 \rangle$$

y, en caso afirmativo, expresarlo de tal forma. No obstante, puesto que la longitud de P_0 es menor que la de R, por hipótesis de inducción el problema de la palabra extendido es resoluble para N_0, lo que implica que una vez que tenemos un elemento expresado como elemento de N_0, podemos decidir si ese elemento es expresable en términos de un subconjunto propio de generadores de N_0 y, en caso afirmativo, expresarlo de tal forma.

Por tanto, el problema se reduce a determinar si un elemento de N pertenece a N_0 y, en caso afirmativo, expresarlo como elemento de N_0. Lo que probaremos, de hecho, es que podemos determinar si un elemento de N está en un N_i cualquiera y, si está, expresarlo como elemento de N_i.

Como N es la unión de la cadena de grupos

$$Q_1 = N_0, \quad Q_2 = N_{0,1}, \quad Q_3 = N_{-1,1,1}, \ldots$$

definidos en 3.5 y 3.6, cualquier elemento de N está en algún Q_j. Probaremos que, para todo j, si los generadores de N_i están contenidos en los de Q_j, podemos decidir si un elemento de Q_j está en N_i y, en caso afirmativo, expresarlo como tal. Procederemos por inducción en j. Si $j = 1$, entonces $Q_1 = N_0$ y el único N_i con sus generadores contenidos en los de Q_j es N_0, luego claramente se cumple el resultado. Supongamos el resultado cierto para Q_s. Por construcción, Q_{s+1} es el producto libre de Q_s y algún N_p con el subgrupo K generado por todos los generadores de N_p excepto por uno de los b_k's amalgamado bajo la aplicación identidad. Por tanto, cualquier N_i cuyos generadores estén incluidos en los de Q_{s+1} está contenido en Q_s o en N_p. Utilizamos el lema 3.2.1 tomando $A_1 = Q_s, A_2 = N_p, H_1 = H_2 = K, \varphi =$ identidad. En efecto, se cumplen las hipótesis del lema puesto que el problema de la palabra extendido es resoluble para N_p por hipótesis de inducción pues los P_i's tienen menor longitud que R, luego podemos decidir si un elemento de N está en K. Como K está contenido en algún N_u cuyos generadores están entre los de Q_s, podemos determinar (por hipótesis de inducción) si un elemento dado de Q_s está en N_u. Si el elemento de Q_s está en N_u, podemos decidir si está en K. Luego podemos decidir si el elemento de Q_s está en K. Como además φ está especificada, el lema 3.2.1 nos permite concluir que podemos decidir si un elemento de Q_{s+1} está en Q_s o en N_p. Podemos por tanto decidir, tanto si $N_i \subseteq Q_s$ como si $N_i = N_p$, si un elemento de Q_{s+1} está en N_i y, en tal caso, expresarlo como tal. Esto completa la inducción en j para probar que si los generadores de un N_i están contenidos en los de Q_j, podemos decidir si un elemento de Q_j está en N_i y, en caso afirmativo, expresarlo como tal.

Por tanto, podemos decidir si un elemento de N está en N_i y expresarlo como tal si está. Como esto es cierto para cualquier i, en particular lo es para $i = 0$, lo que finaliza la demostración del caso 1.

Caso 2: Supongamos ahora que $\sigma_a(R) \neq 0$ para todo generador a. R involucra al menos dos generadores, por ejemplo, b, t, y todos los generadores aparecen en R. Supongamos que el generador excluido del subconjunto propio maximal de generadores para el que queremos resolver el problema de la palabra extendido es t. Tomemos el grupo

$$E = \langle x, c, \ldots, t; R(x^\alpha, c, \ldots, t) \rangle \tag{3.11}$$

donde $\alpha = \sigma_t(R)$. Mediante una transformación de Tietze tenemos que E también tiene la presentación $\mathcal{P}$ siguiente:

$$\langle x, c, \ldots, y; R(x^\alpha, c, \ldots, yx^{-\beta}) \rangle \tag{3.12}$$

donde $\beta = \sigma_b(R)$. Ahora $\sigma_x(R(x^\alpha, c, \ldots, yx^{-\beta})) = 0$; por tanto, aplicamos el caso 1 tomando como N el subgrupo normal de E generado por $c, \ldots, y$, obteniendo que el problema de la palabra extendido es resoluble para (3.12).

Sea $W(b, c, \ldots, t)$ una palabra en G. La aplicación $b \to x^\alpha, c \to c, \ldots, t \to t$ define un monomorfismo de G en E. Y la aplicación $x \to x, c \to c, \ldots, t \to yx^{-\beta}$ define un monomorfismo de E en $G(\mathcal{P})$. Luego $b \to x^\alpha, c \to c, \ldots, t \to yx^{-\beta}$ define un monomorfismo de G en $G(\mathcal{P}) \cong E$. Por tanto, $W(b, c, \ldots, t)$ puede definir el mismo elemento que $V(b, c, \ldots)$ en G si y sólo si $W(x^\alpha, c, \ldots, yx^{-\beta})$ puede definir el mismo elemento que $V(x^\alpha, c, \ldots, yx^{-\beta})$ en E. Por tanto, para decidir si W se puede expresar sin t en G debemos decidir si $W(x^\alpha, c, \ldots, yx^{-\beta})$ se puede expresar en términos de $x^\alpha, c, \ldots$ en E y, en caso afirmativo, encontrar una tal expresión. Como el problema de la palabra extendido es resoluble para (3.12), podemos decidir si $W(x^\alpha, c, \ldots, yx^{-\beta})$ se puede expresar en términos de $x, c, \ldots$ (sin y) y lograr, si es posible, una expresión explícita. Ahora bien, por el teorema de la independencia, $x, c, \ldots$ genera libremente un subgrupo libre de (3.12), luego podemos decidir si una palabra en $x, c, \ldots$ se puede expresar en (3.12) como una palabra en $x^\alpha, c, \ldots$. En resumen, podemos decidir si, en (3.12), $W(x^\alpha, c, \ldots, yx^{-\beta})$ se puede expresar en términos de $x^\alpha, c, \ldots$ y encontrar, si es posible, una expresión de dicha forma. En consecuencia, podemos decidir si, en G, $W(b, c, \ldots, t)$ se puede expresar sin t y encontrar, si es posible, una expresión de dicha forma. □

El resultado anterior es válido incluso si G no está finitamente generado.

Corolario 3.2.3 Sean $R(a_1, \ldots, a_n)$ y $S(b_1, \ldots, b_m)$ palabras cíclicamente reducidas involucrando a_n y b_m, respectivamente; y sean $U(a_1, \ldots, a_{n-1})$, $V(b_1, \ldots, b_{m-1})$ palabras no vacías reducidas. Entonces el problema de la palabra para el grupo

$$G = \langle a_1, \ldots, a_n, b_1, \ldots, b_m; R, S, U = V \rangle$$

es resoluble.

