Problema de clasificación de factorizaciones especiales en $SL(2,\mathbb{Z})$

Luis F. Moreno S.
lmorenos@eafit.edu.co
Ingeniero de sistemas, candidato a Magíster en Matemáticas Aplicadas

Asesor
Carlos Alberto Cadavid Moreno
ccadavid@eafit.edu.co
Doctor en matemáticas

Departamento de Ciencias Básicas
Universidad EAFIT
Medellín–Colombia

A los amigos, especialmente a los míos

Índice general

Introducción

Las fibraciones localmente holomorfas han recibido mucha atención recientemente por la relación íntima entre el hecho de que una $4-$variedad suave X admita una estructura simpléctica y el hecho de que exista una fibración localmente holomorfa cuyo dominio sea X, ver [1, 2].

Definición 1. Una *fibración localmente holomorfa* es una función suave $f : X \to \Sigma$, tal que:

1. f es sobreyectiva;
2. X (respectivamente Σ) es una $4-$variedad (respectivamente $2-$variedad) suave con frontera (posiblemente vacía) y que es compacta, orientada y conexa;
3. $f(intX) = int\Sigma$ y $f(\partial X) = \partial\Sigma$;
4. f tiene un número finito (posiblemente cero) de valores críticos $q_1, \ldots, q_k$, y todos están en $int\Sigma$;
5. f es localmente holomorfa, es decir, para cada $p \in intX$ existen cartas orientación preservantes alrededor de p y $f(p)$, que van a abiertos de $\mathbb{C}^2$ y de $\mathbb{C}$ (dotados de la orientación estándar) respecto a las cuales f es holomorfa;
6. la preimagen de cada valor regular es una $2-$variedad suave cerrada, orientable y conexa, de género $g \geqslant 0$.

Definición 2 (Fibración elíptica sobre D^2 de Lefschetz estricta)**.** Una fibración elíptica sobre D^2 de Lefschetz estricta es una fibración localmente holomorfa cuya base Σ es $D^2 = \{z \in \mathbb{C} : |z| \leqslant 1\}$, el género de las preimágenes de valores regulares es uno, cada fibra singular tiene un único punto crítico y es de tipo

nodal, y ninguna fibra contiene una esfera embebida cuya auto–intersección es -1.

El problema de clasificación de fibraciones elípticas sobre D^2, que sean de Lefschetz estrictas, salvo equivalencia topológica, es equivalente al problema de estudiar el conjunto

$$\left\{(g_1,\ldots,g_n) : n \geqslant 0 \text{ y } g_i \in SL(2,\mathbb{Z}) \text{ conjugado de } \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\right\} \Big/ H + C\,,$$

donde $H + C$ es la relación de equivalencia Hurwitz más conjugación, ver [1].

Buena parte de este problema sería satisfactoriamente resuelto si se tuviera:

1. Un método que, dado un $\mathsf{B} \in SL(2,\mathbb{Z})$, produzca una subcolección del conjunto $\mathcal{F}(\mathsf{B})$ de todas las factorizaciones especiales de B, con la propiedad de que todo miembro del conjunto $\mathcal{F}(\mathsf{B})/\equiv_H$, formado por las clases de equivalencia determinadas por la relación de equivalencia $\equiv_H$ (Hurwitz equivalencia), sea representado por al menos un elemento de dicha subcolección; y

2. Un método que, dado un B y dos factorizaciones especiales suyas decida si éstas son o no Hurwitz equivalentes.

Se obtiene en el presente trabajo un algoritmo que lleva a cabo la tarea propuesta en 1. Este algoritmo no aparece en la literatura revisada. La parte 2 no es desarrollada en este trabajo.

En [3] y [4] se estudia el problema análogo al que se propone estudiar acá, pero en el caso en que la base es cerrada, es decir, carece de frontera.

Este trabajo está organizado de la siguiente forma: la unidad 1 trata de los elementos necesarios de la Teoría de Grupos para la comprensión del problema, en la unidad 2 se enuncia el problema y se reduce éste a un grupo en el cual es práctico de resolver. En la unidad 3 se muestra el algoritmo solución del problema, el código en Maple y se da un ejemplo de la ejecución del código.

Unidad 1

Elementos de Teoría de grupos

En matemáticas, la Teoría de grupos estudia ciertas estructuras algebraicas conocidas como grupos; estas estructuras aparecen naturalmente en diversas situaciones matemáticas y físicas, entre otras.

En esta unidad se enunciarán algunas definiciones y teoremas de la Teoría de grupos necesarios para la comprensión de la unidad 2. La presente unidad es incluida en aras de la completitud de este trabajo; para una comprensión más profunda de cada aspecto se recomienda al lector consultar [5, 6, 7, 8, 9, 10, 11, 12, 13].

Comencemos por recordar las nociones fundamentales de operación binaria y grupo.

Definición 3 (Operación)**.** Sean X, Y conjuntos. Una *operación n–aria en X con valores en Y* es una regla que le asigna a cada elemento de $\underbrace{X \times X \times \cdots \times X}_{n-\text{veces}} = X^n$ un elemento de Y, es decir, es una función $f : X^n \to Y$. Cuando $Y = X$ se dice que tal operación es *interna*. En caso contrario se dice que la operación es *no interna*. Llamaremos *operación binaria* a una operación interna 2–aria. Si $*$ es una operación binaria en X entonces $*((x_1, x_2))$ se denotará por $x_1 * x_2$.

Ejemplo 1. En los enteros $\mathbb{Z}$, la operación de multiplicación entre estos es una operación binaria. En símbolos es $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
En $\mathbb{R}^n$, $n \geqslant 2$, el producto punto entre elementos es una operación no interna, pues el resultado es un real. En símbolos es $\bullet : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. ◇

Definición 4 (Homomorfismo)**.** Sean A y B conjuntos no vacíos con operaciones binarias $\cdot : A \times A \to A$ y $* : B \times B \to B$. Entonces, una función $f : A \to B$ es un

homomorfismo si y sólo si $\forall\ a_1, a_2 \in A$ se cumple que $f(a_1 \cdot a_2) = f(a_1) * f(a_2)$. El hecho de que f sea un homomorfismo equivale a la conmutatividad del diagrama

$$\begin{array}{ccc} A \times A & \xrightarrow{\cdot} & A \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ B \times B & \xrightarrow{*} & B \end{array}$$

es decir, equivale a $f \circ \cdot = * \circ (f \times f)$.

