Grupos de Artin de ángulo recto

Javier Cuesta Cocera
Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Directores del trabajo: Conchita Martínez Pérez y
Marcos Escartín Ferrer
7 de julio de 2022

Preface

Groups are a concept frequently introduced in algebra as a tool for studying the properties of other objects, such as permutations, and for providing resources like the isomorphism theorems. However, if we shift our focus from viewing groups as a means to an end and instead concentrate on their intrinsic properties, we will uncover the relationships between groups. The first chapter will address the notion of free group and how to use it to describe other groups.

In the study of any subject, results are often constrained by the tools available, which can at times prove to be a limitation. Within mathematics, certain proofs rely on results from other fields due to their versatility and effectiveness. We might, for instance, consider the relationship between algebra and topology. In this work, algebra and computational theory are brought together to efficiently address the so-called word problem. In the second chapter, we will seek a representation of groups that enables us to extract properties to solve the word problem using a general algorithm.

We will then proceed with *Bass-Serre* theory, which employs the fundamental group of a graph of groups to connect group actions on trees with group decompositions involving amalgamated free products and HNN extensions, although we will only see a simplified version excluding this last notion. This powerful tool will allow us to prove, in a more straightforward manner than the original *Nielsen-Schreier* argument, that every subgroup of a free group is itself free.

The aforementioned general algorithm for the word problem is primarily theoretical and not particularly practical. Hence, the final chapter is devoted to the search for an efficient algorithm to solve the word problem applied to RAAGs. To this end, we will work with Thue systems to deduce properties that will be applicable to RAAGs through identification via an equivalence relation. Ultimately, this will lead to the development of a linear-time algorithm in terms of input length, utilizing a pushdown automaton.

I would like to express my sincere gratitude to my supervisors, Conchita and Marcos, for their expertise and commitment to the subject. Beyond the outcomes of this work, they have enabled me to grow and learn throughout the entire process.

Prefacio

Los grupos son un concepto que se introducen en álgebra a menudo como instrumento para estudiar las propiedades de otros objetos como por ejemplo las permutaciones y ofrecer herramientas como los teoremas de isomorfía. Si en lugar de pensar en los grupos como un medio, nos centramos en sus propiedades, descubriremos las relaciones entre unos grupos y otros. En el primer capítulo se abordará la noción de grupo libre y cómo se puede usar para describir otros grupos.

Habitualmente en el estudio de una materia los resultados están delimitados por las herramientas disponibles, lo cual en ocasiones puede ser un inconveniente. Dentro de las matemáticas algunas demostraciones se basan en resultados procedentes de otras áreas por su versatilidad y eficacia. Podemos imaginar la relación existente entre el álgebra y la topología. En el presente trabajo se unen el álgebra y la teoría de la computación para resolver eficientemente el llamado problema de la palabra. En el segundo capítulo, buscaremos una representación de los grupos que nos permita extraer propiedades para resolver el problema de la palabra con un algoritmo general.

Proseguiremos con la teoría de *Bass Serre*, que emplea el grupo fundamental de un grafo de grupos para relacionar las acciones de los grupos sobre los árboles con la descomposición de grupos basada en el producto libre amalgamado y las extensiones HNN, aunque solo veremos una versión simplificada sin esta última noción. Se trata de una herramienta poderosa que nos conducirá a probar que todo subgrupo de un grupo libre es libre de una manera directa en comparación al argumento original de *Nielsen–Schreier*.

El algoritmo general mencionado para el problema de la palabra es de carácter teórico al no resultar muy útil en la práctica. Por ello, el último capítulo está dedicado a la búsqueda de un algoritmo eficiente para resolver el problema de la palabra aplicado a RAAGs. Con este objetivo, se trabajará con sistemas de Thue para deducir propiedades que serán aplicables a un RAAG a partir de la identificación de ambos vía una relación de equivalencia. Finalmente se llegará a un algoritmo de coste lineal en la longitud de la entrada utilizando un autómata de pila.

Quiero agradecer en especial a mis tutores, Conchita y Marcos, por sus destrezas y compromiso en la materia porque más allá del presente resultado, me han permitido aprender a lo largo del proceso.

Índice general

Preface III

Prefacio V

1. Grupos libres 1
1.1. Grupos combinatorios . . . 1
1.2. Forma normal . . . 2
1.3. Propiedades de los grupos libres . . . 4

2. Presentaciones de grupos 5
2.1. Grupos finitamente presentados . . . 6
2.2. Problema de la palabra . . . 6

3. Grupos de Artin de ángulo recto (RAAG) 9
3.1. Grupo derivado . . . 9
3.2. Grafos triangulados . . . 10
3.3. Producto libre amalgamado . . . 11
3.4. Palabras reducidas . . . 12
3.5. Acción de grupos sobre árboles . . . 13
3.6. Grafo de grupos . . . 15
3.7. Propiedades de los RAAG . . . 16
3.8. Caracterización de los grafos triangulados . . . 17

4. El problema de la palabra para RAAGs 19
4.1. Sistemas de Thue . . . 19
4.2. Resolución vía autómatas de pila . . . 24

Capítulo 1

Grupos libres

1.1. Grupos combinatorios

Notación 1.1. Si $f : X \to Y$ es una aplicación, la imagen de $x \in X$ por f es $(x)f$ o simplemente xf (las aplicaciones actúan por la derecha).

En primer lugar, vamos a introducir la definición de grupo libre, que utilizaremos en capítulos posteriores. También se probarán algunos resultados de interés.

Definición 1.2. Sea F un grupo, $\emptyset \neq X$ un conjunto y $\sigma : X \to F$ una aplicación. Se dice que (F, σ) es un *grupo libre* en X si para toda aplicación $\alpha : X \to G$, siendo G un grupo, existe un único homomorfismo $\beta : F \to G$ tal que $\alpha = \sigma\beta$, es decir, el siguiente diagrama es conmutativo:

$$\begin{tikzcd} X \arrow[r, "\sigma"] \arrow[dr, "\alpha"'] & F \arrow[d, "\beta"] \\ & G \end{tikzcd}$$

Lema 1.3. *La aplicación σ definida anteriormente es inyectiva.*

Demostración. Sean x_1, $x_2 \in X$ tales que $x_1\sigma = x_2\sigma$ con $x_1 \neq x_2$. Sea G un grupo con al menos dos elementos distintos g_1 y g_2, y $\alpha : X \to G$ tal que $x_1\alpha = g_1$ y $x_2\alpha = g_2$. Se tiene $x_1\sigma\beta = x_2\sigma\beta$, luego $x_1\alpha = x_2\alpha$ y así $g_1 = g_2$, lo que es imposible. □

Dado un conjunto, podemos construir palabras yuxtaponiendo sus elementos. A partir de esta observación, podemos definir una relación de equivalencia entre las palabras.

Definición 1.4. Sea $\emptyset \neq X$ un conjunto. A los elementos de X les llamaremos *letras*. Sea

$$X^{-1} = \{x^{-1} \mid x \in X\}$$

un conjunto disjunto y de la misma cardinalidad que X (simplemente es una notación). Una *palabra* en X se define como una secuencia de elementos de $X \sqcup X^{-1}$ de la forma $w = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$ donde $x_i \in X$, $\varepsilon \in \{-1, +1\}$ y $r \geq 0$. Si $r = 0$, w se llama *palabra vacía* y se denota 1. En este contexto, llamaremos a X *alfabeto*. Si w es una palabra, denotamos su *longitud* como $|w|$.

Definimos la operación yuxtaposición dadas dos palabras $w = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$ y $v = y_1^{\tau_1} \dots y_s^{\tau_s}$ como

$$wv = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r} y_1^{\tau_1} \dots y_s^{\tau_s}$$

Tomamos el convenio $w1 = w = 1w$. Definimos la *palabra inversa* de la palabra w como $w^{-1} = x_r^{-\varepsilon_r} \dots x_1^{-\varepsilon_1}$ donde $(x^{-1})^{-1} = x$, $\forall x \in X$. En particular, $1^{-1} = 1$. Dos palabras son *iguales* si tienen exactamente los mismos elementos en las mismas posiciones.

Denotaremos por W el conjunto de todas las palabras en X. Consideramos $\forall y \in X$ la relación de equivalencia en W generada por

$$1 \sim yy^{-1} \sim y^{-1}y$$

y extendida por yuxtaposición, es decir, si $a \sim b$ entonces $wa \sim wb$ y también $aw \sim bw$ $\forall w \in W$.

Hemos definido ya qué es un grupo libre, pero nos hacemos la siguiente pregunta: dado un conjunto, ¿existe un grupo libre sobre él? Veremos a continuación la trascendencia de este resultado.

Teorema 1.5. *Sea $\emptyset \neq X$ un conjunto. Existe un grupo F y una aplicación $\sigma : X \to F$ tales que (F, σ) es libre en X. Además, $F =< \operatorname{Im}\sigma >$.*

Demostración. La clase de equivalencia de $w \in W$ respecto a la relación anterior se denotará $[w]$. Sea F el conjunto cociente $W/\sim$.

Veamos que F es un grupo. Por definición, si $w \sim w'$ y $v \sim v'$ entonces $wv \sim w'v'$, luego podemos definir en F la operación $[w][v] = [wv]$. Se tiene que $[w][1] = [w] = [1][w]$ y $[w]\left[w^{-1}\right] = \left[ww^{-1}\right] = [1]$, luego contiene el elemento neutro y todo elemento tiene inverso. También se cumple trivialmente la propiedad asociativa ya que $(wv)u = w(vu)$ por yuxtaposición, luego $([w][v])[u] = [(wv)u] = [w(vu)] = [w]([v][u])$. Así, F es un grupo con la operación producto de clases definida con elemento neutro $[1]$ e inverso $\left[w^{-1}\right]$ para todo elemento $[w]$.

Definimos la aplicación

$$\begin{aligned} \sigma : X &\to F \\ x &\mapsto [x] \end{aligned}$$

Veamos que (F, σ) es libre en X. Sea $\alpha : X \to G$ una aplicación con G un grupo. Sea también

$$\begin{aligned} \tilde{\beta} : W &\to G \\ x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r} &\mapsto g_1^{\varepsilon_1} \dots g_r^{\varepsilon_r} \end{aligned}$$

siendo $g_i = x_i\alpha \in G$. Notemos que si $y \in X$ se tiene $(yy^{-1})\tilde{\beta} = y\alpha(y\alpha)^{-1} = 1$, es decir, $\tilde{\beta}$ preserva la relación de equivalencia de donde $w \sim v$ implica $w\tilde{\beta} = v\tilde{\beta}$. Definimos ahora

$$\begin{aligned} \beta : F &\to G \\ [w] &\mapsto w\tilde{\beta} \end{aligned}$$

Así si $v, w \in W$ entonces $[wv]\beta = (wv)\tilde{\beta} = (w)\tilde{\beta}(v)\tilde{\beta} = [w]\beta[v]\beta$. Se deduce que β es un homomorfismo de grupos. Además $x\sigma\beta = [x]\beta = x\tilde{\beta} := x\alpha$, $\forall x \in X$.

Para la unicidad, notemos que si $\gamma : F \to G$ es otro homomorfismo tal que $\sigma\gamma = \alpha$, entonces $\sigma\gamma = \sigma\beta$ y como claramente $F =< \operatorname{Im}\sigma >$ se llega a $\gamma = \beta$. □

1.2. Forma normal

Hasta este momento, queda claro que pueden existir infinitas palabras equivalentes según la relación de equivalencia previamente definida. Nos interesa encontrar de entre todas las equivalentes aquella que sea mínima y represente la clase de equivalencia.

Definición 1.6. Una palabra se dice *reducida* si no tiene ninguna subpalabra de la forma xx^{-1} con $x \in X \cup X^{-1}$. El conjunto de palabras reducidas se denotará R.

Observemos que dada una palabra, podemos eliminar todas las subpalabras xx^{-1} y obtener una única palabra reducida equivalente según la relación definida en 1.4, es decir, toda clase de equivalencia tiene un representante único.

Teorema 1.7. *Sea (F,σ) un grupo libre en X siendo $\sigma : X \to F$ tal que $x \mapsto [x]$. Dada una palabra $w \in W$ existe una única palabra reducida en su clase de equivalencia.*

Demostración. Sea $u \in X \cup X^{-1}$. Definimos la aplicación

$$\begin{aligned} \tilde{u}_u : R &\to R \\ u_1^{\varepsilon_1} \dots u_r^{\varepsilon_r} &\mapsto \begin{cases} u_1^{\varepsilon_1} \dots u_r^{\varepsilon_r} u & \text{si } u \neq u_r^{-\varepsilon_r} \\ u_1^{\varepsilon_1} \dots u_{r-1}^{\varepsilon_{r-1}} & \text{si } u = u_r^{-\varepsilon_r} \end{cases} \end{aligned}$$

$\tilde{u_u}$ es una permutación de R así que si consideramos el grupo simétrico S_R tenemos

$$\begin{aligned} \alpha : X &\to S_R \\ x &\mapsto \tilde{x}_x \end{aligned}$$

Por definición de grupo libre existe un homomorfismo

$$\begin{aligned} \beta : F &\to S_R \\ [x] &\mapsto \tilde{x}_x \end{aligned}$$

tal que $\alpha = \sigma\beta$. Sean $v = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$ y w dos palabras reducidas equivalentes. Como $[v] = [w]$ se tiene $[v]\beta = [w]\beta$. Aplicando la permutación $[v]\beta$ a la palabra vacía $1 \in R$ obtenemos $1\,[v]\beta = 1\left[x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}\right]\beta \underset{\beta \text{ hom}}{=} 1(\widetilde{x_1{}_{x_1^{\varepsilon_1}}^{\varepsilon_1}} \dots \widetilde{x_r{}_{x_r^{\varepsilon_r}}^{\varepsilon_r}}) = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r} = v \in R$. Análogamente $1\,[w]\beta = w$. Así $v = 1\,[v]\beta \underset{[v]\beta=[w]\beta}{=} 1\,[w]\beta = w$. $\square$

El resultado anterior muestra que todo elemento del grupo F puede escribirse de manera única como $[w] = [x_1]^{\varepsilon_1} \cdots [x_r]^{\varepsilon_r}$ siendo w una palabra reducida y $\varepsilon_i \in \{-1,1\}$. Podemos agrupar las clases iguales mediante la operación definida en F y así obtenemos $[w] = [x_1]^{l_1} \cdots [x_r]^{l_r}$ siendo $x_i \in X$, $s \geq 0$, $l_i \neq 0$ y $x_i \neq x_{i+1}$.