Demostración: Denotemos $A = \langle a_1, \ldots, a_n; R \rangle$, $B = \langle b_1, \ldots, b_m; S \rangle$ y sea H el subgrupo cíclico de A generado por U y K el subgrupo cíclico de B generado por V. Por el teorema de la independencia sabemos que $a_1, \ldots, a_{n-1}$ generan libremente un subgrupo libre de A y, análogamente, $b_1, \ldots, b_{m-1}$ generan libremente un subgrupo libre de B. Por tanto, $U(a_1, \ldots, a_{n-1})$ y $V(b_1, \ldots, b_{m-1})$ tienen orden infinito, luego H es isomorfo a K bajo el isomorfismo φ dado por $\varphi(U) = V$. Por tanto, $G = *(A, B, H, K, \varphi)$. Para decidir si una palabra $W(a_1, \ldots, a_n, b_1, \ldots, b_m)$ define el neutro en G, lo primero que haremos será ver si define un elemento de A y, en caso afirmativo, expresarlo como tal. Este último problema lo podemos resolver aplicando el lema 3.2.1 con $A_1 = A, A_2 = B, H_1 = H, H_2 = K, \varphi = \varphi$. Tenemos que garantizar que se cumplen las hipótesis del lema. Por el teorema anterior sabemos que el problema de la palabra extendido es resoluble en A y en B. Por tanto, podemos decidir si un elemento de A o de B se puede expresar en términos de $a_1, \ldots, a_{n-1}$ ó $b_1, \ldots, b_{m-1}$, respectivamente y, en caso afirmativo, expresarlo como tal. Resulta evidente entonces, una

vez el elemento está expresado en términos de $a_1, \ldots, a_{n-1}$ ó $b_1, \ldots, b_{m-1}$, si es o no una potencia de U ó V, respectivamente. Esta última afirmación se debe a que $a_1, \ldots, a_{n-1}$ y $b_1, \ldots, b_{m-1}$ generan libremente subgrupos libres en A y B, respectivamente. Como además, φ está especificada por un procedimiento concreto que permite calcularla, que consiste en reemplazar U por V (y para calcular φ^{-1} de una palabra en K basta reemplazar V por U), tenemos que se cumplen las hipótesis del lema 3.2.1. Por tanto, este lema nos garantiza que podemos determinar si W define un elemento de A y, en caso afirmativo, expresarlo como tal. Si W no define un elemento de A, en particular no define el neutro. En caso contrario, una vez expresado como elemento de A, podemos usar el teorema anterior para resolver el problema de la palabra en A y, por tanto, decidir si W determina el neutro en A y, en consecuencia, en G. □

Corolario 3.2.4 Sea, para cada $i = 1, \ldots, r$, $R_i(x_i, y_1, \ldots, y_n)$ una palabra cíclicamente reducida involucrando el simbolo x_i. Entonces el problema de la palabra para el grupo

$$G = \langle x_1, \ldots, x_r, y_1, \ldots, y_n; R_1, R_2, \ldots, R_r \rangle$$

es resoluble.

Demostración: Por el teorema 3.2.2 sabemos que el problema de la palabra para el grupo $G_i = \langle x_i, y_1, \ldots, y_n; R_i \rangle$ es resoluble y podemos decidir si un elemento dado se puede expresar exclusivamente en términos de $y_1, \ldots, y_n$.

Definiendo $H_j = \langle x_1, \ldots, x_j, y_1, \ldots, y_n; R_1, R_2, \ldots, R_j \rangle$, podemos concluir por inducción en j que $H_1 = G_1$ y, para $j \geq 2$, H_j es el producto libre de H_{j-1} y G_j con el subgrupo libre en cada uno libremente generado por $y_1, \ldots, y_n$ amalgamado bajo la aplicación identidad. Por tanto, podemos probar también por inducción en j, y gracias al lema 3.2.1, que es posible decidir si un elemento de H_j puede ser expresado en términos de $y_1, \ldots, y_n$ y, en caso afirmativo, expresarlo de dicha forma. Como $y_1, \ldots, y_n$ generan libremente un subgrupo libre de $H_r = G$, podemos resolver el problema de la palabra en G. La solución viene dada de la siguiente manera: una palabra W en los generadores de G define el elemento neutro de G si y sólo si se puede expresar en términos de $y_1, \ldots, y_n$ y, una vez expresada de tal forma, al reducirla libremente obtenemos la palabra vacía. □

Capítulo 4

Algunos desarrollos recientes sobre el problema de la palabra

Este capítulo está dedicado a tratar, en términos generales, algunas de las líneas de investigación de teoría combinatoria de grupos estudiadas más recientemente, tanto en su vertiente más algebraica como desde un punto de vista más computacional.

Los problemas de decisión en teoría de grupos, como el problema de la palabra o el de la conjugación, se sitúan en la frontera entre las matemáticas y las ciencias de la computación, convirtiéndose así en un campo de estudio interdisciplinar que aúna teoría combinatoria de grupos, teoría de grafos y aspectos de complejidad algorítmica. Aunque se plantea desde una perspectiva algebraica, el desarrollo de la teoría de la complejidad computacional propició también el estudio de la complejidad del problema de la palabra como línea de investigación. Los desarrollos en este campo han atraído la atención por las potenciales aplicaciones de la teoría combinatoria de grupos a la construcción de criptosistemas, cuestión sobre la que se recoge una breve aproximación en el último capítulo de esta memoria.

El presente capítulo recoge desarrollos recientes sobre del problema de la palabra, que tras ser planteado por Dehn en 1911 adquirió fama cuando en 1954 Novikov y (de forma independiente) Boone en 1958, y Britton [3], también en 1958, probaron que no era resoluble en general, lo que implica que otros problemas de decisión en teoría de grupos, como el problema de la conjugación o el problema de la pertenencia, tampoco son resolubles. Concretamente, Britton construye un grupo finitamente presentado con problema de la palabra no resoluble que es producto amalgamado de grupos para los cuales el problema de la palabra sí es resoluble.

Más recientemente, se ha estudiado el problema de la palabra en variedades de grupos. Una variedad es una clase de grupos que satisfacen un determinado sistema de relaciones o identidades. El conjunto de estas relaciones se denomina "base" de la variedad. Una subclase

de una variedad que constituye, a su vez, una variedad en sí misma se denomina subvariedad.

Algunos ejemplos de variedades de grupos son:

- La mayor variedad es la formada por todos los grupos, definida por un conjunto de relaciones vacío.
- La variedad de los grupos abelianos: los grupos abelianos forman una variedad definida por las identidades $\{[x_1, x_2] = 1\}$, donde $[x_1, x_2]$ denota el conmutador de x_1 y x_2.
- Los grupos nilpotentes de clase de nilpotencia menor o igual que c forman una variedad definida por $\{[[\dots[[x_1, x_2], x_3]\dots], x_c] = 1\}$. Los grupos abelianos forman una subvariedad de esta variedad.
- Los grupos resolubles de longitud resoluble menor o igual que c forman también una variedad y, como en el caso anterior, la variedad de los grupos abelianos es una subvariedad suya.
- Para cada entero positivo n, los grupos de exponente divisor de n forman una variedad definida por la identidad $\{x^n = 1\}$. A esta variedad se la suele denotar B_n. También forman una variedad los grupos abelianos de exponente divisor de n, y se la suele denotar por A_n.

El producto $\mathcal{UB}$ de dos variedades $\mathcal{U}$ y $\mathcal{B}$ se define como la variedad de grupos formada por todos los grupos G que tienen un subgrupo normal $N \in \mathcal{U}$ tal que $G/N \in \mathcal{B}$. Así, la variedad A_pB_n está formada por los grupos G que tienen un subgrupo normal abeliano N de exponente divisor de p tal que G/N tiene exponente divisor de n.

Un grupo de una variedad $\mathcal{V}$ se dice finitamente presentado en la variedad si viene dado por un número finito de generadores y un número finito de relatores junto con las identidades de la variedad.

Se dice que una variedad tiene problema de la palabra no resoluble si la variedad contiene un grupo finitamente presentado en la variedad que tiene problema de la palabra no resoluble.