Un homomorfismo inyectivo es llamado *monomorfismo*; uno sobreyectivo es llamado *epimorfismo*; y si es biyectivo, *isomorfismo*. Decimos que las estructuras $(A, \cdot)$ y $(B, *)$ son isomorfas (o también, $(A, \cdot)$ es isomorfa a $(B, *)$) si existe un isomorfismo $f : A \to B$. Abreviadamente, siempre y cuando no se presente confusión, diremos que A y B son isomorfas (o también que A es isomorfa a B).

Un homomorfismo $f : A \to A$ es llamado *endomorfismo*, y si es biyectivo *automorfismo*.

Proposición 1. *Sean $(A, \cdot)$ y $(B, *)$ conjuntos dotados de operaciones binarias. Si $f : A \to B$ es un isomorfismo entonces $f^{-1} : B \to A$ también lo es.*

Prueba.

①	$f : A \to B$ es un isomorfismo,	hipótesis
②	$f(a_1 \cdot a_2) = f(a_1) * f(a_2)\ \forall a_1, a_2 \in A$,	por ①
③	$f^{-1} : B \to A$ existe y es biyectiva,	por ①
④	$\forall b_1, b_2 \in B$, $\exists a_1, a_2 \in A$ tales que $b_1 = f(a_1)$ y $b_2 = f(a_2)$,	de ①
⑤	$f^{-1}(b_1 * b_2) = f^{-1}(f(a_1) * f(a_2))$,	por ④
⑥	$= f^{-1}(f(a_1 \cdot a_2))$,	por ②
⑦	$= a_1 \cdot a_2$,	$f^{-1} \circ f = I$ (identidad)
⑧	$= f^{-1}(b_1) \cdot f^{-1}(b_2)$,	por ④ y definición de f^{-1}

Luego, por ③ y ⑤ a ⑧, f^{-1} es un isomorfismo. □

Definición 5 (Grupo)**.** Un grupo $(G, *)$ es un conjunto $G \neq \emptyset$ dotado de una operación binaria $*$ que cumple los siguientes axiomas:

1. $\forall g_1, g_2, g_3 \in G$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.
2. $\exists h \in G$ tal que $\forall g \in G$, se cumple que $g * h = h * g = g$. Se puede ver que un h con esta propiedad es único. Este elemento se denotará por e y se llamará el *elemento identidad* del grupo $(G, *)$.

3. $\forall g \in G$, $\exists h \in G$ con la propiedad $g * h = h * g = e$. También se puede ver que un h con esta propiedad es único. Este elemento se denotará por g^{-1} y se le llamará el *inverso de* g.

Nota. Siempre que no dé lugar a confusión, se denotará $(G, *)$ por G y $g_1 * g_2$ por $g_1 g_2$.

Ejemplo 2. El conjunto $\mathbb{R}^* = \mathbb{R} - \{0\}$ con la operación multiplicación $\cdot$ conforman un grupo. Veamos:

1. La multiplicación de dos reales distintos de cero es otro real distinto de cero, y por tanto $\cdot$ es una operación binaria en $\mathbb{R}^*$.

2. $\forall r_1, r_2, r_3 \in \mathbb{R}^*$, se cumple que $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$, pues la multiplicación de reales es asociativa.

3. El 1, perteneciente a $\mathbb{R}^*$, es tal que $\forall r \in \mathbb{R}^*$, se cumple que $r \cdot 1 = 1 \cdot r = r$. Así, el elemento 1 es el elemento identidad para la multiplicación sobre $\mathbb{R}^*$.

4. $\forall r \in \mathbb{R}^*$, $\exists s = \frac{1}{r} \in \mathbb{R}^*$ tal que $r \cdot s = s \cdot r = 1$. El elemento $\frac{1}{r}$ es el inverso de r respecto a la multiplicación sobre $\mathbb{R}^*$. $\diamond$

Definición 6 (Grupo abeliano)**.** Si en un grupo $(G, *)$ su operación binaria es conmutativa, es decir, $\forall g_1, g_2 \in G$, $g_1 g_2 = g_2 g_1$, entonces se dice que es un grupo abeliano.

Ejemplo 3. Se puede probar que $(\mathbb{R}, +)$ es un grupo y además es abeliano pues $\forall a, b \in \mathbb{R}, a + b = b + a$.

También se puede probar que $(\mathbb{Z}, +)$ es un grupo abeliano. $\diamond$

El conjunto de enteros $n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$, $n \in \mathbb{Z}$, junto con la operación suma usual de enteros conforma un grupo abeliano y lo escribiremos como $(n\mathbb{Z}, +)$. Por ejemplo, el conjunto $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ junto con la operación suma usual es un grupo abeliano.

El conjunto de enteros $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ junto con la operación *suma módulo* n, $+_n$, definida por $a +_n b :=$ residuo no negativo de dividir $a + b$ entre n, conforma un grupo abeliano. Por simplicidad denotaremos $+_n$ como $+$ siempre que no dé lugar a confusión. Por ejemplo, el conjunto $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ junto con la operación suma módulo 5 es un grupo abeliano.

El conjunto de matrices de dimensión dos por dos, con entradas enteras y determinante igual a uno, junto con la operación multiplicación de matrices,

forma un grupo no abeliano, el cual escribiremos como $SL(2,\mathbb{Z})$. En la sección 2.2 profundizaremos en el estudio de este grupo. También se puede ver que $SL(2,\mathbb{C})$, es decir, el conjunto de matrices de dimensión dos por dos, con entradas complejas y determinante igual a uno, junto con la operación multiplicación de matrices, forma un grupo.

Definición 7 (Orden de un grupo)**.** El orden de un grupo $(G,*)$ se refiere a la cardinalidad del conjunto G; así, los grupos, pueden clasificarse en grupos de *orden finito* y grupos de *orden infinito*.

Por ejemplo, el orden de los grupos $(\mathbb{R}^*,\cdot)$, $(\mathbb{R},+)$ y $(\mathbb{Z},+)$ es infinito, mientras que el orden de $(\mathbb{Z}_n,+)$ es n, en particular, finito.