Definición 1.8. Una palabra reducida $w = x_1^{l_1} \dots x_s^{l_s} \in R$ con $x_i \in X$, $s \geq 0$, $l_i \neq 0$ y $x_i \neq x_{i+1}$ se dice *forma normal* de $[w]$ en X y por construcción es única.

La forma normal permite representar unívocamente los elementos de un grupo. Esta observación nos da la clave para identificar cuándo un grupo es libre en un subconjunto suyo.

Teorema 1.9. *Sea G un grupo y $X \subseteq G$ tal que todo elemento $g \in G$ está en forma normal en X. Entonces G es libre en X.*

Demostración. Por 1.5 existe un grupo libre F en X y $\sigma : X \to F$ una aplicación que por 1.3 es inyectiva. Tomamos la inclusión $\alpha : X \hookrightarrow G$. Por ser F libre existe un único homomorfismo $\beta : F \to G$ tal que $\alpha = \sigma\beta : X \hookrightarrow G$ es la inclusión. Notemos que si $x \in X$ entonces $x \underset{\alpha \text{ inclusión}}{=} x\alpha = (x)\sigma\beta = (x\sigma)\beta = f\beta$ con $f \in F$ ya que por 1.5, $F =< \operatorname{Im}\sigma >$. Por hipótesis $g = x_1^{l_1} \cdots x_s^{l_s}\ \forall g \in G$ luego $g = x_1^{l_1} \cdots x_s^{l_s} = (f_1\beta)^{l_1} \cdots (f_s\beta)^{l_s} \underset{\beta \text{ hom}}{=} (f_1^{l_1} \cdots f_s^{l_s})\beta$ de donde β es un epimorfismo. Además si $f_1\beta = f_2\beta = g = x_1^{l_1} \cdots x_s^{l_s} \in G$, como esta expresión es única, β también es un monomorfismo. Así, F y G son isomorfos. $\square$

Estamos en disposición de dar una caracterización de los grupos libres vía la forma normal.

Corolario 1.10. ***[Caracterización de los grupos libres]*** *Un grupo F es libre si y solo si existe $X \subset F$ tal que todo elemento $f \in F$ está en forma normal en X.*

1.3. Propiedades de los grupos libres

En la sección anterior hemos visto que todo conjunto tiene un grupo libre asociado. El propósito de esta sección es probar que todo grupo es imagen de algún grupo libre.

Teorema 1.11. *Sean F_1 libre en X_1 y F_2 libre en X_2 tal que $|X_1| = |X_2|$, entonces $F_1 \cong F_2$.*

Demostración. Sea $\alpha : X_1 \to X_2$ una biyección. Se tienen los siguientes diagramas conmutativos

$$\begin{tikzcd} X_1 \arrow[r, "\sigma_1"] \arrow[dr, "\alpha\sigma_2"'] & F_1 \arrow[d, "\beta_1"] \\ & F_2 \end{tikzcd} \qquad \begin{tikzcd} X_2 \arrow[r, "\sigma_2"] \arrow[dr, "\alpha^{-1}\sigma_1"'] & F_2 \arrow[d, "\beta_2"] \\ & F_1 \end{tikzcd}$$

siendo β_i homomorfismos y σ_i inyecciones. Así, $\sigma_1\beta_1\beta_2 = \alpha\sigma_2\beta_2 = \alpha\alpha^{-1}\sigma_1 = \sigma_1$ y llegamos al diagrama conmutativo

$$\begin{tikzcd} X_1 \arrow[r, "\sigma_1"] \arrow[dr, "\sigma_1"'] & F_1 \arrow[d, "\beta_1\beta_2"] \\ & F_1 \end{tikzcd}$$

pero tomando la identidad 1_{F_1} se tendría en mismo diagrama. Por unicidad, $\beta_1\beta_2 = 1_{F_1}$. Análogamente, $\beta_2\beta_1 = 1_{F_2}$, luego β_1 es un isomorfismo y $F_1 \cong F_2$. □

Teorema 1.12. *Sean G un grupo, $X \subseteq G$, F libre en un conjunto Y y $\alpha : Y \to X$ suprayectiva. Entonces α se puede extender a un homomorfismo β de F a G. Si $G =< X >$ entonces β es un epimorfismo. En particular, todo grupo es imagen de un grupo libre.*

Demostración. Por ser F libre en Y se tiene el diagrama conmutativo

$$\begin{tikzcd} Y \arrow[r, "\sigma"] \arrow[dr, "\alpha"'] & F \arrow[d, "\beta"] \\ & G \end{tikzcd}$$

siendo β un homomorfismo de grupos. Si $G =< X >$ está claro que β es un epimorfismo. La última afirmación se deriva de lo anterior. □

Veamos ahora la relación que existe entre los grupos libres y el resto de grupos: Todo grupo se puede describir en base a un grupo libre. Además, veremos que todo homomorfismo de grupos se puede extender a ese grupo libre.

Teorema 1.13. ***[Propiedad proyectiva de los grupos libres]*** *Sean G y H dos grupos y F un grupo libre. Si $\alpha : F \to H$ es un homomorfismo y $\beta : G \to H$ un epimorfismo entonces existe $\gamma : F \to G$ un homomorfismo tal que $\gamma\beta = \alpha$, es decir el siguiente diagrama es conmutativo*

$$\begin{tikzcd} F \arrow[r, "\gamma"] \arrow[dr, "\alpha"'] & G \arrow[d, "\beta"] \\ & H \end{tikzcd}$$

Demostración. Sea F libre en Y e $y \in Y$. Como por hipótesis β es un epimorfismo entonces $y\alpha \in H = \mathrm{Im}\,\beta$ luego existe $x_y \in G$ tal que $x_y\beta = y\alpha$. Por 1.12 podemos extender la aplicación $y \mapsto x_y$ a un homomorfismo $\gamma : F \to G$. Como $y\gamma\beta = x_y\beta = y\alpha$ $\forall y \in Y$ y además $F =< Y >$, se sigue que $\gamma\beta = \alpha$. □

Capítulo 2

Presentaciones de grupos

Queremos describir un grupo a partir de sus generadores y un conjunto de relaciones, es decir, palabras equivalentes al elemento neutro en G.

Definición 2.1. Sea G un grupo. Una *presentación libre* de G es un epimorfismo $\pi : F \to G$ con F un grupo libre. Si $R = \operatorname{Ker}\pi$ entonces $R \trianglelefteq F$ y por el primer teorema de isomorfía $F/R \cong G$. Los elementos de R se llaman *relaciones* de la presentación.

Observación 2.2. Sea $\pi : F \to G$ una presentación libre de G. Si $F =< Y >$ con Y un conjunto de generadores libres, entonces $X = Y\pi$ es un conjunto generador de G al ser π un homomorfismo.

Observación 2.3. Sea $\pi : F \to G$ una presentación libre de G. Sea S un subconjunto de F tal que $S^F = \{fsf^{-1} \mid s \in S, f \in F\} = \operatorname{Ker}\pi$, entonces

$$r \in R \iff \exists s_i \in S, \varepsilon_i \in \{-1,1\} \text{ y } f_i \in F \text{ tales que } r = f_1 s_1^{\varepsilon_1} f_1^{-1} \cdots f_k s_k^{\varepsilon_k} f_k^{-1}$$

En este caso, se dice que r es una consecuencia de S.

Definición 2.4. Una presentación libre π junto con la elección de Y (2.2) y S (2.3) determinan un conjunto de generadores y relaciones de G llamada *presentación* de G y se denota $G =< Y|S >$. Será más habitual dar la presentación de G identificando X con Y, denotado $G =< X|S >$.

A partir de un conjunto Y, vamos a construir un grupo vía una presentación de tal manera que Y es generador del grupo.

Teorema 2.5. *Sea $\emptyset \neq Y$ un conjunto. Por 1.5 existe un grupo libre F sobre Y. Dado $S \subseteq F$ tomamos $R =< S >$. Como $R \trianglelefteq F$, definimos $G = F/R$. Entonces el homomorfismo natural $\pi : F \to G$ es una presentación libre de G y $G =< Y|S >$.*

Veamos que las presentaciones libres nos pueden servir para definir homomorfismos de grupos.

Teorema 2.6. ***[Von Dyck]** Sean G y H grupos con respectivas presentaciones libres $\varepsilon : F \to G$ y $\delta : F \to H$ tales que cada relación de ε lo es de δ. Entonces la aplicación $f\varepsilon \mapsto f\delta$ es un epimorfismo de G a H.*

Demostración. Por hipótesis $\operatorname{Ker}\varepsilon \leq \operatorname{Ker}\delta$. Si $g \in G$ existe $f \in F$ tal que $g = f\varepsilon$ por ser las presentaciones libres suprayectivas. Además, g determina unívocamente $f\delta$. En efecto, si existiera otro $f_1 \in F$ tal que $g = f_1\varepsilon$, como ambos f y f_1 tienen la misma imagen por ε entonces $f = f_1 k$ para un cierto $k \in \operatorname{Ker}\varepsilon \leq \operatorname{Ker}\delta$ luego $f\delta = f_1\delta$. Como δ es un epimorfismo, $f\varepsilon \mapsto f\delta$ es también un epimorfismo de G a H. $\square$

2.1. Grupos finitamente presentados

Definición 2.7. Un grupo se dice *finitamente presentado* si tiene una presentación finita $< X \mid R >$, es decir, si X y R son finitos.

A continuación vamos a ver una propiedad que determina si un grupo es finitamente presentado vía un subgrupo normal y el conjunto cociente.

Teorema 2.8. ***[P.Hall]*** *Sea $N \trianglelefteq G$ con N y G/N grupos finitamente presentados. Entonces G es finitamente presentado.*

Demostración. Sean

$$N =< x_1, \dots, x_n \mid r_1 = \dots = r_m = 1_N >$$
$$G/N =< y_1N, \dots, y_{n'}N \mid s_1 = \dots = s_{m'} = 1_{G/N} >$$

Es evidente que un conjunto de generadores para G es $\{x_1, \dots, x_n, y_1, \dots, y_{n'}\}$. Así $\forall i \in \{1, \dots, m\}$ existen las relaciones ya definidas

$$r_i(x) = 1_N \tag{1}$$

Además $\forall j \in \{1, \cdots, m'\}$ tenemos $s_j(yN) = 1_{G/N}$ luego

$$s_j(yN) = \alpha_j(x) \in N \tag{2}$$

Como $N \trianglelefteq G$ se cumple también $\forall k \in \{1, \dots, n\}$ y $\forall l \in \{1, \dots, n'\}$

$$\begin{aligned} y_l^{-1} x_k y_l &= u_{kl}(x) \\ y_l x_k y_l^{-1} &= v_{kl}(x) \end{aligned} \tag{3}$$

Sea $\overline{G}$ el grupo finitamente presentado generado por el conjunto $\{\overline{x_1}, \dots, \overline{x_n}, \overline{y_1}, \dots, \overline{y_{n'}}\}$ y las relaciones (1), (2), (3) y (4). Por el teorema de Von Dyck, existe un epimorfismo $\alpha : \overline{G} \to G$ tal que $\overline{x_k}\alpha = x_k$ y $\overline{y_l}\alpha = y_l$. Llamemos $K = \operatorname{Ker}\alpha$. Notemos que $\overline{N} =< \overline{x_1}, \dots, \overline{x_n} > \trianglelefteq \overline{G}$ ya que en $\overline{G}$ se cumple $\overline{y_l}^{-1}\overline{x_k}\overline{y_l} = u_{kl}(\overline{x})$ luego la restricción de α a $\overline{N}$ es además inyectiva porque todas las relaciones entre los x_k se deben a $r_i(x) = 1_N$ y así $K \cap \overline{N} = 1$. A partir de α podemos construir un isomorfismo $\overline{G}/\overline{N} \to G/N$ con $\overline{y_l}\overline{N} \mapsto y_lN$ porque todas las relaciones de y_lN se deben a $s_j(yN) = 1_{G/N}$. Utilizando los teoremas de isomorfía $K = K/(K \cap \overline{N}) = K\overline{N}/\overline{N} = 1$ luego $\overline{G} \cong G$ y se deduce que G es finitamente presentado. □

2.2. Problema de la palabra

Introducimos ahora el problema de la palabra, que consiste en determinar si una palabra dada corresponde o no a la identidad en un grupo en base a una presentación suya.

Definición 2.9. Dado el grupo $G =< x_1, \dots, x_n \mid r_1, \dots, r_k >$ se dice que el *problema de la palabra* es *resoluble* para G si existe un algoritmo que diga si $w = 1_G$ para cualquier palabra w en el alfabeto $X = \{x_1, \cdots, x_n\}$.

Definición 2.10. Un grupo G se dice *residualmente finito* si para todo $1 \neq g \in G$ existe $N \trianglelefteq G$ tal que $g \notin N$ y G/N es finito.