En 1991, M. V. Sapir probó (ver [19]) que, para cualquier número impar $n \geq 665$ y cualquier $p > 1$ coprimo con n, la variedad de grupos A_pB_n tiene problema de la palabra no resoluble.

Un grupo localmente finito es un grupo tal que todos sus subgrupos finitamente generados son finitos. Con esta definición, el problema de Burnside se puede enunciar de la siguiente manera: "¿Existe una variedad de grupos de exponente finito que no es localmente finita?" En 1968 Novikov y Adian dieron respuesta afirmativa a este problema: probaron que para cualquier número impar $n \geq 4381$, la variedad B_n definida por la identidad $x^n = 1$ no es

localmente finita. En 1975, Adian rebajó esta cota a 665. Este problema guarda relación con el problema de la palabra pues la propiedad de que una variedad tenga problema de la palabra no resoluble es más fuerte que la propiedad de que esa variedad sea no-localmente finita. En 1981, Adian construyó un ejemplo de un grupo, presentado por medio de un conjunto infinito recursivo de relaciones, en la variedad B_n que tiene problema de la palabra no resoluble. Unos años después, el propio Adian junto con Makanin plantearon la pregunta de si existe un ejemplo con las mismas propiedades pero dado por una presentación con un número finito de relaciones. Esta cuestión fue resuelta en 1995 por O. Kharlampovich, quien demostró en [14] que si $n = pr$ con $p \geq 3$ primo y r cumpliendo que, o bien tiene un divisor impar mayor o igual que 665 o bien $r \geq 2^{48}$, entonces existe un grupo, finitamente presentado en la variedad B_n, con problema de la palabra no resoluble.

No obstante, el problema de la palabra no sólo se ha planteado para grupos, sino también para álgebras de Lie, estructura para la que se pueden dar algunas definiciones que recuerdan claramente a la teoría de grupos, por ejemplo la definición de álgebra de Lie libre sobre un conjunto X, que es un álgebra de Lie L de modo que existe una aplicación $i : X \to L$ cumpliendo que para cualquier otro álgebra de Lie A y cualquier aplicación $f : X \to A$ existe un único homomorfismo de álgebras de Lie $g : L \to A$ tal que $f = g \circ i$.

Como en el caso de grupos, se puede probar que dado un conjunto X, existe una única álgebra de Lie $L(X)$ libre sobre X. También podemos hablar de la presentación de un álgebra de Lie por medio de generadores y relatores viendo el álgebra como cociente del álgebra de Lie libre sobre A, $L(A)$ (para cierto alfabeto A), por un ideal I de $L(A)$.

Del mismo modo que para grupos podemos hablar de variedades de álgebras de Lie, definiéndolas como clases de álgebras de álgebras de Lie sobre un cuerpo K que satisfacen un determinado sistema de identidades. Por ejemplo, la variedad $\mathcal{U}$ de las álgebras de Lie abelianas satisface la identidad $[x, y] = 0$. Otros ejemplos de variedades de álgebras de Lie son la variedad de las álgebras de Lie resolubles con longitud resoluble menor o igual que l (cuya serie derivada se estaciona en 0 en no más de l pasos) o la variedad $\mathcal{N}_c$ de las álgebras de Lie nilpotentes de clase de nilpotencia menor o igual que c. Como en el caso de grupos, la variedad producto $\mathcal{VW}$ está formada por todas las extensiones de álgebras de Lie en $\mathcal{V}$ por álgebras de Lie en $\mathcal{W}$. La variedad $Z\mathcal{W}$ está formada por las álgebras de Lie cuyo cociente módulo el centro pertenece a $\mathcal{W}$. Se dice que una variedad tiene problema de la palabra resoluble hereditario si la variedad y todas sus subvariedades tienen problema de la palabra resoluble.

En [15], O. Kharlampovich y D. Gildenhuys dieron una condición necesaria que ha de cumplir toda variedad $\mathcal{M}$ de álgebras de Lie sobre un cuerpo K de característica cero con problema de la palabra resoluble hereditario.

La variedad $Z\mathcal{N}_2\mathcal{U}$ está definida por la identidad

$$[[[[x_1, x_2], [x_3, x_4]], [x_5, x_6]], x_7] = 0 \tag{4.1}$$

Para simplificar, denotaremos $[x_1, x_2] = x_1x_2$ y usaremos la notación $x_1x_2 \dots x_n = [\dots[[x_1, x_2], x_3], \dots, x_n]$. Así, la igualdad (4.1) se escribiría:

$$(x_1x_2)(x_3x_4)(x_5x_6)x_7 = 0 \tag{4.2}$$

Esta variedad cumple que el problema de la palabra es no resoluble en toda variedad que la contiene. Sin embargo, el problema de la palabra es resoluble en cualquier subvariedad de la variedad (más pequeña) $\mathcal{N}_2\mathcal{U}$. En 1990, Kharlampovich construyó en $Z\mathcal{N}_2\mathcal{U}$ una colección infinita $\mathcal{W}_\alpha$ de variedades minimales de álgebras de Lie sobre un cuerpo de característica cero con problema de la palabra no resoluble.

Por otra parte, $Z\mathcal{U}\mathcal{N}_2$ es la variedad de álgebras de Lie dada por la identidad

$$(x_1x_2x_3)(x_4x_5x_6)x_7 = 0 \tag{4.3}$$

Introduciendo las identidades:

$$\sum_{\sigma \in A_3} (y_1y_2x_{\sigma(1)})(x_{\sigma(2)}x_{\sigma(3)})z = 0 \tag{4.4}$$

$$\sum_{\sigma \in A_3} y_1y_2(x_{\sigma(1)}x_{\sigma(2)}z_1 \dots z_{2k+1})x_{\sigma(3)} = 0, \qquad k \geq 0 \tag{4.5}$$

Kharlampovich demostró en [6] que la variedad $\mathcal{W}$ definida por las identidades (4.2), (4.3), (4.4) y (4.5) tiene problema de la palabra no resoluble, y todas sus subvariedades propias tienen problema de la palabra resoluble.

El problema de la palabra también se ha estudiado desde un punto de vista más computacional. Entre otros resultados, se conoce que para ciertos grupos, por ejemplo grupos nilpotentes finitamente generados, el problema de la palabra es resoluble mediante algoritmos lineales en tiempo.

También se conocen (ver [20]) soluciones en tiempo polinomial para el problema de la palabra en grupos libres por cíclicos y en grupos de automorfismos de grupos libres, así como soluciones en tiempo polinomial al problema de pertenencia para ciertos tipos de grupos. El problema de pertenencia, también llamado problema de la palabra generalizado, es el siguiente problema matemático: dado un grupo G finitamente presentado, un subgrupo suyo H y una palabra W en los generadores de G, determinar si W define o no un elemento de H. Notar que si H es normal, un algoritmo que resuelva el problema de la pertenencia para H también resuelve el problema de la palabra para G/H.

Un grupo G se dice policíclico si cumple cualquiera de las siguientes propiedades equivalentes:

- Tiene una serie subnormal de longitud finita que empieza en el subgrupo trivial y termina en G tal que todos los factores de la serie son cíclicos, es decir, existen una serie de subgrupos:
$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$
donde cada H_{i+1}/H_i es cíclico.
- Es un grupo resoluble tal que todos los factores de su serie derivada son grupos abelianos finitamente generados.
- Es a la vez un grupo Noetheriano (todo subgrupo es finitamente generado) y un grupo resoluble.

Por ejemplo, todo grupo abeliano finitamente generado es policíclico.