A manera de ilustración, veamos a continuación dos grupos finitos:

El *grupo cuaterniónico* es aquel grupo no abeliano de orden ocho $(\mathbb{Q},\cdot)$, donde $\mathbb{Q}=\{\pm 1,\pm i,\pm j,\pm k\}$ y $\cdot$ es la operación binaria $x\cdot y$ indicada en la tabla 1.1, x leído de la primera columna y y de la primera fila, y $x\cdot y$ es el elemento de la intersección de la fila en la que se encuentra x con la columna en la que se encuentra y; por ejemplo $i\cdot j=k$. El elemento identidad es 1.

Tabla 1.1: operación binaria en el grupo cuaterniónico

·	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Note que este grupo no es conmutativo; por ejemplo, $ij=-ji$.

Se puede ver que la función $f:\mathbb{Q}\to SL(2,\mathbb{C})$ definida como

$$f(1)=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ f(i)=\begin{pmatrix}i&0\\0&-i\end{pmatrix},\ f(j)=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\ \text{y}\ f(k)=\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

es un monomorfismo.

Definición 8 (Permutación)**.** Dado un conjunto A diferente de vacío, una permutación de A es una función $\rho:A\to A$ biyectiva.

Ejemplo 4. Sea $A = \{0, 1, 2\}$ con $\rho_1(0) = 1$, $\rho_1(1) = 2$, $\rho_1(2) = 0$ y $\rho_2(0) = 2$, $\rho_2(1) = 0$, $\rho_2(2) = 1$; entonces ρ_1 y ρ_2 son permutaciones de A. $\diamond$

Es claro que la composición (como funciones) de dos permutaciones de A es nuevamente una permutación de A, y la inversa (como función) de una permutación de A es también una permutación de A. El conjunto formado por todas las permutaciones posibles de A, S_A, dotado de la operación binaria composición, es un grupo, cuyo elemento identidad, e, es aquella permutación que envía cada elemento $a \in A$ en sí mismo.

Un elemento ρ perteneciente a S_n se acostumbra representar como

$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix}.$$

Ejemplo 5. Sea $A = \{1, 2, 3, 4, 5, 6\}$ y ρ la permutación dada por

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}.$$

Sea τ otra permutación dada por

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 2 & 6 \end{pmatrix},$$

entonces $\tau\rho$, componiendo de derecha a izquierda, como en la composición de funciones, es

$$\tau\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 2 & 1 \end{pmatrix}.$$

La permutación inversa de $\tau\rho$ es

$$(\tau\rho)^{-1} = \rho^{-1}\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}. \quad \diamond$$

Definición 9 (Grupo simétrico)**.** Sea A el conjunto finito $\{1, 2, \ldots, n\}$. El grupo S_A se llama grupo simétrico en n símbolos, y es denotado por S_n.

Ejemplo 6. El grupo simétrico S_3 es $\{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$ con

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Note que S_3 tiene 3! elementos. En general, S_n contiene $n!$ elementos, es decir, $n!$ es el orden de S_n. ◇

Definición 10 (Subgrupo)**.** Sea $(G, *)$ un grupo. Si $H \subseteq G$, $H \neq \emptyset$, es un grupo bajo la operación $*$, entonces decimos que H es un subgrupo de G y lo denotamos como $H \leqslant G$.

Ejemplo 7. El grupo $(\mathbb{Z}, +)$ es subgrupo de $(\mathbb{R}, +)$, pues $\mathbb{Z} \subseteq \mathbb{R}$ y en $(\mathbb{Z}, +)$, la operación suma es la restricción de la operación suma en $(\mathbb{R}, +)$. ◇

De acuerdo a la definición 5, se puede mostrar que todo grupo G tiene al menos dos subgrupos: $\{e\}$ y G mismo. También se puede probar que la intersección de una colección de subgrupos de G es un subgrupo de G.

Teorema 1. *Si $H \subseteq G$, $H \neq \emptyset$, entonces H es subgrupo de $(G, *)$ si y sólo si*

i) $\forall h_1, h_2 \in H$, entonces $h_1 * h_2 \in H$.

ii) Si $h \in H$, entonces $h^{-1} \in H$.

Prueba. Dado un grupo $(G, *)$ y $H \subseteq G$ se tiene que:
"$\Rightarrow$"

① Sea H subgrupo de $(G, *)$, hipótesis.
② Puesto que H es grupo, entonces *i)* y *ii)* se cumplen, por definición.

"$\Leftarrow$"

③ Sean $h_1, h_2 \in H$, entonces $h_1 * h_2 \in H$ por *i)*.
④ Sean $h_1, h_2, h_3 \in H$. Puesto que $h_1 * h_2 \in H$ y $h_2 * h_3 \in H$ por *i)*, $H \subseteq G$, y $(G, *)$ es grupo, entonces $(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$.
⑤ Puesto que $H \neq \emptyset$, entonces existe un $h \in H$, y también existe $h^{-1} \in H$ por *ii)*, tales que $h * h^{-1} = e \in H$, por *i)*.
⑥ Para todo $h \in H$, existe $h^{-1} \in H$ por ii).

Entonces, por ③, ④, ⑤ y ⑥ H es un grupo y por tanto subgrupo de $(G, *)$. □

El conjunto $n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\} = \{zn : z \in \mathbb{Z}\}$ junto con la operación suma de enteros es subgrupo de $(\mathbb{Z}, +)$. En efecto, $n\mathbb{Z} \subseteq \mathbb{Z}$,

$n\mathbb{Z} \neq \emptyset$, y $\forall z_1, z_2 \in \mathbb{Z}$ se cumple que $z_1 n + z_2 n = (z_1 + z_2)n \in n\mathbb{Z}$, y $\forall z \in \mathbb{Z}$ el inverso de zn es $(-z)n$.

Definición 11 (Subgrupo generado y conjunto generador de un grupo)**.** Sea $(G, *)$ un grupo y $S \subseteq G$. Definimos $\langle S \rangle$ como la intersección de todos los subgrupos de G que contienen a S; en símbolos

$$\langle S \rangle := \bigcap_{\substack{H \leqslant G \\ S \subseteq H}} H \,.$$

Decimos que S es generador de G, si $\langle S \rangle = G$.

Se puede demostrar que un elemento de G está en $\langle S \rangle$, si y sólo si se puede obtener como un producto finito de elementos de $S \cup S^{-1}$, donde $S^{-1} := \{g^{-1} : g \in S\}$. Si $S = \emptyset$, entonces $\langle S \rangle$ resulta ser el grupo trivial $\{e\}$.