Ejemplo 2.11. Un ejemplo de grupo residualmente finito son los grupos libres abelianos:

$$G =< a_1, \cdots, a_n \mid a_i a_j = a_j a_i \ \forall i, j \in \{1, \cdots, n\} >$$

En efecto, si $1 \neq g \in G$ entonces $g = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ para ciertos enteros $\alpha_1, \cdots, \alpha_n$. Como algún α_i es no nulo, podemos elegir un entero $0 \neq \beta$ que no lo divida y definimos $N =< a_i^{\beta} >$. Entonces $g \notin N$ luego $gN \neq 1$ y N es normal ya que todo subgrupo de un grupo abeliano es normal.

Veamos un resultado que utiliza esta propiedad para resolver el problema de la palabra.

Teorema 2.12. *Sea G un grupo residualmente finito y finitamente presentado. Entonces el problema de la palabra es resoluble para G.*

Demostración. Consideremos una presentación finita de G dada por $< X \mid S >$ y $\pi : F \to G$ con $R = Ker\pi = S^F$. Observemos que determinar si $w = 1$ en G es equivalente a determinar si $w \in R$ en F. Sea w una palabra en el conjunto de generadores.

El grupo libre F es finitamente generado luego es contable. Como $R \leq F$, también es contable, luego podemos enumerar sus elementos $r_0 = 1, r_1, \cdots$. Definimos el proceso A como la búsqueda de la palabra en R por orden de los r_i. Si encontramos w entonces $w = 1$ está en G y hemos acabado.

Veamos que el conjunto de todos los posibles subgrupos finitos de G es contable. Sea n cualquiera y consideremos todos los grupos de orden n. Hay un número finito de posibles tablas de multiplicar entre ellos. Como cada tabla de multiplicar determina totalmente el grupo, existe el número finito de grupos de orden n.

Definimos el proceso B como la enumeración de todos los grupos finitos a partir de las tablas multiplicativas. Para cada uno de ellos, por ejemplo H, construimos los homomorfismos $\theta : G \to H$ asignando un elemento de F a cada generador de G. Como cada θ está determinado por las imágenes de una familia generadora, existe un número finito de posibles θ. Para cada homomorfismo θ, calculamos $w\theta$ en F y comprobamos si es la identidad. Si no lo es, entonces $w \neq 1$ luego w no está en G y hemos acabado.

Al ser G residualmente finito, al menos uno de los dos procesos acabará ya que si $w \neq 1$ entonces w no es la identidad en algún cociente finito. Si el proceso A acaba entonces $w = 1 \in G$. Si el proceso B acaba entonces $w \neq 1 \in G$. $\square$

Esta solución del problema de la palabra es de carácter teórico, ya que no es un algoritmo que se pueda utilizar en la práctica. Hay toda una teoría detrás de la búsqueda de algoritmos útiles para resolver el este problema en ciertas familias de grupos. En lo que sigue llamaremos algoritmo general al descrito en este resultado.

Capítulo 3

Grupos de Artin de ángulo recto (RAAG)

Dado el grafo Γ, denotaremos el conjunto de sus vértices por $V(\Gamma)$ y el de ejes $E(\Gamma)$. Dados dos vértices x, $y \in V(\Gamma)$, el eje que los une se denota $e = \overline{xy}$.

Definición 3.1. Un grafo se dice *orientado* si para cada eje hay un vértice inicial, $o(e)$, llamado *origen* y un eje terminal, $f(e)$, llamado *final*.

Definición 3.2. Un grafo Γ se dice *simple* si es finito y no tiene lazos ni ejes dobles.

Introducimos el concepto central de este trabajo, el grupo de Artin de ángulo recto de un grafo simple.

Definición 3.3. Sea Γ un grafo simple. El *grupo de Artin de ángulo recto* de Γ es

$$A_\Gamma =< V(\Gamma) \mid xy = yx, \forall e = \overline{xy} \in E(\Gamma) >$$

Estos grupos también se llaman *grupos parcialmente conmutativos*.

3.1. Grupo derivado

Para los resultados posteriores necesitamos algunos resultados auxiliares sobre el grupo derivado de un grupo.

Definición 3.4. Sea G un grupo. Se define el *grupo derivado* de G como $G' =< [g,h] \mid g,h \in G >$ siendo $[g,h] = g^{-1}h^{-1}gh$.

Corolario 3.5. *Sea G un grupo, entonces $G' \trianglelefteq G$.*

Demostración. Queremos ver que $\forall g \in G$ se cumple $gG'g^{-1} = G'$. Veamos que $gG'g^{-1} \subseteq G'$. Sea $[g_1,g_2] \in G'$ con $g_1,g_2 \in G$. Notemos que $g(g_1^{-1}g_2^{-1}g_1g_2)g^{-1} = (gg_1^{-1}g^{-1})(gg_2^{-1}g^{-1})(gg_1g^{-1})(gg_2g^{-1}) = (gg_1g^{-1})^{-1}(gg_2g^{-1})^{-1}(gg_1g^{-1})(gg_2g^{-1}) \in G'$. El mismo razonamiento implica $g^{-1}G'g \subseteq G'$, es decir, $G' \subseteq gG'g^{-1}$. $\square$

Corolario 3.6. *G es abeliano si y solo si $G' = 1$.*

Demostración. Se deduce de la observación $[g,h] = 1 \iff gh = hg$. $\square$

Teorema 3.7. *Sea $N \trianglelefteq G$. Entonces G/N es abeliano si y solo si $G' \leq N$.*

Demostración.
$\Rightarrow$) Sean $g,h \in G$. Como G/N es abeliano $(gN)(hN) = (hN)(gN)$. Por ser $N \trianglelefteq G$ se tiene $(gN)(hN) = g(Nh)N = g(hN)N = ghN$. Análogamente $(hN)(gN) = hgN$. Por lo tanto $ghN = hgN$ luego $(hg)^{-1}gh = g^{-1}h^{-1}gh \in N$. Así, $G' \leq N$.
$\Leftarrow$) Sean $g,h \in G$. Entonces $g^{-1}h^{-1}gh \in G' \leq N$. Por ser $N \trianglelefteq G$ se cumple $(gN)(hN) = ghN = hgN = (hN)(gN)$ $\forall g,h \in G$. Así G/N es abeliano. $\square$

Observemos que dados dos grupos $H \leq G$, en general $G' \cap H \neq H'$. No obstante, sí que podemos obtener un resultado más débil:

Teorema 3.8. *Sean $H \leq G$ dos grupos. Entonces $H' \leq G' \cap H$.*

Demostración. Como $H \leq G$ entonces $H' \leq G'$. Además $H' \leq H$ luego $H' \leq G' \cap H$. □

3.2. Grafos triangulados

En este capítulo probaremos un resultado importante sobre los grafos triangulados, que son aquellos que no tienen ciclos de más de 3 vértices.

Definición 3.9. Sea Γ un grafo. Un *ciclo* Λ de Γ es un camino simple cerrado $v_1 \cdots v_n v_1$ con $v_i \in V(\Gamma)$. Una *cuerda* de Λ es un eje que conecta dos vértices no adyacentes en Λ.

Definición 3.10. Sea Γ un grafo. Se dice que $S \subseteq \Gamma$ es un subgrafo *inducido* de Γ si $\forall u,\, v \in S$ tales que $\overline{uv} \in E(\Gamma)$ se cumple $\overline{uv} \in E(S)$.

Definición 3.11. Un grafo se dice *triangulado* si no contiene ningún subgrafo inducido isomorfo a un n-ágono para $n \geq 4$. Es equivalente a que todo ciclo de cuatro o más vértices tiene una cuerda.

Definición 3.12. Un grafo Γ se dice *completo* si $\overline{vw} \in E(\Gamma)\ \forall v, w \in V(\Gamma)$.

Necesitaremos un resultado de grafos sobre la descomposición de un grafo triangulado no completo, para lo cual se introduce el concepto desconexión de un grafo.

Definición 3.13. Sea Γ un grafo. Se dice que $\Lambda \subset \Gamma$ *desconecta* Γ si $\Gamma - \Lambda$ es no conexo.

Teorema 3.14. *Sea Γ triangulado no completo. Entonces existen subgrafos propios Γ_1, Γ_2 y Δ tales que $\Gamma = \Gamma_1 \cup \Gamma_2$ y $\Delta = \Gamma_1 \cap \Gamma_2$ con Δ un grafo completo.*

Demostración. Veamos que si Γ es no completo entonces existe un subgrafo que desconecta Γ. Como Γ es no completo, existen $u,\, v \in V(\Gamma)$ tales que $\overline{uv} \notin E(\Gamma)$. Sea S el subgrafo inducido por el conjunto $\{w \in \Gamma \mid w \neq v, \overline{wv} \in E(\Gamma)\}$. Veamos que $\Gamma - S$ es disconexo. Se tiene $u,\, v \in \Gamma - S$. Si fuera conexo, existirían $z_1, \cdots, z_n \in V(\Gamma - S)$ tales que

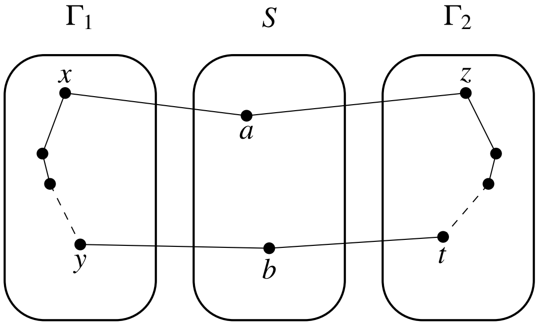
es un subgrafo de $\Gamma - S$, pero entonces $z_n \in S$ lo cual es imposible. Hemos comprobado que existen subgrafos que desconectan Γ. Tomamos $S \subset \Gamma$ minimal que desconecta Γ.

Veamos que si $\Gamma_1 \subset \Gamma - S$ es una componente conexa, entonces $\forall v \in S$ existe algún $x \in \Gamma_1$ tal que $\overline{vx} \in E(\Gamma)$. En efecto, si no fuese así existiría $v \in S$ que no forma un eje con ningún elemento de Γ_1. Veamos que $S - \{v\}$ también desconecta Γ. Notemos que $v \in \Gamma - (S - \{v\})$ y $\Gamma_1 \subseteq \Gamma - (S - \{v\})$. Además, dado $x \in \Gamma_1$, si v y x estuvieran conectados en $\Gamma - (S - \{v\})$ existirían $z_1, \cdots, z_n \in V(\Gamma - (S - \{v\}))$ tales que

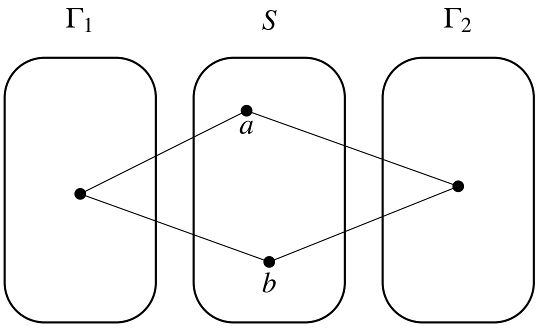
$$\subseteq \Gamma - (S - \{v\}) = (\Gamma - S) \cup \{v\}$$

El grafo de la izquierda (excepto el elemento inicial v) está en $\Gamma - S$. Como $x \in \Gamma_1$ y Γ_1 es una componente conexa de $\Gamma - S$, se deduce que $z_1 \in \Gamma_1$. Hemos encontrado un vértice de Γ_1 que forma un eje con v. Esto es absurdo por la elección de v. Así que v y Γ_1 están en componentes conexas distintas de $\Gamma - (S - \{v\})$, es decir, $\Gamma - (S - \{v\})$ no es conexo y $S - \{v\}$ también desconecta Γ. Esto es absurdo por la elección de S ya que $S - \{v\} \subsetneq S$.

Por último, veamos que S es completo. Dados $a,\, b \in S$, queremos ver que forman un eje. Sean Γ_1, $\Gamma_2 \subset \Gamma - S$ dos componentes conexas (hay al menos dos ya que $\Gamma - S$ no es conexo). Tal y como hemos demostrado antes, existen x, $y \in \Gamma_1$ y también z, $t \in \Gamma_2$ tales que $\overline{xa}, \overline{za}, \overline{yb}, \overline{tb} \in E(\Gamma)$ pudiendo ser $x = y$ y también $z = t$. Como Γ_1, Γ_2 son conexos en $\Gamma - S$, podemos encontrar un camino en Γ_1 entre x e y y lo mismo en Γ_2 entre z y t. Tenemos el siguiente diagrama



Como Γ es triangulado por hipótesis, sabemos que en este ciclo hay alguna cuerda. Pero no puede haber ninguna cuerda que una Γ_1 con Γ_2 al ser dos componentes conexas distintas. Así que si vamos añadiendo cuerdas, cada vez obtenemos ciclos más pequeños, luego o bien hay una cuerda entre a y b, es decir, $\overline{ab} \in E(\Gamma)$, o bien llegamos a un ciclo de la forma



Aquí tiene que haber necesariamente una cuerda que une a y b luego $\overline{ab} \in E(\Gamma)$. □

3.3. Producto libre amalgamado

Nos adentramos en la definición del producto libre amalgamado de dos grupos que utilizaremos en los siguientes resultados. Este junto con las extensiones HNN son esenciales en la llamada *Teoría de Bass Serre*.