Un grupo G se dice metabeliano si cumple cualquiera de las siguientes propiedades equivalentes:

- G es resoluble de longitud derivada menor o igual que 2.
- Su subgrupo derivado es abeliano.

Se sabe que el problema de pertenencia o problema de la palabra generalizado es resoluble, por ejemplo, para grupos libres finitamente generados, para grupos policíclicos y para grupos metabelianos finitamente generados.

Un grupo G se dice residualmente finito si para todo $1 \neq g \in G$ existe un homomorfismo $\varphi : G \to F$ para cierto grupo finito F cumpliendo que $\varphi(g) \neq 1$. Es decir, G posee una familia de subgrupos normales $\{N_i\}$ tal que $\cap N_i = 1$ y los cocientes G/N_i son finitos.

Un subgrupo H de G se dice separable si para todo $g \in G \backslash H$ existe un homomorfismo $\varphi : G \to F$ para cierto grupo finito F cumpliendo que $\varphi(g) \notin \varphi(H)$. El grupo G se dice de subgrupos separables si todo subgrupo finitamente generado es separable.

Se sabe que todo grupo de subgrupos separables finitamente presentado tiene problema de la palabra generalizado resoluble.

Mihailova demostró que si el problema de la palabra generalizado es resoluble para G_1 y G_2, también lo es para el producto libre $G_1 * G_2$. Por otra parte, también probó que el producto directo de dos grupos libres de rango 2 tiene problema de la palabra generalizado no resoluble, es decir, se puede construir algún subgrupo H finitamente generado tal que no se puede determinar si una determinada palabra en los generadores de G define o no un elemento de H.

Para estudiar la complejidad computacional del problema de la palabra se introduce también el "problema de la palabra comprimido" que se basa en los llamados "straight-line programs" (abreviadamente, SLP).

Si Γ es un conjunto finito de caracteres, es decir, un alfabeto finito, entonces Γ^* denotará el conjunto de todas las palabras en dicho alfabeto, mientras que 1 denotará la palabra vacía. Un SLP $\mathbb{A} = (\Gamma, V, A_n, P)$ sobre un alfabeto Γ consta del alfabeto finito $\Gamma = \{a_1, \ldots, a_m\}$ de caracteres "terminales", un alfabeto finito $V = \{A_1, \ldots, A_n\}$ de caracteres "no-terminales", un no-terminal inicial $A_n \in V$ y un conjunto $P = \{A_i \to W_i\}$ de "reglas de producción". Este último conjunto nos permite reemplazar cada no-terminal A_i por su "producción": una palabra (posiblemente vacía) $W_i \in (\Gamma \cup V)^*$ cumpliendo que si A_j es un no-terminal que aparece en W_i entonces $j < i$. Cuando los subíndices no sean relavantes usaremos A para representar A_n.

Definimos $w(A) = w_A$ como la palabra de Γ^* que se obtiene al ejecutar el SLP $\mathbb{A}$. Es decir, si A_n es el no-terminal inicial, se produce W_n, se reemplazan todos los no-terminales que aparezcan en W_n por sus producciones y se repite este proceso hasta que la palabra resultante pertenezca a Γ^*.

Dado un SLP $\mathbb{A}$, las siguientes tareas se pueden realizar en tiempo polinomial:

- Calcular la longitud de w_A.
- Dado un número natural i menor o igual que la longitud de w_A, calcular la i-ésima posición de w_A.
- Dado otro SLP $\mathbb{B}$, decidir si $w_A = w_B$.

A partir de la noción de SLP se puede enunciar el problema de la palabra comprimido, que es el siguiente problema matemático: Dado un grupo G finitamente generado, Γ un conjunto finito de generadores de G, decidir si un SLP dado $\mathbb{A}$ sobre el alfabeto $\widetilde{\Gamma}$ cumple que la palabra w_A define el neutro en G. (En esta definición, hemos denotado $\widetilde{\Gamma} = \{a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1}\}$ si $\Gamma = \{a_1, \ldots, a_n\}$).

En [8] se estudia el problema de la palabra comprimido para las llamadas "extensiones HNN" y para productos amalgamados.

A partir de los SLP, S. Schleimer prueba en [20] algunos de los resultados mencionados anteriormente, por ejemplo, que el problema de la palabra para grupos libres por cíclicos y para grupos de automorfismos de grupos libres es resoluble en tiempo polinomial.

Aunque se conocen algoritmos polinomiales que resuelven problemas de decisión para ciertas clases de grupos, también hay grupos finitamente presentados cuyo problema de la palabra tiene complejidad arbitrariamente alta. Sin embargo, este tipo de análisis se refiere

solamente al comportamiento de un algoritmo en el peor caso. Se le suele llamar complejidad de peor caso. Algunos algoritmos para resolver el problema de la palabra en grupos finitamente presentados son difíciles de analizar y no se conoce su complejidad de peor caso. Lo que sí se sabe es que ésta es un invariante del grupo y, en particular, no depende de la presentación elegida.

Sin embargo, I. Kapovich, A. Myasnikov, P. Schupp y V. Shpilrain estudiaron en [12] la complejidad de los problemas de decisión en teoría de grupos bajo un enfoque alternativo y complementario: la "complejidad de caso genérico". Los autores partían del hecho experimental de que suele existir algún tipo de algoritmo que resuelve eficientemente el problema en la "mayoría" de los casos. Esto ocurre incluso si la complejidad de peor caso de un problema particular es muy alta o si el problema no es resoluble. Así, muchos problemas de decisión en teoría de grupos pueden ser resueltos rápidamente en numerosos casos. Si bien los autores parten de una intuición basada en experimentos computacionales, en [12] desarrollan la explicación matemática de este fenómeno a partir de la teoría de caminos aleatorios en grafos regulares.

Para estudiar la complejidad de caso genérico, los autores introducen primero la noción de conjunto genérico. Si X es el conjunto de generadores, sea ν una distribución de probabilidad sobre el conjunto X^* de palabras en X o, de forma más general, sea ν una función aditiva arbitraria con valores en $[0,1]$ definida sobre algunos subconjuntos del conjunto X^*. Un subconjunto T de X^* se dice genérico con respecto a ν si $\nu(X^* \backslash T) = 0$. Diremos entonces, por ejemplo, que un algoritmo Ω tiene complejidad de caso genérico polinomial con respecto a ν si Ω se ejecuta en tiempo polinomial para todos los elementos de algún subconjunto T de X^* que es genérico con respecto a ν. Del mismo modo se puede definir la complejidad de caso genérico de cualquier clase de complejidad, no solo para tiempo polinomial.

Los autores también se plantean, además del estudio de caso genérico, el llamado estudio de caso medio. El tipo de situación que contemplan es similar a la que se plantea con el algoritmo simplex de programación lineal. Este algoritmo se usa cientos de veces diariamente, y en la práctica casi siempre funciona de manera eficiente. No obstante, se conocen ejemplos de problemas para los que el algoritmo requiere un tiempo exponencial. Estos ejemplos son, sin embargo, casos muy especiales. Un problema de programación lineal "genérico" o "aleatorio" difícilmente resultará ser un caso tan especial y el algoritmo funcionará eficientemente. Este tipo de observaciones llevan a plantearse el estudio de la complejidad de caso medio de un algoritmo, que se basa en calcular el tiempo esperado de ejecución del algoritmo.