Definición 12. Un subgrupo H de G se dice que es cíclico si existe $a \in H$ tal que $H = \langle \{a\} \rangle$. En este caso $H = \{a^n : n \in \mathbb{Z}\}$.

Ejemplo 8. El grupo $(\mathbb{Z}, +)$ es cíclico pues $\mathbb{Z} = \langle 1 \rangle$. Este grupo también puede ser generado por el conjunto $\{2, 3\}$.

Otro ejemplo de grupo cíclio es $(\mathbb{Z}_3, +)$. En efecto, $\mathbb{Z}_3 = \langle 1 \rangle = \langle 2 \rangle$. ◇

Definición 13 (Producto entre conjuntos)**.** Dados dos subconjuntos S y T de un grupo G, definimos su producto ST como

$$ST = \{st : s \in S \text{ y } t \in T\} \,.$$

Si S, R, T son subconjuntos de un grupo G, entonces $S(RT) = (SR)T$, pues para todo $s \in S$, $r \in R$ y $t \in T$ se cumple que $s(rt) = (sr)t$; luego el producto entre conjuntos es asociativo. Si $S = \{g\}$ entonces escribimos gT y Tg en vez de $\{g\}T$ y $T\{g\}$, respectivamente.

Es importante observar que si H es subgrupo de G entonces $HH = H$.

Definición 14 (Clase lateral)**.** Dado un grupo G, H subgrupo de G y un $g \in G$, decimos que:

1. $gH = \{gh : h \in H\}$ es una *clase lateral izquierda* de H en G.
2. $Hg = \{hg : h \in H\}$ es una *clase lateral derecha* de H en G.

Ejemplo 9. $H = \{0, 3\}$ es un subgrupo de $(\mathbb{Z}_6, +)$. Las clases laterales izquierdas de H son:

- $0 + H = \{0, 3\} = H$
- $1 + H = \{1, 4\}$
- $2 + H = \{2, 5\}$
- $3 + H = \{3, 0\} = H$
- $4 + H = \{4, 1\} = 1 + H$
- $5 + H = \{5, 2\} = 2 + H$.

Se puede observar que realmente hay tres clases laterales izquierdas diferentes: $H, 1 + H$ y $2 + H$. Observe también que las diferentes clases laterales izquierdas particionan a $\mathbb{Z}_6$. Además, como $(\mathbb{Z}_6, +)$ es un grupo abeliano, entonces cada clase lateral izquierda, es igual a su respectiva clase lateral derecha: $0 + H = H + 0, 1 + H = H + 1$ y $2 + H = H + 2$. ◇

Definición 15 (Conjugado)**.** Dado un grupo G y $x, a \in G$, decimos que el conjugado de x bajo a es $a^{-1}xa$.

Definición 16 (Subgrupo normal)**.** Un subgrupo N de un grupo G, es llamado normal, lo cual se representa por $N \lhd G$, si es invariante bajo la conjugación, es decir, $\forall n \in N$ y $\forall g \in G, g^{-1}ng \in N$ o, equivalentemente, $\forall g \in G, Ng = gN$.

Ejemplo 10. Si G es un grupo, entonces los subgrupos $\{e\}$ y G son subgrupos normales. Ahora, si G es abeliano, todos sus subgrupos son normales puesto que $\forall n \in N$ y $g \in G$, $g^{-1}ng = g^{-1}gn = en = n$.

El conjunto $\{\pm \mathsf{I}_2\}$, siendo I_2 la matriz identidad de dimensión dos, es un subgrupo normal de $SL(2,\mathbb{Z})$. ◇

Definición 17 (Grupo cociente)**.** Dado un subgrupo normal N de un grupo G, definimos el grupo cociente, G/N, como el conjunto de todas las clases laterales izquierdas de N en G, es decir, $G/N = \{gN : g \in G\}$, con la operación de grupo dada por el producto de estos subconjuntos.

Teorema 2 (Grupo cociente)**.** *Dados G un grupo y N un subgrupo normal, entonces G/N es un grupo.*

Prueba. Sean aN, bN y cN clases laterales izquierdas de N en G, entonces:

① Veamos la clausuratividad

$$\begin{aligned}(aN)(bN) &= (aN)(Nb)\\ &= a(NN)b\\ &= aNb\\ &= a(Nb)\\ &= a(bN)\\ &= (ab)N\,.\end{aligned}$$

Como $ab \in G$, entonces $(ab)N$ es una clase lateral izquierda de N en G.

② Ahora la asociatividad

$$\begin{aligned}[(aN)(bN)]\,(cN) &= ((ab)N)\,cN\\ &= (ab)(Nc)N\\ &= (ab)(cN)N\\ &= ((ab)c)\,N\\ &= (a(bc))\,NN\\ &= (aN)\,((bc)N)\\ &= (aN)\,[(bN)(cN)]\,.\end{aligned}$$

③ N juega el papel de elemento neutro de G/N, pues

$$\begin{aligned}N(aN) &= (Na)N\\ &= (aN)N\\ &= a(NN)\\ &= aN\,.\end{aligned}$$

④ $\forall aN \in G/N, \exists bN \in G/N$ tal que $(aN)(bN) = N$; tal elemento es $a^{-1}N$ pues $(aN)(a^{-1}N) = (aa^{-1})N = N$. □

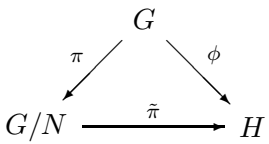
Ejemplo 11. Considere el grupo $(\mathbb{Z}, +)$ y el subgrupo $(n\mathbb{Z}, +)$, con n un entero positivo; es obvio que $n\mathbb{Z}$ es normal puesto que $(\mathbb{Z}, +)$ es abeliano. Entonces, el conjunto de las clases laterales izquierdas $\{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, forman el grupo cociente $\mathbb{Z}/n\mathbb{Z}$. Éste es un grupo cíclico de orden n. El grupo $(\mathbb{Z}/n\mathbb{Z}, +)$ es isomorfo a $(\mathbb{Z}_n, +)$.

Otro ejemplo es el cociente entre el grupo $SL(2, \mathbb{Z})$ y el subgrupo normal $\{\pm \mathsf{I}_2\}$, donde cada elemento resulta ser $\{\pm \mathsf{A}\}$, $\mathsf{A} \in SL(2, \mathbb{Z})$. Este grupo es denotado como $PSL(2, \mathbb{Z})$ y es objeto de estudio en la sección 2.2. ◇

Definición 18 (Núcleo de un homomorfismo)**.** Sea $\phi : G \to H$ un homomorfismo entre grupos. Al conjunto $\{g \in G : \phi(g) = e\}$ se le llama núcleo de ϕ.