Definición 3.15. Sean A y B dos grupos dados por las presentaciones $A =< S_A \mid R_A >$ y $B =< S_B \mid R_B >$. Supongamos que existen subgrupos $C_A \leq A$ y $C_B \leq B$ tales que $C_A \cong C_B$. Llamemos $C := C_A$. Fijamos el isomorfismo

$$\begin{aligned} \phi : C &\to C_B \\ g &\mapsto \phi(g) \end{aligned}$$

Se define el *producto libre amalgamado* de A y B como

$$A \underset{C}{*} B =< S_A, S_B \mid R_A, R_B, g = \phi(g), \forall g \in C >$$

En el caso $C = 1$ se le llama *producto libre* $A * B =< S_A, S_B \mid R_A, R_B >$. En caso de que haya más de dos grupos, $G_1, \cdots, G_n$, se denota el producto libre de todos ellos por $\underset{1 \leq i \leq n}{*} G_i$. El producto libre amalgamado se denota $\underset{C_1, \cdots, C_n}{*} G_i$ siendo cada C_i un subgrupo de G_i de manera que $C_1 \cong \cdots \cong C_n$.

Veamos un ejemplo de producto libre amalgamado de dos grupos.

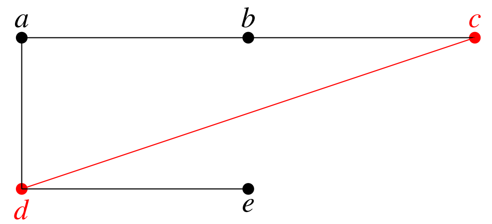
Ejemplo 3.16. Sean $A =< x,z \mid z^5 = 1, x^2 = 1, xz = zx >$ y $B =< y,z \mid z^5 = 1, y^3 = 1, yz = zy >$. Así $A \underset{C}{*} B =< x,y,z \mid z^5 = 1, x^2 = 1, xz = zx, y^3 = 1, zy = yz >$ con $C =< z >$.

Si tenemos una descomposición de un grafo como se explicó en 3.14, entonces dicha descomposición se preserva en los correspondientes RAAGs.

Lema 3.17. *Sea el grafo $\Gamma = \Gamma_1 \cup \Gamma_2$ con $\Delta = \Gamma_1 \cap \Gamma_2$ de forma que $\Gamma_1 - \Delta$ y $\Gamma_2 - \Delta$ no están conectados. Entonces $A_\Gamma = A_{\Gamma_1} \underset{A_\Delta}{*} A_{\Gamma_2}$.*

El hecho de que $\Gamma_1 - \Delta$ y $\Gamma_2 - \Delta$ no estén conectados asegura que no haya relaciones ocultas fuera de A_Δ entre los generadores de A_{Γ_1} y los de A_{Γ_2}. Veamos un ejemplo:

Ejemplo 3.18. Sea Γ el siguiente grafo, Γ_1 el subgrafo inducido por a, b, c y d, Γ_2 el inducido por e, c, d y $\Delta = \Gamma_1 \cap \Gamma_2$.



Entonces $A_\Gamma =< a,b,c,d,e \mid 1 = [a,b] = [b,c] = [c,d] = [a,d] = [d,e] >= A_{\Gamma_1} \underset{A_\Delta}{*} A_{\Gamma_2}$.

Probemos una propiedad intuitiva: el producto libre de dos grupos libres es de nuevo un grupo libre.

Teorema 3.19. *Sean G_1 y G_2 dos grupos libres. Entonces $G_1 * G_2$ es libre.*

Demostración. Por 1.10 un grupo libre no tiene relaciones. Si $G_1 =< S_1 >$ y $G_2 =< S_2 >$ entonces $G_1 * G_2 =< S_1, S_2 >$. Por 1.10 $G_1 * G_2$ es libre. □

3.4. Palabras reducidas

Al igual que se introdujo en el primer capítulo el concepto de palabra reducida de un alfabeto, se introduce ahora el análogo para grupos descompuestos como productos libres amalgamados.

Definición 3.20. Sea $G = A \underset{C}{*} B$. Una palabra $w = x_1 \cdots x_n$ se dice *reducida* en G si se cumple

I. O bien $x_i \in A$ y $x_{i+1} \in B$ $\forall i \in \{1, \cdots, n\}$ o viceversa.

II. Si $n > 1$ entonces $x_i \notin C$ $\forall i \in \{1, \cdots, n\}$.

III. Si $n = 1$ entonces $w \neq 1$.

Un resultado que nos será de gran utilidad más tarde es que una palabra reducida en un grupo no puede ser el elemento neutro. La demostración utiliza un resultado sobre extensiones HNN que no se incluye por su extensión.

Teorema 3.21. *Sea $G = A \underset{C}{*} B$ y $w = x_1 \cdots x_n$ una palabra reducida en G. Entonces $w \neq 1$.*

Demostración. Ver [6]. □

3.5. Acción de grupos sobre árboles

Definición 3.22. Un *árbol* T es un grafo conexo y sin ciclos. Equivalentemente, es un grafo conexo con grupo fundamental trivial.

Definición 3.23. Dado un grupo G y un árbol T decimos que G *actúa sobre* T si existe una aplicación $V(T) \times G \to V(T)$ tal que $\forall v \in V(T)$ y $\forall g, h \in G$

$$\begin{aligned} (vg)h &= v(gh) \\ v1 &= v \end{aligned}$$

y también

$$\overline{vw} \in E(T) \iff \overline{(v)g(w)g} \in E(T)$$

Dados $v \in V(T)$ y $e \in E(T)$, se definen sus *estabilizadores de vértice* y *eje* como

$$\begin{aligned} G_v &= \{g \in G \mid vg = v\} \\ G_e &= \{g \in G \mid eg = e\} \end{aligned}$$

Por convención, asumiremos que la acción es sin inversiones, es decir, que si $e = \overline{vw}$ entonces $G_e \subseteq G_v$, G_w. Esto significa que si un eje queda fijo entonces también quedan fijos los vértices que definen dicho eje. Así $G_e = G_v \cap G_w$.

Por otra parte, dado $g \in G$ y $\forall v \in V(T)$ se cumple $G_{vg} = \{h \in G \mid (vg)h = vg\} = \{h \in G \mid vghg^{-1} = v\} = \{h \in G \mid ghg^{-1} \in G_v\} = g^{-1}G_v g$. Análogamente, $G_{eg} = g^{-1}G_e g$ $\forall e \in E(T)$.

La *órbita* de $v \in V(T)$ se denota $O_v = \{vg \mid g \in G\}$. Se define el *cociente* T/G como el grafo formado por un vértice $\hat{v}$ por cada órbita O_v con $v \in V(T)$ y ejes con vértices $\hat{v}$ y $\hat{w}$ siempre que exista un eje $\overline{vw} \in E(T)$. Aunque T sea árbol, T/G puede no serlo en general.

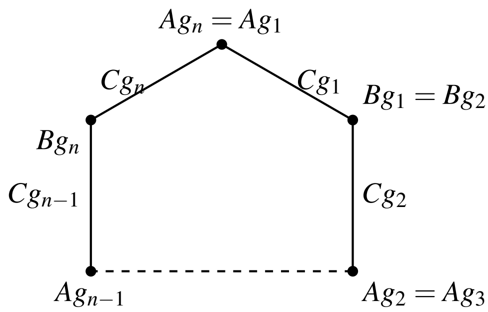
Nos preguntamos si dado un grupo cualquiera G existe un árbol T sobre el que actúe. Veamos que esto es cierto si G es producto libre amalgamado.

Proposicion 3.24. *Si $G = A \underset{C}{*} B$ entonces existe un árbol T sobre el cual actúa G con estabilizadores de vértice de la forma $g^{-1}Ag$ y $g^{-1}Bg$, y estabilizadores de eje de la forma $g^{-1}Cg$ con $g \in G$ de manera que* $T/G = \underset{v}{\bullet}\overset{e}{\rule[0.5ex]{4em}{0.4pt}}\underset{w}{\bullet}$

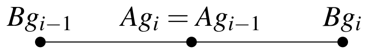
Demostración. Encontremos un grafo T. Consideramos las clases a izquierda de A, B y C en G: $A/G = \{Ag \mid g \in G\}$, $B/G = \{Bg \mid g \in G\}$ y $C/G = \{Cg \mid g \in G\}$. Vamos a formar un grafo T con $V(T) = (A/G) \cup (B/G)$ y $E(T) = C/G$ de forma que los extremos del eje Cg son Ag y Bg. Notemos que G actúa en este grafo por multiplicación a derecha, es decir $(Ag, h) \mapsto Agh$ y $(Bg, h) \mapsto Bgh$.

Por otra parte, sea $e = \overline{vw} \in E(T)$. Veamos que en T hay dos órbitas de vértices, O_v y O_w, con $v = A$ y $w = B$, es decir, los vértices de T son $V(T) = \{vg \mid g \in G\} \cup \{wg \mid g \in G\}$. De la misma manera, los ejes de T son $E(T) = \{eg \mid g \in G\}$ con $e = C$. Como $C \leq A, B$ entonces $g^{-1}Cg \leq g^{-1}Ag$ y $g^{-1}Cg \leq g^{-1}Bg$ luego se cumple $G_e \subseteq G_v$, G_w.

Para ver que T es árbol, veamos que T no tiene ciclos. Supongamos que hay un ciclo en T. Los ejes tienen siempre un extremo en la órbita de A y el otro en la de B.



Podemos suponer que el ciclo es reducido, es decir, que no hay dos vértices iguales. Para cada i impar, $Ag_i = Ag_{i-1}$ implica $g_i = a_{i-1}g_{i-1}$ con $a_{i-1} \in A$. Además, si $a_{i-1} \in A \cap B = C$ tendríamos $Bg_{i-1} = Bg_i$ así que

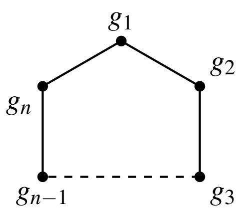


tendríamos dos vértices iguales luego $a_{i-1} \notin C$. Análogamente para los Bg_i con i par. Reiterando tenemos

$$g_n = b_{n-1}a_{n-2}\cdots b_1 g_1$$
$$g_1 = a_n g_n = a_n b_{n-1}\cdots b_1 g_1$$

luego $1 = a_n b_{n-1}\cdots b_1$ con $a_i, b_i \notin C$, $a_i \in A$, $b_i \in B$. Esto contradice el teorema 3.21. $\square$

Sea F un grupo libre sobre el conjunto S. Consideremos un grafo T con un vértice por cada elemento $g \in F$ y un eje entre g_1 y g_2 si $g_2 = ag_1$ con $a \in S$. Entonces F actúa sobre T por multiplicación a derecha. Para ver que T es un árbol se utiliza un argumento similar al empleado en 3.24: si T no fuera un árbol existiría un ciclo del que podemos suponer que todos los vértices son distintos:



tendríamos que

$$g_2 = a_1 g_1$$
$$g_3 = a_2 g_2$$
$$\vdots$$
$$g_n = a_{n-1} g_{n-1}$$
$$g_1 = a_n g_n$$

con $a_i \in S \cup S^{-1}$. Así $g_1 = a_n a_{n-1}\cdots a_2 a_1 g_1$. Si hubiera dos elementos $a_i a_{i-1}$ tales que $a_{i-1} = a_i^{-1}$ tendríamos

$$g_i = a_{i-1} g_{i-1}$$
$$g_{i+1} = a_i g_i = a_{i-1}^{-1} g_i = g_{i-1}$$

y esto es imposible. Por tanto, $1 = a_n \cdots a_1$ pero $a_n \cdots a_1$ es una palabra reducida lo cual también es imposible.

Además, como $hg = h$ implica $g = 1$ se deduce que los estabilizadores de vértice (y por consiguiente los de eje) son triviales. Esta observación implica el siguiente teorema.

Teorema 3.25. *Sea F un grupo libre. Entonces F actúa sobre un árbol con estabilizadores de vértice y de eje triviales.*

3.6. Grafo de grupos

Definición 3.26. Un *grafo de grupos* sobre el grafo Γ consiste en un grupo H_v llamado *grupo de vértice* para cada $v \in V(\Gamma)$ y un grupo H_e llamado *grupo de eje* para cada $e = \overline{vw} \in E(\Gamma)$ junto con monomorfismos $H_e \to H_v$ y $H_e \to H_w$.

Definición 3.27. Sea Γ un grafo. Se dice que $T \subseteq \Gamma$ es un *subárbol maximal* si T es un árbol y para todo $T \subsetneq \Gamma' \subseteq \Gamma$, Γ' no es árbol. Si $T \subseteq \Gamma$ es un subárbol maximal entonces $V(T) = V(\Gamma)$. Todo grafo tiene algún subárbol maximal.

Veamos que al cociente de toda acción se le puede asignar un grafo de grupos, lo que permitirá construir el teorema de estructura a continuación.

Proposicion 3.28. *Sea G un grupo que actúa sobre el árbol T. Entonces existe un grafo de grupos asociado al cociente T/G.*

Demostración. Sea $X \subseteq T/G$ un subárbol maximal. Elegimos un vértice $v \in V(X)$ y lo utilizamos para definir una orientación en T. La hipótesis de que la acción es sin inversiones implica que la acción respeta esta orientación luego tenemos una orientación inducida en T/G. Podemos definir una aplicación $\phi : X \to T$ tal que $X\phi$ es un árbol formado por un subconjunto de representantes de T módulo G. Para ello, elegimos $v\phi \in V(T)$ tal que v representa la órbita de $v\phi$. A partir de v, elegimos $e\phi \in T$ para cada eje e con $o(e) = v$ y así sucesivamente.

Podemos extender ϕ a $\tilde{\phi} : E(T/G) \to E(T)$. Para ello elegimos $e\widetilde{\phi}$ tal que $o(e\widetilde{\phi}) = (o(e))\phi$. Notemos que tanto $f(e\widetilde{\phi})$ como $(f(e))\phi$ se proyectan sobre $f(e)$ en T/G luego dado $e \in E(T/G)$ existe $g_e \in G$ tal que $f(e\widetilde{\phi}) = (f(e))\phi g_e$. Así que existe una aplicación $e \mapsto g_e$ para todo elemento $e \in E(T/G)$. Además si $e \in E(X)$ entonces $f(e\widetilde{\phi}) = (f(e))\phi$ luego $g_e = 1$.