Hay que destacar que la complejidad de caso general y la complejidad de caso medio son diferentes. En primer lugar, para estudiar la complejidad de caso medio, el problema de decisión considerado debe de ser resoluble y se necesita tener un algoritmo total para resol-

verlo. En tal caso, la complejidad de caso medio se centra en el valor esperado del tiempo de ejecución del algoritmo. Por otra parte, en la complejidad de caso genérico, se considera el comportamiento del algoritmo en un conjunto genérico T y se ignora por completo su comportamiento en el complementario de T. Por tanto, se pueden considerar algoritmos parciales que se detienen solamente para argumentos de entrada pertenecientes al conjunto T y el problema considerado en su totalidad puede tener complejidad de peor caso arbitrariamente alta o incluso no ser resoluble.

Los mismos autores de [12] estudian en [13] la complejidad de caso medio utilizando para ello los resultados obtenidos sobre complejidad de caso genérico y concluyendo condiciones suficientes para que el problema de la palabra de un grupo tenga complejidad de caso medio lineal. Estos resultados son aplicables, entre otros, a los grupos de trenzas B_n que definiremos en el próximo capítulo.

Los problemas de decisión en grupos siguen siendo a día de hoy una línea de investigación viva y dinámica que sigue produciendo nuevos resultados. En 2012, Bludov y Glass contruyeron en [1] un grupo totalmente ordenable (es decir, un grupo con un orden total que se preserva por productos tanto a izquierda como a derecha) finitamente presentado con problema de la palabra no resoluble, usando para ello un resultado anterior en el que se construian grupos ordenables a derecha (grupos para los que existe un orden total que se preserva por productos a derecha) finitamente presentados con problema de la palabra no resoluble.

Capítulo 5

Algunas aplicaciones

En este último capítulo, consideraremos algunas aplicaciones de problemas de teoría combinatoria de grupos a otros ámbitos. Si bien la teoría combinatoria de grupos se utiliza en otros campos, nos centraremos en mencionar su influencia en criptografía, concretamente en criptografía de clave pública, para la construcción de criptosistemas y de protocolos de intercambio de claves.

5.1. Protocolos de intercambio de claves.

Comentaremos ahora algunos esquemas de intercambio de claves basados en los llamados "grupos de trenzas", que definiremos mediante una presentación.

Definición 5.1.1 Dado $n \in \mathbb{N}$, llamamos grupo de trenzas de n cuerdas (y lo denotamos B_n) al grupo dado por la siguiente presentación finita:

$$\langle \sigma_1, \ldots, \sigma_{n-1}; \sigma_i\sigma_j = \sigma_j\sigma_i \text{ si } |i-j| \geq 2, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ para } i = 1, \ldots, n-2 \rangle$$

Lo elementos σ_i, $i = 1, \ldots, n-1$, se llaman generadores de Artin.

Nos referimos a los elementos de B_n como "trenzas", haciendo referencia a su interpretación geométrica. Cada elemento de B_n puede verse como una estructura de n cuerdas entre dos barras paralelas horizontales. La cuerda i-ésima es la que parte de la posición i de la barra superior. A cada posición $j \in \{1, \ldots, n\}$ de la barra inferior llega exactamente una de las cuerdas. Esta estructura se suele llamar diagrama de la trenza. Según esta representación, se identifica el i-ésimo generador de Artin σ_i con el diagrama en el que todas las cuerdas unen la posición j de la barra superior con la posición j de la inferior, salvo las cuerdas que empiezan en las posiciones i e $i+1$, que acaban respectivamente, en las posiciones $i+1$ e i, cruzándo la cuerda que sale de la posición $i+1$ por delante de la que sale de la posición i.

En grupos de trenzas, el problema de la palabra es resoluble en tiempo polinomial.

5.1.1. El esquema de Anshel, Anshel y Goldfeld.

El esquema de intercambio de claves propuesto por Anshel, Anshel y Goldfeld utiliza el problema de la conjugación múltiple en grupos de trenzas. En general, dadas dos tuplas $(a_1, \ldots, a_s)$ y $(b_1, \ldots, b_s)$ de elementos de un grupo G, el problema de la conjugación múltiple consiste en encontrar un elemento $x \in G$ tal que $b_i = x^{-1}a_i x \ \forall i = 1, \ldots, s$.

Asumiendo la dificultad del problema de la conjugación múltiple en grupos de trenzas, Anshel, Anshel y Goldfeld proponen su esquema de intercambio de claves, que es el siguiente:

Intercambio de claves AAG

Considerar disponibles en un directorio público un número natural n y dos conjuntos de palabras, $\mathcal{X}_A$ y $\mathcal{X}_B$, en los generadores de Artin del grupo B_n.

$$\mathcal{X}_A = \{S_1, \ldots, S_m\}, \quad \mathcal{X}_B = \{T_1, \ldots, T_l\}$$

Alice y Bob pretenden intercambiar una clave perteneciente a un conjunto K de posibles claves. Disponen para ello de una aplicación $\mathcal{K} : B_n \to K$. Alice y Bob siguen los pasos:

1. Alice elige un elemento secreto a perteneciente al subgrupo de B_n generado por $\mathcal{X}_A$. Después calcula, reescribe y transmite a Bob palabras representando los elementos:
$$a^{-1}T_1 a, \ldots, a^{-1}T_l a$$
Bob elige un elemento secreto b perteneciente al subgrupo de B_n generado por $\mathcal{X}_B$. Después calcula, reescribe y transmite a Alice palabras representando los elementos:
$$b^{-1}S_1 b, \ldots, b^{-1}S_m b$$

2. Usando la expresión de a en función de las palabras de $\mathcal{X}_A$, Alice calcula una palabra representando $b^{-1}ab$.
Análogamente, Bob calcula una palabra representando $a^{-1}ba$.

3. Alice y Bob calculan palabras representantes del elemento conmutador de a y b, $[a, b]$.

4. Alice y Bob pueden usar ahora como clave común $\mathcal{K}([a, b])$.

El argumento que los autores utilizaron para justificar la dificultad de este problema en grupos de trenzas es que el problema del logaritmo discreto en B_n es considerado difícil para $n > 6$ por no conocerse ningún algoritmo polinomial que lo resuelva.

Posteriormente, se propuso un algoritmo para el problema de la conjugación múltiple en grupos de trenzas, muy rápido en ciertos casos particulares. Aunque dicho algoritmo no es polinomial, su existencia basta para considerar este problema "demasiado sencillo" para basar en él la seguridad de herramientas criptográficas.

5.1.2. El esquema de Ko-Lee-Cheon-Han-Khan-Park.

En primer lugar, enunciemos el siguiente problema:

Definición 5.1.2 Se llama problema de Ko-Lee al siguiente problema matemático: dado G un grupo no abeliano, G_1, G_2 dos subgrupos suyos tales que $g_1 g_2 = g_2 g_1 \ \forall g_1 \in G_1, g_2 \in G_2$ y una terna (u, aua^{-1}, bub^{-1}) con $u \in G, a \in G_1, b \in G_2$, calcular el elemento $baua^{-1}b^{-1}$.

El problema de Ko-Lee se aplicará en los grupos de trenzas considerando ciertos subgrupos particulares que definiremos a continuación:

Definición 5.1.3 Sea n un número natural cualquiera y l, r dos números naturales con $l + r = n$. Llamaremos l-subgrupo a izquierda de B_n, y lo denotaremos LB_l, al subgrupo que generan los $l - 1$ primeros generadores de Artin. Llamaremos r-subgrupo a derecha de B_n, y lo denotaremos RB_r, al subgrupo que generan los $r - 1$ últimos generadores de Artin. Es decir,

$$LB_l = \langle \sigma_1, \ldots, \sigma_{l-1} \rangle, \quad RB_r = \langle \sigma_{n-r+1}, \ldots, \sigma_{n-1} \rangle$$

Observación 5.1.4 Por ser $l + r = n$, se tiene que $n - r + 1 = l + 1$, de donde (por las relaciones en B_n) cada elemento de LB_l conmuta con todos los de RB_r, y estamos en las condiciones de considerar el problema de Ko-Lee aplicado a estos subgrupos de B_n.