Resulta inmediato verificar que el núcleo de un homomorfismo es subgrupo normal.

Teorema 3 (Teorema fundamental de homomorfismos)**.** *Dados los grupos G y H, y un epimorfismo $\phi : G \to H$, existe un único isomorfismo $\tilde{\pi} : G/N \to H$, donde N es el núcleo de ϕ tal que el diagrama*



conmuta, es decir, $\phi = \tilde{\pi} \circ \pi$. Acá π denota al homomorfismo canónico, o sea, el que envía cada elemento de G en su clase lateral izquierda.

Definición 19 (Alfabeto, letras, sílabas, palabras)**.** Sea el conjunto $A = \{a_i : i \in I\}$, I un conjunto finito o infinito; a A le llamaremos el alfabeto, a sus elementos a_i letras, a los elementos de la forma a_i^n, $n \in \mathbb{Z}$, sílabas con $a_i^1 = a_i$, y a las cadenas finitas de sílabas de la forma $a_{i_1}^{n_1} a_{i_2}^{n_2} \dots a_{i_m}^{n_m}$ palabras.

Note que en una palabra $a_{i_1}^{n_1} a_{i_2}^{n_2} \dots a_{i_m}^{n_m}$ se permite que $a_{i_j} = a_{i_{j+1}}$ para algún j. Escribiremos la *palabra vacía* como e.

Ejemplo 12. Dado un alfabeto $A = \{a_1, a_2, a_3\}$ entonces

- a_1, a_2, a_3 son las letras de A,
- a_1^3, a_1, a_3^{-2} son sílabas,
- $a_1^2 a_3^{-2} a_3^2, a_3 a_2^2 a_1 a_2^{-1}$ son palabras. ◇

Sea $w = a_{i_1}^{n_1} a_{i_2}^{n_2} \dots a_{i_m}^{n_m}$ una palabra tal que $a_{i_j} = a_{i_{j+1}}$ para algún j. Entonces, diremos que la palabra que resulta de sustituir a $a_{i_{j-1}}^{n_{j-1}} a_{i_j}^{n_j} a_{i_{j+1}}^{n_{j+1}} a_{i_{j+2}}^{n_{j+2}}$ en w por $a_{i_{j-1}}^{n_{j-1}} a_{i_j}^{n_j+n_{j+1}} a_{i_{j+2}}^{n_{j+2}}$ si $n_j + n_{j+1} \neq 0$, ó por $a_{i_{j-1}}^{n_{j-1}} a_{i_{j+2}}^{n_{j+2}}$ si $n_j + n_{j+1} = 0$, fue obtenida de w mediante una *contracción*. Si $w = a_{i_1}^{n_1} a_{i_2}^{n_2} \dots a_{i_m}^{n_m}$ es una palabra tal que $n_j = 0$ para algún j, entonces diremos que la palabra que se obtiene de suprimir a $a_{i_j}^0$ en w fue obtenida también por una *contracción*.

Definición 20 (Palabra reducida)**.** Una palabra donde no hay contracciones posibles es llamada palabra reducida. En caso contrario decimos que no es reducida.

Ejemplo 13. En el alfabeto $B = \{b_1, b_2\}$, la palabra $b_2 b_2^2 b_1 b_1^{-1} b_2 b_1^3$ es no reducida, pero, por contracciones lo puede ser a

$$\begin{aligned} b_2 b_2^2 b_1 b_1^{-1} b_2 b_1^3 &= b_2^3 b_1 b_1^{-1} b_2 b_1^3 \\ &= b_2^3 b_2 b_1^3 \\ &= b_2^4 b_1^3 . \end{aligned}$$ ◇

La *yuxtaposición* entre dos palabras *reducidas* $\omega = s_{i_1}^{a_1} s_{i_2}^{a_2} \dots s_{i_m}^{a_m}$ y $\theta = s_{j_1}^{b_1} s_{j_2}^{b_2} \dots s_{j_n}^{b_n}$, que denotaremos por $\omega * \theta$, se realiza de la siguiente forma: se toma la palabra $\omega\theta := s_{i_1}^{a_1} s_{i_2}^{a_2} \dots s_{i_m}^{a_m} s_{j_1}^{b_1} s_{j_2}^{b_2} \dots s_{j_n}^{b_n}$ que se obtiene de colocar θ a la derecha de ω y se suprimen las últimas k sílabas de ω tales que $s_{i_{m-k+1}}^{a_{m-k+1}} \dots s_{i_m}^{a_m} = s_{j_k}^{-b_k} \dots s_{j_1}^{-b_1}$ junto con las primeras k sílabas de θ, donde k es maximal respecto a esta propiedad. Entonces se tiene que:

- Si $m = n$, y en el caso que $k = m$, $\omega * \theta$ se define como la palabra vacía;
- Si $m < n$, y en el caso que $k = m$, entonces $\omega * \theta := s_{j_{m+1}}^{b_{m+1}} \dots s_{j_n}^{b_n}$;
- Si $m > n$, y en el caso que $k = n$, entonces $\omega * \theta := s_{i_1}^{a_1} \dots s_{i_{m-n}}^{a_{m-n}}$;
- Pero si $k < \text{mín}\{m, n\}$, pueden ocurrir dos situaciones:
  - Si $s_{i_{m-k}}$ es distinto de $s_{j_{k+1}}$, entonces $\omega * \theta := s_{i_1}^{a_1} \dots s_{i_{m-k}}^{a_{m-k}} s_{j_{k+1}}^{b_{k+1}} \dots s_{j_n}^{b_n}$;
  - Si $s_{i_{m-k}}$ es igual a $s_{j_{k+1}}$, entonces $\omega * \theta := s_{i_1}^{a_1} \dots s_{i_{m-k}}^{a_{m-k}+b_{k+1}} s_{j_{k+2}}^{b_{k+2}} \dots s_{j_n}^{b_n}$;

Ejemplo 14. Las palabras reducidas $\omega = a_4 a_3^2 a_4^4 a_5^{-2}$ y $\theta = a_5^2 a_4^{-4} a_3$ construidas sobre el conjunto $S = \{a_1, a_2, a_3, a_4, a_5\}$, al ser yuxtapuestas se obtiene $a_4 a_3^3$. ◇

Al conjunto formado por todas las palabras reducidas de un alfabeto S, lo denotaremos como F_S.