Así para todo $e \in E(T/G)$ se cumple

$$o(e\widetilde{\phi}) = (o(e))\phi$$
$$f(e\widetilde{\phi}) = (f(e))\phi g_e$$

De esta manera se obtiene un grafo de grupos tomando para todo $v \in V(T/G)$ y $e \in E(T/G)$

$$H_v = G_{v\phi}$$
$$H_e = G_{e\widetilde{\phi}}$$

y los monomorfismos $G_{e\widetilde{\phi}} \leq G_{o(e\widetilde{\phi})} = G_{(o(e))\phi}$ y $G_{e\widetilde{\phi}} \leq G_{f(e\widetilde{\phi})} = G_{(f(e))\phi g_e} = g_e^{-1} G_{(f(e))\phi} g_e \overset{g \mapsto g_e g g_e^{-1}}{\to} G_{(f(e))\phi}$ en la definición de grafo de grupos. □

A todo grafo de grupos se le puede asignar un grupo llamado grupo fundamental. La definición de grupo fundamental es compleja y solo la necesitaremos en el caso particular en el que los grupos de los ejes son triviales.

Definición 3.29. Sea Y un grafo de grupos con grupos de eje triviales. Se define su *grupo fundamental* $g(Y)$ como

$$g(Y) = \left(\mathop{*}_{v \in V(Y)} H_v \right) * \pi_1(\hat{Y}, Z)$$

siendo $\hat{Y}$ el grafo subyacente a Y, $Z \subset \hat{Y}$ un árbol maximal y $\pi_1(\hat{Y}, Z)$ el grupo fundamental en sentido habitual de $\hat{Y}$ respecto a Z, es decir, el grupo libre generado por los ejes de $\hat{Y}$ que no están en Z.

Veamos el teorema de estructura, que no incluye demostración completa por falta de espacio.

Teorema 3.30. ***[Teorema de estructura]*** *Sea G un grupo que actúa sobre un árbol T e Y el grafo de grupos asociado al cociente T/G. Entonces G es isomorfo al grupo fundamental de Y.*

Demostración. Ver [9], [10] y [12]. □

Teorema 3.31. *Sea G un grupo que actúa sobre un árbol T con estabilizadores de ejes triviales y estabilizadores de vértice libres. Entonces G es libre.*

Demostración. Sea Y el grafo de grupos asociado al cociente T/G. Sus grupos de eje son de la forma H_e con $e \in E(T)$, luego son triviales. Por el teorema de estructura:

$$G \cong g(Y) = \left(\underset{v \in V(Y)}{*} H_v \right) * \pi_1(\hat{Y}, Z)$$

y tanto los H_v como $\pi_1(\hat{Y}, Z)$ son libres, luego G también lo es. □

Corolario 3.32. *Todo subgrupo de un grupo libre es libre.*

Demostración. Sea F un grupo libre. Por 3.25 F actúa sobre un árbol T con estabilizadores de vértice y de eje triviales. Si $H \leq F$ entonces H actúa sobre T y los estabilizadores son la intersección con H de los de F así que son triviales. Por 3.31 H es libre. □

3.7. Propiedades de los RAAG

Sean $G =< X \mid R >$, $Y \subset X$, R_y las relaciones de R en las que solo aparecen elementos de Y y T el subgrupo de G generado por Y. Podríamos pensar intuitivamente que $T =< Y \mid R_y >$. Sin embargo, en general las relaciones de R_y pueden no ser suficientes para dar una presentación de T y solo podemos afirmar que $T =< Y \mid R_y, S >$ para cierto conjunto S.

A continuación vamos a ver en el caso que nos interesa sí se tiene una presentación sencilla y también que se tiene la igualdad en 3.8.

Teorema 3.33. *Sean $G = A_\Gamma$ y $H = A_{\Gamma_1}$ siendo $\Gamma_1 \subset \Gamma$ un subgrafo inducido. Entonces H es isomorfo al subgrupo de G generado por los vértices Γ_1. Además $H' = G' \cap H$.*

Demostración. Sea la inclusión

$$\begin{aligned} \iota : V(\Gamma_1) &\hookrightarrow G \\ v &\mapsto v \end{aligned}$$

Notemos que está bien definida porque $V(\Gamma_1) \subseteq V(\Gamma)$. Además Γ_1 es un subgrafo inducido luego todo eje de Γ_1 $\underset{v}{\bullet}\!\!-\!\!-\!\!-\!\!\underset{w}{\bullet}$ lo es también de Γ por lo que dado $[v,w] = 1_H$, $[v,w]\iota = (1_H)\iota = 1_G$. Por 2.6 ι se puede extender a un homomorfismo de grupos $\tilde{\iota} : H \mapsto G$.

Sea ahora ϕ la aplicación inducida por

$$\begin{aligned} \phi : \quad V(\Gamma) &\to H \\ v &\mapsto \begin{cases} v & \text{si } v \in V(\Gamma_1) \\ 1 & \text{si } v \notin V(\Gamma_1) \end{cases} \end{aligned}$$

Sea el eje $\underset{v}{\bullet}\!\!-\!\!-\!\!-\!\!\underset{w}{\bullet}$ $\in E(\Gamma)$. Distinguimos 3 casos:

I. $v, w \in \Gamma_1$: $[v\phi, w\phi] = [v,w] = 1$ porque ambos vértices están también conectados en H.

II. $v,w \notin \Gamma_1$: $[v\phi, w\phi] = 1$ porque ningún vértice está en H.

III. $v \in \Gamma_1$, $w \notin \Gamma_1$: $[v\phi, w\phi] = [v,1] = 1$.

Por 2.6 ϕ se puede extender a un homomorfismo de grupos $\tilde{\phi} : G \mapsto H$. Tenemos el siguiente diagrama

$$\begin{array}{ccccc} H & \xrightarrow{\tilde{\imath}} & G & \xrightarrow{\tilde{\phi}} & H \\ v & \longmapsto & v & \longmapsto & v \end{array}$$

Es decir $\tilde{\imath}\tilde{\phi} = 1_H$. Así $\tilde{\imath}$ es inyectiva. Deducimos que la restricción de $\tilde{\imath}$ sobre la imagen, es decir $\tilde{\imath} : H \mapsto H\imath$, es un isomorfismo. Así H es isomorfo al subgrupo de G generado por los vértices de Γ_1. Vamos a denotar por H también a este subgrupo.

Por 3.8 sabemos que $H' \leq G' \cap H$. Veamos el otro contenido. Por ser ϕ un homomorfismo de grupos $G'\phi \leq H'$. Notemos que $G' \cap H = (G' \cap H)\tilde{\imath}\tilde{\phi} = (G' \cap H)\tilde{\phi} \leq (G')\phi \leq H'$ porque $\tilde{\imath}\tilde{\phi} = 1_H$. Hemos probado el otro contenido, luego $H' = G' \cap H$. □

Definición 3.34. Sean $H \leq G$ grupos. Se dice que H es un *retracto* si existe un homomorfismo de grupos $\pi : G \to H$ tal que la composición $H \overset{\iota}{\hookrightarrow} G \overset{\pi}{\mapsto} H$ es la identidad, siendo ι la inclusión.

Corolario 3.35. *Sea A_Γ un RAAG y $\Gamma_1 \subset \Gamma$ un grafo inducido. Entonces A_{Γ_1} es un retracto de A_Γ.*

Para probar que los RAAGs son residualmente finitos, lo que será de interés para el último capítulo, se usa el siguiente resultado que enunciamos sin demostración.

Teorema 3.36. *Sea $G = A \underset{C}{*} B$ tal que $C \leq A, B$ es un retracto de A y B, y además A y B son residualmente finitos. Entonces G es residualmente finito.*

Demostración. Ver el teorema 1 en [1]. □

Teorema 3.37. *Todo RAAG A_Γ es residualmente finito.*

Demostración. Por inducción sobre $|V(\Gamma)|$. Si Γ es completo entonces A_Γ es libre abeliano luego es residualmente finito. Si no lo es, existen grafos Γ_1, Γ_2, $\Delta \subset \Gamma$ tales que $A_\Gamma = A_{\Gamma_1} \underset{A_\Delta}{*} A_{\Gamma_2}$. Por paso de inducción, A_{Γ_1} y A_{Γ_2} son residualmente finitos. Además A_Δ es un retracto de ambos luego A_Γ es residualmente finito. □

3.8. Caracterización de los grafos triangulados

Veamos que un grafo triangulado se caracteriza porque el derivado de su grupo de Artin es libre. Para ello utilizaremos el siguiente resultado.

Lema 3.38. *Sea S una superficie cerrada, conexa, orientable y sin frontera. Si S no es una esfera, entonces su grupo fundamental es*

$$\pi_1(S) = < x_1, \cdots, x_g, y_1, \cdots, y_g \mid [x_1, y_1] \cdots [x_g, y_g] = 1 >$$

para un cierto g llamado género de S que es el número de agujeros de la superficie.

Demostración. Ver teorema 6.3 en [5]. □

Veamos el resultado principal de este capítulo que permite caracterizar los grafos finitos triangulados. La demostración completa requiere argumentos topológicos que no podemos incluir por extensión, por lo que solo daremos la idea principal.

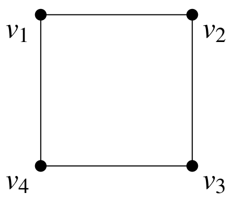
Teorema 3.39. *Sea Γ un grafo finito, entonces Γ es triangulado si y solo si A'_Γ es libre.*

Demostración. (Idea)
$\Rightarrow$) Si Γ es completo entonces A_Γ es abeliano luego $A'_\Gamma = 1$. En otro caso, por 3.14 existen subgrafos propios inducidos Γ_1, Γ_2 y Δ tales que $\Gamma = \Gamma_1 \cup \Gamma_2$ y $\Delta = \Gamma_1 \cap \Gamma_2$ con Δ un grafo completo. Por 3.17 $A_\Gamma = A_{\Gamma_1} \underset{A_\Delta}{*} A_{\Gamma_2}$. Sean $A = A_{\Gamma_1}, B = A_{\Gamma_2}, C = A_\Delta$ y $H = A'_\Gamma$. Por 3.5 $H \trianglelefteq A_\Gamma$. Tenemos $H \leq A_{\Gamma_1} \underset{A_\Delta}{*} A_{\Gamma_2} = G$. Sea T el árbol asociado a la descomposición $A_{\Gamma_1} \underset{A_\Delta}{*} A_{\Gamma_2}$. H actúa sobre T con:

- Estabilizadores de vértice de la forma $H \cap g^{-1} A_{\Gamma_i} g \underset{H \trianglelefteq G}{=} g^{-1}(H \cap A_{\Gamma_i})g$ para $i = 1,2$ y $g \in G$. Por 3.33 $H \cap A_{\Gamma_i} = A'_{\Gamma_i}$ y por paso de inducción podemos suponer que A'_{Γ_i} es libre luego los estabilizadores de vértice son libres.
- Estabilizadores de eje de la forma $H \cap g^{-1} A_\Delta g \underset{H \trianglelefteq G}{=} g^{-1}(H \cap A_\Delta)g$ con $g \in G$. De nuevo por 3.33 $H \cap A_\Delta = A'_\Delta \underset{\Delta \text{ completo}}{=} 1$ luego los estabilizadores de eje son triviales.

Por 3.31 H es libre.

$\Leftarrow$) Razonamos por reducción al absurdo. Supongamos que existe un n-ágono $\Lambda \subset \Gamma$. Por 3.33 podemos poner $A_\Lambda \leq A_\Gamma$. Al ser el derivado un subgrupo $A'_\Lambda \leq A'_\Gamma$. Como Λ es un n-ágono con $n \geq 4$, podemos representarlo como una cadena de n vértices $v_1, \cdots, v_n$ tal que v_i, v_{i+1} son adyacentes. Veamos el caso $n = 4$. En este caso, tenemos $1 = [v_1, v_2] = [v_2, v_3] = [v_3, v_4] = [v_4, v_1]$.

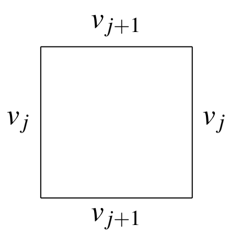


Notemos que

$$v_1[v_2, v_4] = [v_2, v_4]v_1$$
$$v_3[v_2, v_4] = [v_2, v_4]v_3$$

luego $[v_1, v_3][v_2, v_4] = [v_2, v_4][v_1, v_3]$. Hemos llegado a que A'_Λ contiene al subgrupo abeliano de rango 2 generado por $[v_1, v_3]$ y $[v_2, v_4]$ luego no es libre ya que por 3.32, todo subgrupo de un grupo libre es libre. Así A'_Γ tampoco es libre.

Para el caso general veremos solo la idea de la demostración. Si tenemos un n-ágono $\Lambda \subset \Gamma$ de vértices $v_1, \cdots, v_n$, consideramos el 1-esqueleto de un n-cubo I^n y etiquetamos con $v_1, \cdots, v_n$ de manera que v_j sea la etiqueta de los ejes de la forma $i_1 \times \cdots \times \underset{\text{j-ésimo}}{I} \times \cdots \times i_n$ siendo todo $i_k \in I = [0,1]$. Para cada $j \in \{1, \cdots, n\}$ pegamos un cuadrado de la forma:



Notar que cada eje pertenece exactamente a 2 caras luego tenemos una superficie que denotamos Y. Utilizando un argumento topológico se puede demostrar que A'_Λ contiene al grupo fundamental $\pi_1(Y)$ y que Y cumple las hipótesis de 3.38 y no es una esfera luego por 3.38, $\pi_1(Y)$ no es libre. Como G' tiene un subgrupo que no es libre entonces G' no puede ser libre. $\square$

Capítulo 4

El problema de la palabra para RAAGs

4.1. Sistemas de Thue

Hemos visto que los RAAGs son residualmente finitos. Además son obviamente finitamente presentados, así que por 2.12, el problema de la palabra es resoluble para RAAGs por el método general. Sin embargo, dicho algoritmo no es eficiente. Vamos a buscar un algoritmo optimizado.