El principal argumento que los autores utilizaban para justificar la dificultad del problema de Ko-Lee para los subgrupos LB_l, RB_r es la dificultad del "problema de la conjugación generalizado" en grupos de trenzas.

Definición 5.1.5 Se llama problema de la conjugación generalizado al siguiente problema matemático: dado G un grupo no abeliano, H un subgrupo suyo y dos elementos $g_1, g_2 \in G$ que son conjugados por un elemento de H, encontrar $h \in H$ tal que $g_2 = h g_1 h^{-1}$.

Los autores del esquema partían de la suposición de que dicho problema es muy difícil para $G = B_n$, $H = B_m$ con $m \leq n$. Si esto no fuese cierto, tampoco el problema de Ko-Lee sería difícil para $G_1 = LB_l$, $G_2 = RB_r$ ya que, como $LB_l \cong B_l$, recuperar a conocidos u, aua^{-1} es resolver el problema de la conjugación generalizado.

El esquema de intercambio de claves que proponen los autores es el siguiente:

Esquema de intercambio de claves de Ko-Lee-Cheon-Han-Khan-Park

Sean n un número natural y l, r dos números naturales con $l + r = n$. Se hacen públicos estos números, al igual que un elemento $x \in B_n$. Alice y Bob quieren intercambiar una clave secreta para comunicarse. Para ello hacen lo siguiente:

1. Alice elige un elemento secreto $a \in LB_l$ y calcula, reescribe y transmite a Bob una palabra representando el elemento x^a.

   Análogamente, Bob elige un elemento secreto $b \in RB_r$ y calcula, reescribe y transmite a Alice una palabra representando el elemento x^b.

2. Alice y Bob calculan palabras representando el elemento $y := x^{ba} = x^{ab}$.

3. Alice y Bob obtienen, a partir del elemento y, su clave privada.

5.2. Criptosistemas basados en problemas de la palabra y de la conjugación

Se mencionan en esta sección algunos métodos de cifrado cuya seguridad reside en la dificultad de ciertos problemas de decisión en teoría de grupos.

Uno de los problemas matemáticos más conocidos y utilizados para construir criptosistemas de clave pública es el problema de la factorización de enteros. Ya que todavía no se conoce un algoritmo general y eficiente que resuelva este problema, en su dificultad se apoya la seguridad de métodos criptográficos como el RSA. En la actualidad, no sólo se estudian criptosistemas basados en problemas de teoría de números, como el mencionado problema de la factorización de enteros, sino que han surgido también propuestas más recientes que basan su seguridad en otros problemas matemáticos. Es en este punto donde la criptografía de clave pública conecta con la teoría combinatoria de grupos, pues algunos de dichos problemas se enmarcan en este ámbito, como el problema de la palabra u otros problemas de decisión en teoría de grupos.

Comenzaremos esta sección describiendo el criptosistema de clave pública de Ko-Lee, construido a partir del protocolo de intercambio de claves de Ko-Lee-Cheon-Han-Khan-Park.

Criptosistema de clave pública de Ko-Lee

La clave pública es (r, l, x, y, H) donde r, l son números naturales, $x \in B_{l+r}$, $y \in B_{l+r}$ con $y = x^a$ para cierto $a \in LB_l$ que constituye la clave privada; y H es una función hash adecuada definida de B_{r+l} en el espacio de mensajes (supondremos que el espacio de mensajes es $\{0,1\}^k$).
La clave privada es el elemento $a \in LB_l$.
Supongamos que Alice quiere enviar a Bob un mensaje $m \in \{0,1\}^k$.

- Cifrado: Alice elige un elemento secreto $b \in RB_r$, y calcula, reescribe y envía a Bob una palabra representando el elemento x^b. Alice también envía a Bob la cadena de bits que resulta de sumar (módulo 2) m con $H(y^b)$.
- Descifrado: Bob dispone de la clave privada y recibe de Alice un par (c, d) con $c \in B_{r+l}$ y $d \in \{0,1\}^k$. Bob recupera el mensaje m sumando (módulo 2) la secuencia $H(c^a)$ con d.

Es fácil comprobar que, ciertamente, Bob puede recuperar el mensaje de la forma indicada. Si denotamos por $\oplus$ la suma bit a bit (módulo 2), el mensaje que Bob está calculando es precisamente $H(x^{ba}) \oplus m \oplus H(y^b)$. Ahora bien, $x^{ba} = x^{ab}$ pues a, b conmutan ya que $a \in LB_l$, $b \in RB_r$. Por tanto, el mensaje que Bob está calculando es $H(x^{ab}) \oplus m \oplus H(y^b) = H(y^b) \oplus m \oplus H(y^b) = m$, luego recupera el mensaje.

Desde la década de los ochenta se propusieron algunos esquemas criptográficos basados en el problema de la palabra para grupos finitamente presentados; en concreto, describiremos el esquema propuesto por Wagner y Magyarik en los años ochenta que se puede comprobar que es vulnerable a los llamados "ataques de reacción", que consisten en que el adversario obtenga información sobre la clave secreta suponiendo que puede observar la actuación de un receptor legítimo de los mensajes, lo que se modela matemáticamente suponiendo que el adversario tiene acceso a un oráculo que le permite discernir si un mensaje es o no un mensaje cifrado.

También describiremos el esquema de cifrado basado en grupos de Grigorchuk que propusieron posteriormente Garzón y Zalcstein. Este criptosistema se basa en la misma idea general que habían propuesto Wagner y Magyarik para su esquema de cifrado. No obstante, no asume estar trabajando con grupos finitamente presentados pues los grupos de Grigorchuk no lo son en general.

5.2.1. El criptosistema de Wagner y Magyarik

Supongamos G un grupo dado por una presentación finita

$$\langle a_1, \ldots, a_n; R_1, \ldots, R_p \rangle$$

para el cual el problema de la palabra es "muy difícil" (en concreto, supondremos que al menos no se conoce ningún algoritmo polinomial para resolverlo). Y supongamos, además, que existe un subgrupo normal propio N de G tal que G/N es también finitamente presentado y sí tiene problema de la palabra resoluble en tiempo polinomial. En virtud del resultado 1.5.1, si N es el subgrupo normal propio generado por las palabras de $\mathcal{S} = \{S_1(a_1, \ldots, a_n), \ldots, S_q(a_1, \ldots, a_n)\}$, entonces

$$G/N = \langle a_1, \ldots, a_n; R_1, \ldots, R_p, S_1, \ldots, S_q \rangle$$

Por tanto, para especificar G/N basta dar las palabras $S_1, \ldots, S_q$.

Denotando por Σ el alfabeto utilizado para la comunicación, tomemos un conjunto de palabras $\mathcal{W}$ biyectivo con Σ.

$$\mathcal{W} = \{W_\sigma(a_1, \ldots, a_n) | \sigma \in \Sigma\}$$

Las palabras de $\mathcal{W}$ se eligen de tal forma que definan elementos distintos en G/N (y, por tanto también en G).

La clave pública del criptosistema estará formada por la presentación de G

$$G = \langle a_1, \ldots, a_n; R_1, \ldots, R_p \rangle$$

y por el conjunto $\mathcal{W}$; mientras que la clave privada es el cociente G/N (o equivalentemente, el conjunto de palabras $\mathcal{S}$).