En la categoría de los grupos existen objetos libres llamados *grupos libres*, veamos su definición.

Definición 21 (Grupo libre)**.** Un grupo $(G, *)$ es libre si existe $S \subseteq G - \{e\}$ tal que:

i) Todo $g \in G - \{e\}$ puede escribirse en forma única como

$$g = s_1^{a_1} s_2^{a_2} \dots s_n^{a_n}\,, \tag{1.1}$$

donde $n \geqslant 1$, cada $s_i \in S$, $a_i \in \mathbb{Z} - \{0\}$, y los s_i adyacentes son diferentes entre sí.

ii) Ninguna expresión de la forma (1.1) que tenga las cuatro propiedades da la identidad en G.

Teorema 4. *El conjunto de todas las palabras reducidas, denotado como F_S, de un alfabeto $S = \{s_i : i \in I\}$, junto con la operación yuxtaposición, forma un grupo.*

Prueba.

① Por la definición misma de yuxtaposición, el producto de dos palabras reducidas produce una palabra reducida.

② La palabra vacía e es tal que $\forall \omega \in F_S$ se cumple que $\omega * e = e * \omega = \omega$. Por lo tanto e es el elemento neutro en F_S.

③ Si $\omega_i = s_{i_1}^{a_1} \dots s_{i_m}^{a_m}$ es una palabra reducida, entonces la palabra $\omega_i^{-1} := s_{i_m}^{-a_m} \dots s_{i_1}^{-a_1}$ es también reducida y claramente es inverso de ω.

④ Para cada $s \in F_S$ y $a = \pm 1$, sea

$$\begin{aligned} |s^a| &: F_S \to F_S \\ s_1^{a_1} \dots s_n^{a_n} &\mapsto s^a * s_1^{a_1} \dots s_n^{a_n}\,. \end{aligned}$$

Puesto que $|s| \circ |s^{-1}| = id_{F_S} = |s^{-1}| \circ |s|$, cada $|s^a|$ es una permutación de F_S (con inversa $|s^{-a}|$). Sea $A(F_S)$ el grupo simétrico de F_S, definición 9, y F_0 el subgrupo generado por $\{|s| : s \in S\}$. Definimos la función $\phi : F_S \to F_0$ dada por $e \to id_{F_S}$ y $s_{i_1}^{a_1} \dots s_{i_n}^{a_n} \mapsto |s_{i_1}^{signo(a_1)}|^{\circ |a_1|} \circ \dots \circ |s_{i_n}^{signo(a_n)}|^{\circ |a_n|}$, donde $signo(a)$ es igual a 1 si a es positivo y -1 si a es negativo, y $f^{\circ n}$ significa la composición de f consigo misma n veces. Es claro que ϕ es sobreyectiva y que satisface $\phi(\omega_1 * \omega_2) = \phi(\omega_1) \circ \phi(\omega_2)$ para todo $\omega_1, \omega_2 \in F_S$. Puesto que la función $\phi(s_{i_1}^{a_1} \dots s_{i_n}^{a_n})$ envía la palabra vacía en $s_1^{a_1} \dots s_n^{a_n}$ se deduce inmediatamente que $\phi(s_{i_1}^{a_1} \dots s_{i_n}^{a_n}) = id_{F_S}$ si y sólo si $s_{i_1}^{a_1} \dots s_{i_n}^{a_n}$ es la palabra vacía. Como $\phi(\omega_1 * \omega_2) = \phi(\omega_1) \circ \phi(\omega_2)$, lo anterior implica que ϕ es inyectiva. El hecho de que $(F_0, \circ)$ es un grupo y que ϕ^{-1} transforma $\circ$ en $*$ muestra que la asociatividad se preserva en F_S y que ϕ es un isomorfismo de grupos. Obviamente $F_S = \langle S \rangle$.

Entonces, por ①, ②, ③ y ④, F_S es un grupo. □

Es fácil ver que el grupo F_S descrito en el teorema 4 es un grupo libre. Note que F_S es infinito para todo conjunto $S \neq \emptyset$.

Ejemplo 15. Si $S = \{a\}$ entonces el grupo libre F_S es cíclico y por tanto abeliano.

El conjunto $S = \{a, b\}$ genera el grupo libre F_S donde algunos elementos pertenecientes a F_S son $\omega_1 = a^2b^3$, $\omega_2 = ba^2b^3$, $\omega_3 = a^{-2}b^3a$, $\omega_0 =$, (ω_0 es la palabra vacía), etcétera. Es interesante observar que dos elementos ω_1, ω_2 de F_S conmutan si y sólo si existe ω en F_S tal que $\omega_1 = \omega^m$ y $\omega_2 = \omega^n$ para algunos enteros m, n. ◇

Un modo de definir un grupo es por una presentación: se especifica un conjunto S, y un subconjunto R de F_S. Luego se toma la intersección de todos los subgrupos normales de F_S que contienen a R, que denotamos por $N(R)$. Formamos el grupo $F_S/N(R)$ al cual denotamos por $\langle S|R\rangle$. El grupo $\langle S|R\rangle$ se puede interpretar como el grupo más grande posible en el que se cumplen cada una de las relaciones $r = e$, $r \in R$. De manera precisa, el que se satisfagan las relaciones significa que si $r = s_{i_1}^{a_1} \dots s_{i_m}^{a_m}$, entonces en el grupo $\langle S|R\rangle$ se cumple la igualdad $(s_{i_1}N)^{a_1} \dots (s_{i_m}N)^{a_m} = N$, donde N denota $N(R)$. El que sea el grupo más grande con esta propiedad quedará aclarado por el teorema 5. En la práctica, en lugar de escribir pN, donde $p \in F_S$, se escribe simplemente $\bar{p}$. El hecho de que $(pN)(qN) = (p * q)N$ se refleja en la nueva notación como $\bar{p}\bar{q} = \overline{p * q}$.

Definición 22 (Presentación de un grupo y grupo finitamente presentable)**.** Formalmente se dice que un grupo G admite la presentación

$$\langle S|R\rangle$$

si G es isomorfo a $\langle S|R\rangle$. Se dice que G es finitamente presentable si existe una presentación $\langle S|R\rangle$ suya en la que S y R son finitos.

Normalmente, cuando S y R son finitos se omiten las llaves en la notación $\langle S|R\rangle$.