Denotamos por $W(X)$ el conjunto de palabras en el alfabeto X entendidas como sucesiones de elementos de X pero sin los inversos formales de los elementos de X como se definió en 1.4. Dada una palabra w y una letra a, $|w|_a$ denota el número de veces que aparece a en w.

Definición 4.1. Sea X un alfabeto. Un *sistema Thue* T sobre Γ es $T \subseteq W(X) \times W(X)$, a cuyos elementos llamaremos *reglas*.

Dadas dos palabras u, $v \in W(X)$, decimos que u y v son *congruentes* y se denota $u \longleftrightarrow v$ si existe una regla $(x,y) \in T$ tal que para ciertas palabras w_1 y $w_2 \in W(X)$ o bien $u = w_1xw_2$ y $v = w_1yw_2$, o bien $u = w_1yw_2$ y $v = w_1xw_2$. La clausura reflexiva y transitiva de $\longleftrightarrow$ la denotaremos $\overset{*}{\longleftrightarrow}$. Como claramente la relación $\longleftrightarrow$ es simétrica, entonces la relación $\overset{*}{\longleftrightarrow}$ es de equivalencia. Estos nos permite considerar el conjunto cociente $W(X)/\overset{*}{\longleftrightarrow}$, siendo la clase de la palabra $u \in W(X)$

$$[u] = \{v \in W(X) \mid u \overset{*}{\longleftrightarrow} v\}$$

Vamos a adoptar una notación concreta en función de la longitud de dos palabras congruentes $u \longleftrightarrow v$:

- Si $|u|=|v|$: $u \vdash\!\dashv v$
- Si $|u|\geq|v|$: $u \longmapsto v$
- Si $|u|>|v|$: $u \longrightarrow v$

Análogamente, denotamos las clausuras reflexivas y transitivas de $\vdash\!\dashv$ y $\longmapsto$ por $\overset{*}{\vdash\!\dashv}$ y $\overset{*}{\longmapsto}$. Además, pondremos $u \overset{*}{\longrightarrow} v$ si $u \overset{*}{\longmapsto} v$ y $|u|>|v|$.

Un sistema Thue se dice *preperfecto* si siempre que $u \overset{*}{\longleftrightarrow} v$, existe una palabra $w \in W(X)$ tal que $u \overset{*}{\longmapsto} w \overset{*}{\longleftarrow\!\!\dashv} v$. Un sistema Thue se dice *cuasiperfecto* si siempre que $u \overset{*}{\longleftarrow\!\!\dashv} w \overset{*}{\longmapsto} v$, existe una palabra $z \in W(X)$ tal que $u \overset{*}{\longmapsto} z \overset{*}{\longleftarrow\!\!\dashv} v$. Un sistema Thue se dice *casi confluyente* si siempre que $u \overset{*}{\longleftrightarrow} v$, existen dos palabras x, $y \in W(X)$ tales que $u \overset{*}{\longrightarrow} x \overset{*}{\vdash\!\dashv} y \overset{*}{\longleftarrow} v$.

De las definiciones se extrae que todo sistema casi confluyente es preperfecto (si $u \stackrel{*}{\longrightarrow} x \stackrel{*}{\vdash\!\dashv} y \stackrel{*}{\longleftarrow} v$ entonces también $u \stackrel{*}{\longmapsto} y \stackrel{*}{\longmapsfrom} v$) pero no al revés. Además, se puede determinar si un sistema es casi confluyente pero no si es preperfecto.

Teorema 4.2. *Un sistema Thue es cuasiperfecto si y solo si es preperfecto.*

Demostración. $\Rightarrow$) Sean $u \stackrel{*}{\longleftrightarrow} v$. Supongamos que $u \longleftrightarrow v$. Hay dos casos:

- Si $u \longmapsto v$ tomamos $w = v$ y así $u \longmapsto v = w \longmapsfrom v$.
- Si $u \longmapsfrom v$ tomamos $w = u$ y así $u \longmapsto w = u \longmapsfrom v$.

En el caso general, existe una cadena

$$u \longleftrightarrow w_1 \longleftrightarrow \cdots \longleftrightarrow w_n \longleftrightarrow v$$

y razonamos por inducción sobre n. Por paso de inducción, existe $z \in W(X)$ tal que

$$u \longleftrightarrow w_1 \stackrel{*}{\longmapsto} z \stackrel{*}{\longmapsfrom} v$$

De nuevo existen dos casos:

- Si $u \longrightarrow w_1$ tomamos $w = z$ y así $u \stackrel{*}{\longmapsto} z = w \stackrel{*}{\longmapsfrom} v$.
- Si $u \longmapsfrom w_1$ entonces $u \longmapsfrom w_1 \stackrel{*}{\longmapsto} z$ y por ser cuasiperfecto existe $w \in W(X)$ tal que $u \stackrel{*}{\longmapsto} w \stackrel{*}{\longmapsfrom} z$ luego $u \stackrel{*}{\longmapsto} w \stackrel{*}{\longmapsfrom} v$.

$\Leftarrow$) Si $u \stackrel{*}{\longmapsfrom} w \stackrel{*}{\longmapsto} v$ entonces $u \stackrel{*}{\longleftrightarrow} v$ luego existe $w \in W(X)$ tal que $u \stackrel{*}{\longmapsto} w \stackrel{*}{\longmapsfrom} v$. □

Teorema 4.3. *Sea T un sistema Thue tal que $\forall x, u, v, y \in W(X)$ $x \longleftarrow u \stackrel{*}{\vdash\!\dashv} v \longrightarrow y$ implica que existe $z \in W(X)$ tal que $x \stackrel{*}{\longmapsto} z \stackrel{*}{\longmapsfrom} y$. Entonces T es preperfecto.*

Demostración. Veamos que dicha condición implica que T es cuasiperfecto. Supongamos que se tiene $x \stackrel{*}{\longmapsfrom} w \stackrel{*}{\longmapsto} y$. Queremos probar que existe $z \in W(X)$ con $x \stackrel{*}{\longmapsto} z \stackrel{*}{\longmapsfrom} y$. Razonamos por inducción sobre $|w|$. Si $|w| = 0$ entonces w es la palabra vacía y en este caso es trivial. Así que podemos suponer que se cumple para todas las palabras de longitud menor que $|w|$.

Si tenemos $x \stackrel{*}{\longmapsfrom} w \stackrel{*}{\longmapsto} y$ con $|w| = |x|$, entonces $x \stackrel{*}{\vdash\!\dashv} w \stackrel{*}{\longmapsto} y$ luego $x \stackrel{*}{\longmapsto} y$ y también $y \stackrel{*}{\longmapsto} y$ así que basta tomar $y = z$. Análogo para $|w| = |y|$. Por tanto, podemos suponer que $|x|, |y| < |w|$ lo que implica que en la serie de pasos necesarios para ir de w a x (y de w a y) debe haber alguno estrictamente decreciente. Así tenemos

$$w \stackrel{*}{\vdash\!\dashv} u \longrightarrow x_1 \stackrel{*}{\longmapsto} x$$

$$w \stackrel{*}{\vdash\!\dashv} v \longrightarrow y_1 \stackrel{*}{\longmapsto} y$$

para ciertas palabras u, x_1, v, $y_1 \in W(X)$.

Por tanto $x_1 \longleftarrow u \stackrel{*}{\vdash\!\dashv} v \longrightarrow y_1$ y por hipótesis esta condición implica que existe una palabra $z_1 \in W(X)$ tal que $x_1 \stackrel{*}{\longmapsto} z_1 \stackrel{*}{\longmapsfrom} y_1$. Tenemos $x \stackrel{*}{\longmapsfrom} x_1 \stackrel{*}{\longmapsto} z_1$ con $|x_1| < |w|$ así que por paso de inducción existe $z_2 \in W(X)$ tal que $x \stackrel{*}{\longmapsto} z_2 \stackrel{*}{\longmapsfrom} z_1$. Se deduce que $z_2 \stackrel{*}{\longmapsfrom} y_1 \stackrel{*}{\longmapsto} y$ con $|y_1| < |w|$ así que de nuevo por paso de inducción existe $z \in W(X)$ tal que $z_2 \stackrel{*}{\longmapsto} z \stackrel{*}{\longmapsfrom} y$ luego $x \stackrel{*}{\longmapsto} z \stackrel{*}{\longmapsfrom} y$ como queríamos probar. Así, T es cuasiperfecto y por 4.2 es preperfecto. □

Para el resto del capítulo, vamos a considerar un grafo Γ fijo. Asociado a Γ fijaremos el siguiente sistema Thue sobre el alfabeto $X = V(\Gamma) \cup V(\Gamma)^{-1}$

$$T_0 = \{(aa^{-1}, 1), (a^{-1}a, 1) \mid a \in V(\Gamma)\} \cup \{(cd, dc) \mid \overline{cd} \in E(\Gamma)\}$$

Notemos que $aa^{-1} \longleftrightarrow 1$ y también $a^{-1}a \longleftrightarrow 1$ luego $aa^{-1} \longleftrightarrow a^{-1}a$. Además, las reglas de T_0 expresan una relación parcialmente conmutativa sobre $V(\Gamma)$. De esta manera, $W(X)/\overset{*}{\longleftrightarrow}$ se puede identificar con el grupo A_Γ.

Observación 4.4. Si $E(\Gamma) \neq \emptyset$, el sistema T_0 no es casi confluyente: Sea $\overline{ab} \in E(\Gamma)$, entonces a y b conmutan por construcción de T_0, es decir, $(ab, ba) \in T_0$ y también $(ab)a^{-1} \longleftrightarrow (ba)a^{-1}$ luego $aba^{-1} \longleftrightarrow b$. Supongamos que existen $x, y \in W(X)$ tales que $aba^{-1} \overset{*}{\longrightarrow} x \overset{*}{\longmapsto\!\!\dashv} y \overset{*}{\longleftarrow} b$. Así $|y| < |b| = 1$, luego $y = 1$ así que $b \longleftrightarrow 1$ lo cual es imposible.

Definición 4.5. Sea Γ un grafo. Denotamos por Γ^c al *grafo complementario*, es decir, el grafo con los mismos vértices que Γ pero tal que

$$\overline{ab} \in E(\Gamma^c) \iff \overline{ab} \notin E(\Gamma)$$

Nos gustaría asociar a A_Γ cierto producto cartesiano de grupos libres. Para ello sean los conjuntos $A_1, \cdots, A_n \subseteq X = V(\Gamma) \cup V(\Gamma)^{-1}$ tales que $\bigcup_{1 \leq i \leq n} A_i = X$ y que cumplen las siguientes propiedades:

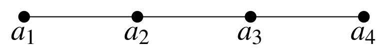
I. Si $a \in A_i$ entonces $a^{-1} \in A_i$.

II. $\overline{ab} \in E(\Gamma^c)$ con $a, b \in V(\Gamma) \iff \exists i$ tal que $a, b \in A_i$.

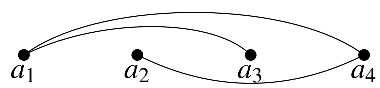
Estas propiedades implican que cada A_i es el conjunto de vértices de un subgrafo completo de Γ^c y sus inversos.

Puede parecer poco intuitivo encontrar dichos conjuntos, por ello veamos un ejemplo.

Ejemplo 4.6. Sea Γ el grafo



el grafo complementario Γ^c es



Podemos tomar los conjuntos $A_1 = \{a_1^{\pm 1}, a_4^{\pm 1}\}$, $A_2 = \{a_1^{\pm 1}, a_3^{\pm 1}\}$ y $A_3 = \{a_2^{\pm 1}, a_4^{\pm 1}\}$.

Sea $B \subset X$. Definimos la proyección de X sobre B como

$$\begin{aligned} \overline{\pi}_B : X &\to B \\ a &\mapsto \begin{cases} a & \text{si } a \in B \\ 1 & \text{si } a \notin B \end{cases} \end{aligned}$$

y el homomorfismo

$$\begin{aligned} \pi_B : W(X) &\to W(B) \\ a_1 \cdots a_r &\mapsto a_1\overline{\pi}_B \cdots a_r\overline{\pi}_B \end{aligned}$$

Por simplicidad, vamos a utilizar la siguiente notación $\overline{\pi}_i := \overline{\pi}_{A_i}$, $\pi_i := \overline{\pi}_i$, $\pi_a = \pi_{\{a\}}$ y $\pi_{a,b} = \pi_{\{a,b\}}$.