El cifrado de un símbolo $\sigma \in \Sigma$ es una palabra $V(a_1, \ldots, a_n)$ equivalente a $W_\sigma(a_1, \ldots, a_n)$ en G. Para descifrar hay que identificar la palabra de $\mathcal{W}$ equivalente a $V(a_1, \ldots, a_n)$ en G. El legítimo receptor del mensaje puede descifrarlo resolviendo el problema de la palabra en G/N ya que si dos palabras son equivalentes en G también lo son en cualquier cociente suyo. Como además las palabras de $\mathcal{W}$ son inequivalentes en G/N, resolviendo el problema de la palabra en G/N se obtiene un único $W_\sigma(a_1, \ldots, a_n)$ equivalente a $V(a_1, \ldots, a_n)$ en G/N. Este W_σ es el descrifrado de $V(a_1, \ldots, a_n)$.

Uno de los aspectos importantes para que este esquema pueda considerarse seguro es que sea robusto frente a un ataque por construcción de una clave privada alternativa. Es decir, que un adversario no pueda construir otro subgrupo normal N' tal que G/N' tenga problema de la palabra resoluble en tiempo polinomial y las palabras de $\mathcal{W}$ sean inequivalentes en G/N',

pues distinguir palabras en G/N' bastaría para descifrar, incluso aunque dicho cociente no sea isomorfo a G/N.

El esquema de Wagner y Magyarik es vulnerable, como ya adelantábamos en la introducción del capítulo, a ataques de reacción. Supongamos, por simplicidad, que el alfabeto Σ es binario. Esto implica que solamente existen dos palabras en $\mathcal{W}$, que representan los bits 0 y 1, respectivamente.

$$\mathcal{W} = \{W_0, W_1\}$$

Supondremos también que las palabras W_0W_1 y W_1W_0 definen elementos distintos en G y en G/N.

El hecho de que el adversario puede observar la actuación de un receptor legítimo de los mensajes se modela suponiendo que el adversario tiene acceso a un oráculo $\mathcal{O}$, que puede verse como una aplicación que a cada palabra $W(a_1, \ldots, a_n)$ le asocia un 1 en caso de que $W(a_1, \ldots, a_n)$ defina el mismo elemento en G que $W_i(a_1, \ldots, a_n)$ para algún $i \in \{0, 1\}$, y un 0 en caso contrario. Es decir, el oráculo permite al adversario distinguir entre textos cifrados y palabras que no son textos cifrados.

También hemos de suponer que existe un conjunto $\mathcal{A}$ de palabras en los símbolos $a_1, \ldots, a_n$ en el que se puede realizar una búsqueda exhaustiva. Además, partiremos de la hipótesis de que el subconjunto de $\mathcal{A}$

$$\overline{\mathcal{S}} = \{A \in \mathcal{A} | A \sim 1 \text{ en G/N}\}$$

permite construir un conjunto $\tilde{\mathcal{S}}$ de palabras que forman un conjunto completo de relatores para G/N (o para otro cociente de G que sirva como clave privada) respecto a los símbolos $a_1, \ldots, a_n$.

El objetivo del adversario será encontrar $\overline{\mathcal{S}}$ por medio del oráculo $\mathcal{O}$. Esto podrá hacerlo mediante una búsqueda exhaustiva en $\mathcal{A}$: para cada $A \in \mathcal{A}$ el adversario hace a lo sumo dos consultas al oráculo para decidir si $A \in \overline{\mathcal{S}}$.

1. AW_0

- si $\mathcal{O}(AW_0) = 0$, claramente $A \notin \overline{\mathcal{S}}$.
- si $\mathcal{O}(AW_0) = 1$, o bien $A \in \overline{\mathcal{S}}$ o bien $AW_0 \sim W_1$ en G/N (y, por tanto, $A \notin \overline{\mathcal{S}}$). Para distinguir estas dos posiblidades, el adversario puede hacer una segunda llamada al oráculo.

2. W_0A

- si $\mathcal{O}(W_0A) = 0$, claramente $A \notin \overline{\mathcal{S}}$.
- si $\mathcal{O}(W_0A) = 1$, o bien $A \in \overline{\mathcal{S}}$ o bien $W_0A \sim W_1$ en G/N (y, por tanto, $A \notin \overline{\mathcal{S}}$). En este último caso, se tendría $W_0AW_0 \sim W_1W_0$; pero, por la llamada anterior, tendría

que ocurrir $AW_0 \sim W_1$, de donde $W_0AW_0 \sim W_0W_1$, lo que contradice que W_0W_1 no equivalente a W_1W_0. Por tanto, no puede ser que $\mathcal{O}(W_0A) = 1$ y $A \notin \overline{\mathcal{S}}$, de donde $\mathcal{O}(W_0A) = 1$ implica $A \in \overline{\mathcal{S}}$.

5.2.2. El criptosistema de Garzón y Zalcstein

Si bien el esquema de Garzón y Zalcstein está inspirado en la construcción propuesta por Wagner y Magyarik, no se trata de un caso particular de ésta, pues ahora los grupos involucrados no son todos finitamente presentados.

Comenzaremos introduciendo los grupos de Grigorchuk, que definiremos como ciertos grupos de permutaciones de caminos infinitos que empiezan en la raíz de un árbol binario completo e infinito. Todos los grupos de Grigorchuk pueden generarse con cuatro elementos, pero no todos son finitamente presentados.

Denotemos por Γ el conjunto de todos los caminos infinitos descendentes desde la raíz del árbol binario infinito completo y sea χ una secuencia infinita cuyas entradas pueden tomar los valores 0,1 ó 2. Definimos a partir de χ una matriz de tres filas e infinitas columnas

$$M_\chi = \begin{pmatrix} U \\ V \\ W \end{pmatrix}$$

Las entradas de M_χ son los símbolos S, I. La columna j de M_χ se define de la siguiente forma:

Si $\chi_j = 0$ entonces

$$\begin{pmatrix} u_j \\ v_j \\ w_j \end{pmatrix} = \begin{pmatrix} S \\ S \\ I \end{pmatrix}$$

Si $\chi_j = 1$ se define

$$\begin{pmatrix} u_j \\ v_j \\ w_j \end{pmatrix} = \begin{pmatrix} S \\ I \\ S \end{pmatrix}$$

Por último, si $\chi_j = 2$ entonces

$$\begin{pmatrix} u_j \\ v_j \\ w_j \end{pmatrix} = \begin{pmatrix} I \\ S \\ S \end{pmatrix}$$

Cada camino $\gamma \in \Gamma$ lo identificaremos con una secuencia binaria $(\gamma_i)_{i\geq 1}$ donde 0 representa un giro a izquierda, y 1 un giro a derecha en el descenso por el árbol. En adelante, dado $x \in \{0, 1\}$ denotaremos $\overline{x} := x + 1 \mod 2$.