Ejemplo 16. El grupo cíclico $\mathbb{Z}_n$ tiene la presentación

$$\langle \{a\}|\{a^n\}\rangle\,,$$

la cual, de acuerdo a la convención anterior, puede ser escrita como

$$\langle a|a^n\rangle\,.$$ ◇

Todo grupo admite una presentación, y de hecho diversas presentaciones; una presentación es a menudo la forma más compacta de describir la estructura de un grupo.

Ejemplo 17. Recordemos que el grupo simétrico S_3 es $\{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$ con

$$\rho_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \rho_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \rho_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
$$\rho_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \rho_4 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \rho_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Éste admite la presentación

$$\langle a, b | a^2, b^3, bab^{-2}a^{-1}\rangle\,.$$

En efecto, se puede ver que existe un isomorfismo $\phi : \langle a, b|a^2, b^3, bab^{-2}a^{-1}\rangle \to S_3$, que envía a aN en ρ_2 y a bN en ρ_3, donde N es $N(a^2, b^3, bab^{-2}a^{-1})$. ◇

Teorema 5 (Van Dyck)**.** *Sea G un grupo y $A \subseteq G$ tal que $G = \langle A\rangle$, y sea $\iota : S \to A$ una biyección entre A y un conjunto S. Supongamos que R es un conjunto de palabras en S con la propiedad de que si $s_{i_1}^{n_1} s_{i_2}^{n_2} \dots s_{i_m}^{n_m} \in R$, entonces $\iota(s_{i_1})^{n_1}\iota(s_{i_2})^{n_2}\dots\iota(s_{i_m})^{n_m} = e_G$. Entonces existe un epimorfismo $f : \langle S|R\rangle \to G$ que envía $sN \mapsto f(sN) = \iota(s)$, $\forall s \in S$. Acá N denota $N(R)$.*

Ejemplo 18. Tomando $G = S_3$, y $S = \{\rho_2, \rho_3\}$ se puede ver que el generado de S es S_3. Además, se puede verificar directamente que $\rho_2^2, \rho_3^3, \rho_3\rho_2\rho_3^{-2}\rho_2^{-1}$ son la permutación identidad. El teorema de Van Dyck nos dice que existe un epimorfismo $\phi : \langle \rho_2, \rho_3 | \rho_2^2, \rho_3^3, \rho_3\rho_2\rho_3^{-2}\rho_2^{-1}\rangle \to S_3$ que envía a $\rho_2 N$ en ρ_2 y a $\rho_3 N$ en ρ_3. Se puede ver que ϕ es de hecho un isomorfismo, verificando que el núcleo de ϕ es $\{N\}$.

Definición 23 (Producto libre)**.** Se define el producto libre $G * H$ entre dos grupos G y H como el grupo conformado por:

1. El conjunto de todas las palabras de la forma $s_1 s_2 \dots s_n$, $s_i \notin \{e_G, e_H\}$, $n \geqslant 1$, y la palabra vacía notada como e; donde, si $s_i \in G$ (respectivamente H), entonces $s_{i-1} \in H$ (respectivamente G), $2 \leqslant i \leqslant n$, es decir, cada elemento en $G * H$ corresponde al producto alternado de elementos de G y elementos de H.

2. La operación definida sobre $G * H$ corresponde a la multiplicación de las palabras de dicho grupo definida como:

La *multiplicación* entre dos palabras $\omega = s_{i_1}s_{i_2}\dots s_{i_m}$ y $\theta = s_{j_1}s_{j_2}\dots s_{j_n}$, que denotaremos por $\omega * \theta$, se realiza de la siguiente forma: se toma la palabra $\omega\theta := s_{i_1}s_{i_2}\dots s_{i_m}s_{j_1}s_{j_2}\dots s_{j_n}$ que se obtiene de colocar θ a la derecha de ω y se suprimen las últimas k sílabas de ω tales que $s_{i_{m-k+1}}\dots s_{i_m} = s_{j_k}^{-1}\dots s_{j_1}^{-1}$ junto con las primeras k sílabas de θ, donde k es maximal respecto a esta propiedad. Entonces se tiene que:

- Si $m = n$, y en el caso que $k = m$, $\omega * \theta$ se define como la palabra vacía;
- Si $m < n$, y en el caso que $k = m$, entonces $\omega * \theta := s_{j_{m+1}}\dots s_{j_n}$;
- Si $m > n$, y en el caso que $k = n$, entonces $\omega * \theta := s_{i_1}\dots s_{i_{m-n}}$;
- Pero si $k < \text{mín}\{m, n\}$, pueden ocurrir dos situaciones:
  · Si $s_{i_{m-k}} \in G$ y $s_{j_{k+1}} \in H$ o vicecersa (de donde se deduce que k es igual a cero), entonces $\omega * \theta := s_{i_1}\dots s_{i_m}s_{j_1}\dots s_{j_n}$;
  · Si $s_{i_{m-k}}, s_{j_{k+1}} \in G$ ó $s_{i_{m-k}}, s_{j_{k+1}} \in H$ (en este caso k es mayor o igual a cero), entonces $\omega * \theta := s_{i_1}\dots s_{i_{m-k-1}}ss_{j_{k+2}}\dots s_{j_n}$, donde s es la subpalabra obtenida de la yuxtaposición de $s_{i_{m-k}}$ y $s_{j_{k+1}}$ tal como fue definida en la página 11.

En esta definición se supone implícitamente que los grupos G y H son disjuntos. Esto no constituye pérdida alguna de generalidad puesto que siempre es posible forzar esta condición mediante un simple truco conjuntista.

Note que los grupos G y H son subgrupos de $G * H$.

Si G tiene presentación $\langle S_G | R_G\rangle$ y H tiene presentación $\langle S_H | R_H\rangle$, entonces una presentación de $G * H$ es $\langle S_G \cup S_H | R_G \cup R_H\rangle$

Ejemplo 19. El grupo $\mathbb{Z}_2$ tiene presentación $\langle a|a^2\rangle$ y el grupo $\mathbb{Z}_3$ tiene presentación $\langle b|b^3\rangle$, entonces $\mathbb{Z}_2 * \mathbb{Z}_3$ tiene presentación $\langle a, b|a^2, b^3\rangle$. ◇

Con la siguiente discusión, acerca de factorizaciones en un grupo y su clasificación, concluimos la introducción de los elementos necesarios de la teoría de grupos para abordar el estudio del tema central de este trabajo: el problema de clasificación de factorizaciones especiales en $SL(2, \mathbb{Z})$.