Proposicion 4.7. *Sea una palabra cualquiera w y una letra a con $a \in A_i$. Entonces si $w\pi_i = 1$, toda letra de w conmuta con a.*

Demostración. Si $w = a_1 \cdots a_r$ entonces $w\pi_i = a_1\overline{\pi_i} \cdots a_r\overline{\pi_i}$ y la única forma de que sea la palabra vacía es que cada $a_j\overline{\pi_i}$ lo sea (aquí trabajamos con palabras, no elementos del grupo luego aa^{-1} no es la palabra vacía). □

Extendemos la proyección al producto como sigue

$$\begin{aligned} \pi : W(X) &\to W(A_1) \times \cdots \times W(A_n) \\ w &\mapsto (w\pi_1, \cdots, w\pi_n) \end{aligned}$$

Observemos que $u\pi = v\pi$ equivale a

$$\begin{aligned} u\pi_a &= v\pi_a \\ u\pi_{b,c} &= v\pi_{b,c} \end{aligned}$$

para todo $a \in X$ y todos $b, c \in A_i$. Además, se deduce que si $u\pi = v\pi$ necesariamente $|u| = |v|$. Esta observación motiva la siguiente relación entre $W(X)/\overset{*}{\vdash\!\dashv}$ y $W(A_1) \times \cdots \times W(A_n)$:

Lema 4.8. *Dadas u, $v \in W(X)$, $u \overset{*}{\vdash\!\dashv} v$ si y solo si $u\pi = v\pi$.*

Demostración.
$\Rightarrow$) Se sigue de la observación, ya que podemos suponer que $u \vdash\!\dashv v$ luego u y v solo difieren en una subpalabra ab tal que a y b no están en ningún A_i a la vez.
$\Leftarrow$) Hemos visto que la longitud de u y v debe ser igual. Sea $k = |u| = |v|$. Procedemos por inducción sobre k. Si $k = 1$, como las proyecciones coinciden, entonces necesariamente $u = v$. Si $k \geq 2$, escribimos $u = au'$ con $a \in X$ y $u' \in W(X)$. Como $u\pi_a = v\pi_a$, se tiene que $v\pi_a \neq 1$. Sea $v = v'av''$ con $v'\pi_a = 1$. Veamos que $av' \overset{*}{\vdash\!\dashv} v'a$. Si $v' = 1$ está claro. Si no, sea b una letra de la palabra v'. Entonces $v\pi_{a,b}$ comienza por b mientras que $u\pi_{a,b}$ comienza por a. Como por hipótesis $v\pi_{a,b} = u\pi_{a,b}$ se tiene que $\overline{ab} \in E(\Gamma)$. Reiterando este procedimiento para todas las letras de v' se llega a que todas las letras de v' conmutan con a y así $av' \overset{*}{\vdash\!\dashv} v'a$, de donde $v \overset{*}{\vdash\!\dashv} av'v''$.

Veamos que $v'v'' \overset{*}{\vdash\!\dashv} u'$ para concluir que $u \overset{*}{\vdash\!\dashv} v$. Para poder aplicar el paso de inducción, necesitamos comprobar que las proyecciones sobre cualquier vértice y sobre cualquier eje en el grafo complementario coinciden. Sean $c, d \in X$ tales que $\overline{cd} \in E(\Gamma^c)$. Distinguimos dos casos:

- Si $c \neq a \neq d$: $(v'v'')\pi_{c,d} = v\pi_{c,d} = u\pi_{c,d} = u'\pi_{c,d}$.
- Si $a = c$ o bien $a = d$: Digamos $a = c$. Como $v'\pi_a = 1$ entonces $v'\pi_{a,d} = 1$. Así, $a(u')\pi_{a,d} = u\pi_{a,d} = v\pi_{a,d} = (v'av'')\pi_{a,d} = a(v'')\pi_{a,d} = a(v'v'')\pi_{a,d}$, luego $(v'v'')\pi_{a,d} = u'\pi_{a,d}$.

Además, por hipótesis $a(v'v'')\pi_b = v\pi_b = u\pi_b = au'\pi_b$ $\forall b \in X$, es decir, $(v'v'')\pi_b = u'\pi_b$ $\forall b \in X$ luego por paso de inducción se tiene $v'v'' \overset{*}{\vdash\!\dashv} u'$. Se llega a $u = au' \overset{*}{\vdash\!\dashv} av'v'' \overset{*}{\vdash\!\dashv} v'av'' = v$. □

A continuación vamos a introducir la noción de reducción de una tupla de palabras.

Definición 4.9. Sean dos tuplas de palabras $s = (s_1, \cdots, s_n)$, $t = (t_1, \cdots, t_n) \in W(A_1) \times \cdots \times W(A_n)$. Se dice que s se *reduce* a t y se denota $s \longrightarrow t$ si existen $a \in X$ y $k \geq 0$ tales que para todo $i \in \{1, \cdots, n\}$

I. Si $a \notin A_i$ entonces $s_i = t_i$.

II. Si $a \in A_i$ entonces $s_i = u_i aa^{-1} v_i$ y $t_i = u_i v_i$ siendo $u_i, v_i \in W(X)$ con $|u_i|_a = k$.

La clausura de esta relación se denotará $\xrightarrow{*}$. Se dice que s es *irreducible* si no existe dicha tupla t.

Nuestro objetivo es probar que la reducción de tuplas se corresponde con la reducción de palabras en $W(X)$. Observemos que es necesario imponer que las subpalabras de la forma aa^{-1} aparezcan siempre en la misma posición dentro de s_i, ya que de lo contrario podemos encontrarnos inconsistencias. En efecto, consideremos $V(\Gamma) = \{a,b,c\}$ y $E(\Gamma) = \{(a,b)\}$. Tomamos $A_1 = \{a^{\pm 1}, c^{\pm 1}\}$ y $A_2 = \{b^{\pm 1}, c^{\pm 1}\}$. La palabra $w = c^{-1}acbc^{-1}a^{-1}cb^{-1}$ está reducida y no es congruente a la palabra vacía, pero al proyectarla $w\pi_1 = c^{-1}acc^{-1}a^{-1}c \xrightarrow{*} 1$ y $w\pi_2 = c^{-1}cbc^{-1}cb^{-1} \xrightarrow{*} 1$.

Lema 4.10. *Sean u, $v \in W(X)$ y también x, r, $s \in W(A_1) \times \cdots \times W(A_n)$.*

I. *Si $u \longrightarrow v$ entonces $u\pi \longrightarrow v\pi$.*

II. *Si $u\pi \longrightarrow x$ entonces existen v, $w \in W(X)$ tales que $u \overset{*}{\longmapsto\!\dashv} v \longrightarrow w$, y además $x = w\pi$.*

III. *Si $r \longleftarrow u\pi \longrightarrow s$ entonces o bien $r = s$ o bien $r \longrightarrow t \longleftarrow s$ para cierto $t \in W(A_1) \times \cdots \times W(A_n)$.*

Demostración.

I. Sea $u \longrightarrow v$. Por la definición 4.9, se tiene $u = xaa^{-1}y$ y $v = xy$ para ciertos $a \in X$, $x, y \in W(X)$. Sea $k = |x|_a$. Si $a \notin A_i$ entonces $a^{-1} \notin A_i$ y $u\pi_i = (xy)\pi_i = v\pi_i$. Si $a \in A_i$ también $a^{-1} \in A_i$ entonces $u\pi_i = x\pi_i aa^{-1}(y)\pi_i$ y también $v\pi_i = (x)\pi_i(y)\pi_i$. Además, como $a \in A_i$ se tiene $|x\pi_i|_a = |x|_a = k$. Así $u\pi \longrightarrow v\pi$.

II. Sea $u\pi \longrightarrow x$. Por la definición 4.9 existen ciertos $a \in V(\Gamma)$ y $k \in \mathbb{N}$ tal que para todo $i \in \{1, \cdots, n\}$

$$u\pi_i = \begin{cases} \alpha_i aa^{-1}\beta_i & \text{si } a \in A_i \\ x_i & \text{si } a \notin A_i \end{cases}$$

siendo $x_i = \alpha_i\beta_i$ con $\alpha_i, \beta_i \in W(X)$ y $|\alpha_i|_a = k$. Como la letra a está en al menos un conjunto de entre $A_1, \cdots, A_n$, asumamos sin pérdida de generalidad que $a \in A_1$. Así $u\pi_1 = \alpha_1 aa^{-1}\beta_1$ luego $u = rasa^{-1}t$ con $r\pi_1 = \alpha_1$, $s\pi_1 = 1$, $t\pi_1 = \beta_1$ y $|r|_a = k$. Notemos que $|s|_a = |s|_{a^{-1}} = 0$ ya que $s\pi_1 = 1$.

Consideremos un conjunto cualquiera A_i tal que $a \in A_i$. Veamos que $\alpha_i = r\pi_i$, $\beta_i = t\pi_i$ y $s\pi_i = 1$. Como $u = rasa^{-1}t$ y $u\pi_i = \alpha_i aa^{-1}\beta_i$, entonces $r\pi_i a(s)\pi_i a^{-1}(t)\pi_i = \alpha_i aa^{-1}\beta_i$ siendo $|r\pi_i|_a = |r|_a = k = |\alpha_i|_a$ luego $r\pi_i = \alpha_i$. Por otro lado, $s\pi_i a^{-1}(t)\pi_i = a^{-1}\beta_i$. Como $|s|_{a^{-1}} = 0$, $s\pi_i$ no puede empezar por a^{-1}, así que $s\pi_i = 1$ y $t\pi_i = \beta_i$.

Sean $v = rsaa^{-1}t$ y $w = rst$. Si $a \notin A_i$ entonces $w\pi_i = u\pi_i = x_i$. Si $a \in A_i$ entonces $x_i = \alpha_i\beta_i = (r)\pi_i(t)\pi_i = (r)\pi_i(s)\pi_i(t)\pi_i = w\pi_i$. Así, $x = w\pi$. Hemos visto que si $a \in A_i$ se tiene $s\pi_i = 1$ luego por 4.7 todas las letras de s conmutan con a y así $u = rasa^{-1}t \overset{*}{\longmapsto\!\dashv} rsaa^{-1}t = v \longrightarrow w$.

III. Sea $r \longleftarrow u\pi \longrightarrow s$ y llamemos $u_i = u\pi_i$. Por la definición 4.9, existen $a, b \in X$ y $m, n \geq 0$ tales que para todo $i \in \{1, \cdots, n\}$

$$u_i = \begin{cases} \alpha_i aa^{-1}\beta_i & \text{si } a \in A_i \\ r_i & \text{si } a \notin A_i \end{cases} \qquad u_i = \begin{cases} \gamma_i bb^{-1}\delta_i & \text{si } b \in A_i \\ s_i & \text{si } b \notin A_i \end{cases}$$

siendo $r_i = \alpha_i\beta_i$, $|\alpha_i|_a = m$, $s_i = \gamma_i\delta_i$ y $|\gamma_i|_b = n$. Veamos los dos casos posibles:

- `Caso 1`: Supongamos que $\overline{a^{\pm 1}b^{\pm 1}} \in E(\Gamma)$ de tal manera que para cada $k \in \{1, \cdots, n\}$, A_k no contiene simultáneamente a y b. Definimos la tupla t tomando

$$t_k = \begin{cases} s_k & \text{si } b \in A_k \\ r_k & \text{si } a \in A_k \\ u_k & \text{si } a, b \notin A_k \end{cases}$$

La reducción de r a t se consigue de la siguiente manera: si $b \notin A_k$ entonces $r_k = t_k$ y si $b \in A_k$ entonces $r_k = u_k$ y $t_k = s_k$ luego $r_k = \gamma_k bb^{-1}\delta_k$, $t_k = \gamma_k\delta_k$, $|\gamma_k|_b = n$. Análogamente s se reduce a t. Así $r \longrightarrow t \longleftarrow s$.

- `Caso 2`: Supongamos que $\overline{a^{\pm 1}b^{\pm 1}} \in E(\Gamma^c)$ de tal manera que alguno de los A_i, digamos A_1, contiene $a^{\pm 1}$ y $b^{\pm 1}$. Como veíamos en (II), de $u\pi \longrightarrow r$ se obtiene que si $a \in A_i$, entonces $u = x_1 a z_1 a^{-1} y_1$ siendo $r = (x_1 z_1 y_1)\pi$ y $z_1\pi_i = 1$. Análogamente, como $u\pi \longrightarrow s$ si $b \in A_i$ se tiene $u = x_2 b z_2 b^{-1} y_2$, $s = (x_2 z_2 y_2)\pi$ y $z_2\pi_i = 1$. Como a y b están ambos en A_1, ni z_1 ni z_2 contienen a, a^{-1}, b ni b^{-1} ya que entonces sería $z_i\pi_1 \neq 1$. Asumimos sin pérdida de generalidad que $|x_2| \geq |x_1|$. Distinguimos dos casos:
  - Si $|x_2| = |x_1|$, como a^{-1} no está en z_1 ni z_2, se tiene que $x_1 = x_2$, $a = b$, $z_1 = z_2$ y $y_1 = y_2$, luego $r = s$.
  - Si $|x_2| > |x_1|$ entonces $|x_2| \geq |x_1 a z_1|$ porque en caso contrario b^{-1} estaría en z_1. Veamos por separado los casos. Si $|x_2| = |x_1 a z_1|$ entonces $x_2 = x_1 a z_1$, $b = a^{-1}$ y $y_1 = z_2 b^{-1} y_2 = z_2 a y_2$ luego $x_1 z_1 y_1 = x_1 z_1 z_2 a y_2 \overset{*}{\longmapsto\!\!\!\dashv} x_1 a z_1 z_2 y_2 = x_2 z_2 y_2$ y aplicando π se deduce $r = s$. Si $|x_2| > |x_1 a z_1|$, entonces $x_2 = x_1 a z_1 a^{-1} w$ para cierta $w \in W(X)$ y $y_1 = w b z_2 b^{-1} y_2$. Sea $v = x_1 z_1 w z_2 y_2$, se tiene $x_1 z_1 y_1 = x_1 z_1 w b z_2 b^{-1} y_2 \overset{*}{\longmapsto\!\!\!\dashv} x_1 z_1 w z_2 b b^{-1} y_2 \longrightarrow v$ y además $x_2 z_2 y_2 = x_1 a z_1 a^{-1} w z_2 y_2 \overset{*}{\longmapsto\!\!\!\dashv} x_1 z_1 a\bar{a} w z_2 y_2 \longrightarrow v$ luego $r \longrightarrow v\pi \longleftarrow s$.