El grupo de Grigorchuk asociado a χ (que denotaremos G_χ) es el subgrupo de S_Γ generado por $a, b_\chi, c_\chi, d_\chi$, que son las permutaciones siguientes:

- $a(\gamma) = (a(\gamma)_i)_{i\geq 1}$ con $a(\gamma)_i = \begin{cases} \overline{\gamma_i} & \text{si } i = 1 \\ \gamma_i & \text{en otro caso} \end{cases}$
- $b_\chi(\gamma) = (b_\chi(\gamma)_i)_{i\geq 1}$ con $b_\chi(\gamma)_i = \begin{cases} \gamma_i & \text{si } i \leq k \text{ siendo } \gamma_k \text{ el primer 1 de la secuencia } \gamma \\ \overline{\gamma_i} & \text{si } u_{i-1} = S \text{ e } i > k \\ \gamma_i & \text{si } u_{i-1} = I \text{ e } i > k \end{cases}$
- $c_\chi(\gamma) = (c_\chi(\gamma)_i)_{i\geq 1}$ con $c_\chi(\gamma)_i = \begin{cases} \gamma_i & \text{si } i \leq k \text{ siendo } \gamma_k \text{ el primer 1 de la secuencia } \gamma \\ \overline{\gamma_i} & \text{si } v_{i-1} = S \text{ e } i > k \\ \gamma_i & \text{si } v_{i-1} = I \text{ e } i > k \end{cases}$
- $d_\chi(\gamma) = (d_\chi(\gamma)_i)_{i\geq 1}$ con $d_\chi(\gamma)_i = \begin{cases} \gamma_i & \text{si } i \leq k \text{ siendo } \gamma_k \text{ el primer 1 de la secuencia } \gamma \\ \overline{\gamma_i} & \text{si } w_{i-1} = S \text{ e } i > k \\ \gamma_i & \text{si } w_{i-1} = I \text{ e } i > k \end{cases}$

Si la secuencia χ cumple ciertas propiedades, G_χ no es finitamente presentado y tiene problema de la palabra resoluble en tiempo polinomial. También se sabe, pues los grupos de Grigorchuk han sido muy estudiados, que es posible encontrar una cantidad finita de relaciones $R_1, \ldots, R_m$ satisfechas por $a, b_\chi, c_\chi, d_\chi$ y tales que no se conozca ningún algoritmo polinomial para resolver el problema de la palabra para un grupo con cuatro generadores y dichas relaciones. Una vez fijada una secuencia χ adecuada, Garzón y Zalcstein utilizan un esquema similar al de Wagner y Magyarik tomando las siguientes claves:

La clave pública la forman el grupo $G = \langle a, b, c, d; R_1, \ldots, R_m \rangle$ (con $R_1, \ldots, R_m$ una cantidad finita de relaciones que son satisfechas por $a, b_\chi, c_\chi, d_\chi$ y tales que no se conozca ningún algoritmo polinomial para resolver el problema de la palabra en G) junto con un conjunto de palabras $\mathcal{W}$ que representan elementos distintos de G_χ.

La clave privada es la secuencia χ, a partir de la cual es posible resolver el problema de la palabra en G_χ en tiempo polinomial.

Conclusiones

En esta memoria hemos introducido la teoría combinatoria de grupos haciendo énfasis en los problemas de decisión, en particular el problema de la palabra, a cuya resolución en casos particulares (grupos libres, grupos presentados con un único relator) hemos dedicado parte de los resultados recogidos en los tres primeros capítulos.

En la parte final de la memoria hemos destacado diversos aspectos y resultados más recientes, junto con posibles aplicaciones a criptografía.

Los principales resultados y consideraciones presentados en esta memoria se resumen a continuación:

- El problema de la palabra para grupos presentados con un único relator es resoluble.
- El problema de la palabra no es resoluble en general y, consecuentemente, tampoco lo son otros problemas de decisión en teoría de grupos tales como el problema de la conjugación o el de la pertenencia.
- El problema de la palabra se ha estudiado no sólo en el contexto de grupos sino también en el de variedades.
- El estudio de los problemas de decisión ha evolucionado desde una perspectiva puramente algebraica hasta convertirse en un campo interdisciplinar que aúna teoría combiantoria de grupos, teoría de grafos y teoría de complejidad algorítmica.
- Se ha estudiado la complejidad computacional del problema de la palabra tanto desde un análisis del peor caso como del caso medio o desde un punto de vista más novedoso mediante la complejidad de caso genérico.
- Para extraer conclusiones sobre la complejidad del problema de la palabra, se ha estudiado también el problema de la palabra comprimido y los straight-line programs.
- Se han construido algunos criptosistemas que basan su seguridad en la dificultad del problema de la palabra.

Bibliografía

[1] V. V. Bludov & A. M. W. Glass, *A finitely presented orderable group with insoluble word problem*, Bulletin of the London Mathematical Society, Vol. 44, No. 1, (2012) , págs. 85-98.

[2] Oleg Bogopolski & Andreas Zastrow, *The word problem for some uncountable groups given by countable words*, Topology and its Applications, v. 159, issue 3 (2012), pp. 569-586.

[3] J. L. Britton, *The word problem for groups*, Proceedings of the London Mathematical Society, third series, Vol. 8 (1958), pp. 493-506.

[4] B. Chandler, W. Magnus, *The history of combinatorial group theory: A case study in the history of ideas*, Springer-Verlag, Nueva York, Heidelberg, Berlin, 1982.

[5] Daniel E. Cohen, Klaus Madlener & Friedrich Otto, *Separating the intrinsic complexity and the derivational complexity of the word problem for finitely presented groups*, Math. Log. Quart., No.39 (1993), pp. 143-157.

[6] Benson Farb, *The extrinsic geometry of subgroups and the generalized word problem*, Proc. London Math. Soc. (3) 68 (1994), pp. 577-593.

[7] M.I. González Vasco, *Criptosistemas basados en Teoría de Grupos*, Tesis Doctoral, Universidad de Oviedo, 2003.

[8] Niko Haubold & Markus Lohrey, *Compressed word problems in HNN-extensions and amalgamated products*, Theory Comput. Syst., 49 (2), (2011), pp. 283-305.

[9] Derek F. Holt & Sarah Rees, *Solving the word problem in real time*, Journal of the London Mathematical Society, Vol. 63 (No. 3), (2001), pp. 623-639.

[10] Derek F. Holt, Sarah Rees, Claas E. Röver & Richard M. Thomas, *Groups with context-free co-word problem*, Journal of the London Mathematical Society, Vol. 71, (2005), pp. 643-657.

[11] T. Hungerford, *Algebra*, Springer Verlag, Nueva York, 2003.

[12] Ilya Kapovich, Alexei Myasnikov, Paul Schupp & Vladimir Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, Journal of Algebra, 264, (2003), No. 2, pp. 665-694.

[13] Ilya Kapovich, Alexei Myasnikov, Paul Schupp & Vladimir Shpilrain, *Average-case complexity and decision problems in group theory*, Advances in Mathematics, 190, (2005), No. 2, pp. 343-359.

[14] O. Kharlampovich, *The word problem for the Burnside varieties*, Journal of Algebra, 173, (1995), pp. 613-621.

[15] O. Kharlampovich & D. Gildenhuys, *Varieties of Lie algebras with solvable word problem*, Communications in Algebra, Vol. 21, No.10 (1993), pp. 3571-3609.

[16] Markus Lohrey & Benjamin Steinberg, *An automata theoretic approach to the generalized word problem in graphs of groups*, Proceedings of the American Mathematical Society, Vol. 138, No. 2, (2010), pp. 445-453.

[17] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Dover Publications, Nueva York, 1976.

[18] Klaus Meer & Martin Ziegler, *Real computational universality: The word problem for a class of groups with infinite presentation*, Foundations of Computational Mathematics, Vol. 9, (2009), pp. 599-609.

[19] M. V. Sapir, *On the word problem in periodic group varieties*, International Journal of Algebra and Computations, 1 (1991), No. 1, pp. 115-126.

[20] Saul Schleimer, *Polynomial-time word problems*, Commentarii mathematici helvetici, Vol. 83, N^o 4, (2008) , pp. 741-765.