□

Los resultados anteriores nos conducen a inducir una propiedad importante sobre el sistema T_0 que se utilizará en la construcción del algoritmo final.

Teorema 4.11. *El sistema T_0 es preperfecto.*

Demostración. Sea $x \longleftarrow u \overset{*}{\longmapsto\!\!\!\dashv} v \longrightarrow y$. Por 4.8 y 4.10(I) se tiene $x\pi \longleftarrow u\pi = v\pi \longrightarrow y\pi$. Ahora por 4.10(III), o bien $x\pi = y\pi$ o bien $x\pi \longrightarrow t \longleftarrow y\pi$ para cierta tupla t. Si $x\pi = y\pi$ entonces $x \overset{*}{\longmapsto\!\!\!\dashv} y$ y tomando $z = x$ se tiene $x \overset{*}{\longmapsto} z \overset{*}{\longleftarrow\!\!\!\mid} y$ luego por 4.3 T_0 es preperfecto. Por otro lado, si $x\pi \longrightarrow t \longleftarrow y\pi$, en particular $x\pi \longrightarrow t$ y por 4.10(II) se tiene $t = z\pi$ para alguna $z \in W(X)$ tal que $x \overset{*}{\longmapsto} z$. Análogamente, como $y\pi \longrightarrow t$ se tiene que $t = z'\pi$ para cierta $z' \in W(X)$ tal que $y \overset{*}{\longmapsto} z'$. Como $z\pi = z'\pi$, entonces $z \overset{*}{\longmapsto\!\!\!\dashv} z'$ luego $x \overset{*}{\longmapsto} z \overset{*}{\longmapsto\!\!\!\dashv} z' \overset{*}{\longleftarrow\!\!\!\mid} y$. Así, $x \overset{*}{\longmapsto} z \overset{*}{\longleftarrow\!\!\!\mid} y$. Por 4.3 T_0 es preperfecto. □

4.2. Resolución vía autómatas de pila

El problema de la palabra, es decir, encontrar las palabras que se aceptan en un determinado lenguaje se resuelve en teoría de la computación mediante lo que se llama un autómata de pila. Recordemos estos conceptos.

Definición 4.12. Sea la palabra $w = x_1 \cdots x_n \in W(X)$. Una *pila* es una estructura de datos que permite añadir (apilar) y eliminar (desapilar) una a una las letras de w. La *cima* de la pila es la última palabra apilada. Desapilar una letra equivale a eliminar la letra de la cima. El orden de apilado es de izquierda a derecha.

Un *autómata de pila* es una tupla $M = (S, X, Y, \delta, s, Z, F)$ donde

- S es un conjunto finito de estados.
- X e Y son alfabetos para las letras de entrada y para la pila respectivamente.

- $\delta : S \times X \times Y \longrightarrow \mathscr{P}(S \times W(Y))$ es la función de transición que, dado un estado actual, una letra de entrada y teniendo en cuenta la letra en la cima de la pila, genera todos los posibles estados a los que se puede ir. Cada uno de estos estados tiene asociado un estado de la pila.
- $s \in S$ es el estado inicial del autómata.
- $Z \in \Gamma$ es el símbolo especial que representa el inicio de la pila.
- $F \subseteq S$ es el conjunto de estados de aceptación, es decir, si el último estado por el que pasamos al consumir las letras de una palabra pertenece a F entonces la palabra pertenece al lenguaje. En caso de no acabar en un estado de F, entonces la palabra no pertenece al lenguaje.

Necesitaremos la siguiente generalización de 4.10(II) a la clausura.

Proposicion 4.13. *Si $u\pi \xrightarrow{*} x$ entonces existen v, $w \in W(X)$ tales que $u \overset{*}{\vdash\!\dashv} v \xrightarrow{*} w$, y además $x = w\pi$.*

Demostración. Notemos que $u\pi \xrightarrow{*} x$ implica $u\pi \longrightarrow x_1 \longrightarrow \cdots \longrightarrow x_l = x$. Razonamos por inducción sobre l. Si $l = 1$, se tiene por 4.10(II). Supongamos que el resultado se cumple hasta $l-1$. Por paso de inducción, existen $v, w_1 \in W(X)$ tales que $x_{l-1} = w_1\pi$ y $u \overset{*}{\vdash\!\dashv} v \xrightarrow{*} w_1$. Así $x_{l-1} = w_1\pi \longrightarrow x$ luego por 4.10(II) existen $v_1, w \in W(X)$ tales que $x = w\pi$ y $w_1 \overset{*}{\vdash\!\dashv} v_1 \xrightarrow{*} w$. Por tanto, $u \overset{*}{\vdash\!\dashv} v \xrightarrow{*} w_1 \overset{*}{\vdash\!\dashv} v_1 \xrightarrow{*} w$ de donde $u \overset{*}{\vdash\!\dashv} v \xrightarrow{*} w$. □

Finalmente, probaremos que el problema de la palabra para los RAAGs se puede resolver en tiempo lineal, lo cual mejora mucho el algoritmo general. Cabe recordar la relación ya mencionada entre T_0 y A_Γ.

Teorema 4.14. *Dado el grafo Γ, existen algoritmos para encontrar la palabra reducida de una dada y para resolver el problema de la palabra ambos en tiempo lineal para A_Γ.*

Demostración. El algoritmo para encontrar la palabra reducida de una dada w consta de dos fases: reducción y reconstrucción.

Consideremos n pilas distintas $P_1, \cdots, P_n$, una para cada conjunto $A_1, \cdots, A_n$. Inicialmente todas las pilas están vacías. Supongamos que leemos la letra a de la palabra de entrada w. Las letras se leen de izquierda a derecha. Para todo i tal que $a \in A_i$, hay dos posibilidades:

- Si a^{-1} está en la cima de P_i, desapilamos dicha letra de P_i, es decir, la eliminamos.
- Si a^{-1} no está en la cima de P_i, apilamos a en P_i.

Tras realizar este proceso para todos los ies tales que $a \in A_i$, pasamos a la siguiente letra. Este procedimiento tiene $|w|$ pasos y genera una tupla $R(w) = (x_1, \cdots, x_n)$ donde cada componente representa el contenido final de cada pila. Por construcción $R(w)$ es irreducible (ya que se ha ido reduciendo en cada paso posible al eliminar las posibles ocurrencias consecutivas de una letra y la inversa) y $w\pi \xrightarrow{*} R(w)$.

Veamos en primer lugar que a partir de $R(w)$ podemos generar una palabra $r(w)$ en tiempo lineal cuya proyección sea $R(w)$, es decir, $(r(w))\pi = R(w)$, y en segundo lugar que esta palabra es la que buscamos, es decir, es una palabra que representa el mismo elemento que w y tiene longitud mínima. Por 4.13, dicha palabra existe. Para obtener dicha palabra, se sigue el siguiente procedimiento sucesivamente hasta vaciar todas las pilas: en primer lugar, elegimos una letra a tal que en todas las pilas que la contengan aparezca en la cima de la pila. Escribmos dicha letra y la desapilamos de todas esas pilas. Después repetimos el proceso escribiendo las letras sucesivas de derecha a izquierda.

Este procedimiento es válido ya que si $u\pi = t(a)\pi$, entonces existe $v \in W(X)$ tal que $v\pi = t$ y $u \overset{*}{\vdash\!\dashv} va$. Por otra parte, como $w\pi \overset{*}{\longrightarrow} R(w) = (r(w))\pi$, entonces $w \overset{*}{\longmapsto} r(w)$ así que en efecto $r(w)$ representa el mismo elemento que w en A_Γ. Veamos que $r(w)$ es de longitud mínima. Si existiera v de longitud menor que $r(w)$ y congruente con w, como T_0 es preperfecto, $v \overset{*}{\longmapsto} z \overset{*}{\longmapsfrom} r(w)$ para cierta z, luego por 4.10(I) $v\pi \overset{*}{\longrightarrow} z\pi \overset{*}{\longleftarrow} (r(w))\pi = R(w)$. Pero como $R(w)$ es irreducible, entonces $v\pi \overset{*}{\longrightarrow} (r(w))\pi$ siendo $|v| < |r(w)|$, lo que es imposible.

Finalmente, si lo único que queremos es resolver el problema de la palabra, es decir, decidir si $w = 1$ en A_Γ, la fase de reconstrucción no es necesaria ya que los estados finales de las pilas son los mismos si y solo si las entradas son congruentes, es decir, $w_1 \overset{*}{\longleftrightarrow} w_2 \iff R(w_1) = R(w_2)$. Así, el problema de la palabra tiene el mismo coste que el de reducción, es decir, es lineal en el tamaño de la entrada. $\square$

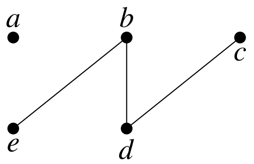
Para entender mejor el algoritmo anterior, veamos un par de ejemplos ilustrativos

Ejemplo 4.15. Sea el grafo Γ con $V(\Gamma) = \{a,b,c\}$ siendo A_Γ libre. Sean $A_1 = \{a^{\pm1}, c^{\pm1}\}$, $A_2 = \{b^{\pm1}, c^{\pm1}\}$ y $A_3 = \{a^{\pm1}, b^{\pm1}\}$. Llamemos P_1, P_2 y P_3 a cada pila. Consideremos la palabra $w = abca^{-1}ac^{-1}$. El algoritmo produce los siguientes pasos:

1. $P_1 = [], P_2 = [], P_3 = []$
2. Letra a, $P_1 = [a]$, $P_2 = []$, $P_3 = [a]$
3. Letra b, $P_1 = [a]$, $P_2 = [b]$, $P_3 = [a,b]$
4. Letra c, $P_1 = [a,c]$, $P_2 = [b,c]$, $P_3 = [a,b]$
5. Letra a^{-1}, $P_1 = [a,c,a^{-1}]$, $P_2 = [b,c]$, $P_3 = [a,b,a^{-1}]$
6. Letra a, $P_1 = [a,c]$, $P_2 = [b,c]$, $P_3 = [a,b]$
7. Letra c^{-1}, $P_1 = [a]$, $P_2 = [b]$, $P_3 = [a,b]$

Finalmente, se forma la proyección $R(w) = (a,b,ab)$ y $r(w) = ab$.

Ejemplo 4.16. Sea el grafo Γ:



Sean $A_1 = \{a^{\pm1}, b^{\pm1}, c^{\pm1}\}$, $A_2 = \{a^{\pm1}, d^{\pm1}, e^{\pm1}\}$ y $A_3 = \{c^{\pm1}, e^{\pm1}\}$. Llamemos P_1, P_2 y P_3 a cada pila. Consideremos la palabra $w = b^{-1}ace^{-1}be$. El algoritmo produce los siguientes pasos:

1. $P_1 = [], P_2 = [], P_3 = []$
2. Letra b^{-1}, $P_1 = [b^{-1}]$, $P_2 = []$, $P_3 = []$
3. Letra a, $P_1 = [b^{-1},a]$, $P_2 = [a]$, $P_3 = []$
4. Letra c, $P_1 = [b^{-1},a,c]$, $P_2 = [a]$, $P_3 = [c]$
5. Letra e^{-1}, $P_1 = [b^{-1},a,c]$, $P_2 = [a,e^{-1}]$, $P_3 = [c,e^{-1}]$
6. Letra b, $P_1 = [b^{-1},a,c,b]$, $P_2 = [a,e^{-1}]$, $P_3 = [c,e^{-1}]$
7. Letra e, $P_1 = [b^{-1},a,c,b]$, $P_2 = [a]$, $P_3 = [c]$

Finalmente, se forma la proyección $R(w) = (b^{-1}acb, a, c)$ y la reconstrucción $r(w) = b^{-1}acb$.

Bibliografía

[1] J. BOLER Y B. EVANS, *The free product of residually finite groups amalgamated along retracts is residually finite*, Proceedings of the American Mathematical Society, Volumen 37, Número 1, Páginas 50-52, 1973.

[2] R. CORI Y D. PERRIN, *Automates et commutations partielles*, Rairo informatique théorique, Volumen 19, Número 1, Páginas 21-32, 1985.

[3] C. DROMS, *Graph groups, coherence and three-manifolds*, Journal of algebra, Volumen 106, Número 2, Páginas 484-489, 1987.

[4] A. KARRASS Y D. SOLITAR, *The subgroups of a free product of two groups with an amalgamated subgroup*, Transactions of the American Mathematical Society, Volumen 150, Páginas 227-255, 1970.

[5] F. LABOURIE, *Lectures on representations of surface groups*, Orsay, 2011.

[6] R.C. LYNDON Y P.E. SCHUPP, *Combinatorial group theory*, Springer-Verlag, Berlín, 1977.

[7] P. NARENDRAN Y R. MCNAUGHTON, *The undecidability of the preperfectness of the Thue systems*, Theoretical Computer Science, Volumen 31, Páginas 165-174, 1984.

[8] D.J.S. ROBINSON, *A course in the theory of groups*, Springer, Universidad de Illinois, 1996.

[9] M. SALAMERO, *Bass-Serre Theory*, TFG, Universidad de Zaragoza, 2023.

[10] J.P. SERRE, *Trees*, Springer-Verlag, Berlín, 1980.

[11] H. SERVATIUS, C. DROMS Y B. SERVATIUS, *Surface subgroups of graph groups*, Proceedings of the American Mathematical Society, Volumen 106, Número 3, Páginas 573-578, 1989.

[12] T. WEIGEL, *Groups acting on trees*, Notes of summer school SMI, Perugia, 2012.

[13] C. WRATHALL, *The word problem for free partially commutative groups*, J. Symbolic Computation, Volumen 106, Número 6, Páginas 99-104, 1988.