Definición 24 (Factorización en un grupo, producto de una factorización y factorización de un elemento)**.** Sea $(G, \cdot)$ un grupo. Una factorización en G es una n-tupla $(g_1, \dots, g_n)$ (con $n \geqslant 0$) de elementos de G. Hay una única 0-tupla que es el conjunto vacío. Llamamos producto de la factorización $(g_1, \dots, g_n)$ al elemento $g_1 \cdots g_n$ de G. El producto de la factorización vacía se define como el

elemento identidad de G. Decimos que $(g_1,\ldots,g_n)$ es una factorización de g si su producto es g.

Definición 25 (Cambio de Hurwitz)**.** Dado un grupo $(G,\cdot)$ y una factorización en G, $(g_1,g_2,\ldots,g_n)$, decimos que se efectúa un cambio de Hurwitz si

$$(g_1,\ldots,g_i,g_{i+1},\ldots,g_n)\mapsto(g_1,\ldots,g_{i-1},g_ig_{i+1}g_i^{-1},g_i,g_{i+2},\ldots,g_n)$$

ó

$$(g_1,\ldots,g_i,g_{i+1},\ldots,g_n)\mapsto(g_1,\ldots,g_{i-1},g_{i+1},g_{i+1}^{-1}g_ig_{i+1},g_{i+2},\ldots,g_n)\,.$$

En el primer caso diremos que se efectuó un cambio de *Hurwitz a la izquierda*, y en el segundo que se efectuó un cambio de *Hurwitz a la derecha* en el $i-$ésimo par.

Note que cada uno es el inverso del otro. Es importante observar que si $(g_1',\ldots,g_m')$ se obtiene de $(g_1,\ldots,g_n)$ por aplicación sucesiva de cambios de Hurwitz, entonces $n=m$ y $g_1'\ldots g_n'=g_1\ldots g_n$, es decir, su producto es igual.

Ejemplo 20. En el grupo $\langle a,b|a^2,b^3\rangle$, dada la factorización (a,b^2,a,b,a^2,b), al realizar un cambio de Hurwitz a la derecha sobre el tercer par, se obtiene (a,b^2,b,b^2ab,a^2,b).

Note que si $g=ab^2aba^2b$ y $g'=ab^2[(b)(b^2ab)]a^2b=ab^2[(bb^2)ab]a^2b=ab^2(ab)a^2b$, entonces g y g' son iguales. ◇

Existen dos relaciones de equivalencia muy naturales que se pueden definir en un conjunto de factorizaciones de un grupo.

Definición 26. Sean $(g_1,\ldots,g_n)$ y $(g_1',\ldots,g_n')$ dos factorizaciones en un grupo G. Decimos que éstas son *Hurwitz equivalentes*, lo cual denotamos como $(g_1,\ldots,g_n)\equiv_H(g_1',\ldots,g_n')$, si existe una secuencia finita de cambios de Hurwitz que transforma la primera en la segunda. Decimos que éstas son equivalentes, lo cual denotamos como $(g_1,\ldots,g_n)\equiv(g_1',\ldots,g_n')$, si existe un elemento de $g\in G$ tal que $(g_1',\ldots,g_n')$ es Hurwitz equivalente a $(gg_1g^{-1},\ldots,gg_ng^{-1})$.

Proposición 2. *Las relaciones $\equiv_H$ y $\equiv$ son relaciones de equivalencia.*

Prueba. Sea $F=\{\alpha:\alpha$ es una factorización de un $g\in G\}$ y permítase a $H_i:F\to F$ denotar un movimiento de Hurwitz a la derecha sobre los factores i e $i+1$, entonces:

- Si a cualquier factorización α de g se le realiza un H_i y seguidamente un H_i^{-1}, donde H_i^{-1} denota un cambio de Hurwitz a la izquierda, se obtiene la factorización original, por lo tanto, $\alpha \equiv_H \alpha$.

- Si α_1 es Hurwitz equivalente a α_2 mediante una secuencia finita de movimientos de Hurwitz $H_{i_1}^{\delta_1} H_{i_2}^{\delta_2} \dots H_{i_n}^{\delta_n}$, con $\delta_i \in \{-1, 1\}$ y $H_{i_j}^1 = H_{i_j}$, entonces la secuencia $H_{i_n}^{-\delta_n} \dots H_{i_2}^{-\delta_2} H_{i_1}^{-\delta_1}$ sobre α_2, convierte α_2 en α_1. Por lo tanto, si $\alpha_1 \equiv_H \alpha_2$ entonces $\alpha_2 \equiv_H \alpha_1$.

- Sean $\alpha_1, \alpha_2, \alpha_3$ tres factorizaciones de g tales que $\alpha_1 \equiv_H \alpha_2$ mediante una secuencia finita de movimientos de Hurwitz $H_{i_1}^{\delta_1} H_{i_2}^{\delta_2} \dots H_{i_n}^{\delta_n}$, y $\alpha_2 \equiv_H \alpha_3$ mediante una secuencia finita de movimientos de Hurwitz $H_{j_1}^{\lambda_1} H_{j_2}^{\lambda_2} \dots H_{j_m}^{\lambda_m}$, entonces $\alpha_1 \equiv_H \alpha_3$ mediante la secuencia $H_{i_1}^{\delta_1} H_{i_2}^{\delta_2} \dots H_{i_n}^{\delta_n} H_{j_1}^{\lambda_1} H_{j_2}^{\lambda_2} \dots H_{j_m}^{\lambda_m}$. Por tanto, si $\alpha_1 \equiv_H \alpha_2$ y $\alpha_2 \equiv_H \alpha_3$ entonces $\alpha_1 \equiv_H \alpha_3$.

Luego, la relación $\equiv_H$ es reflexiva, simétrica y transitiva, lo que implica que es una relación de equivalencia.

De manera similar se puede verificar que $\equiv$ es relación de equivalencia. □

Es importante observar que si dos factorizaciones son equivalentes, entonces son Hurwitz equivalentes.

Concluimos esta unidad diciendo que, de ahora en adelante, siempre que no se presente confusión, al elemento identidad de un grupo lo denotaremos como 1.

Unidad 2

Problema de clasificación de factorizaciones especiales en $SL(2,\mathbb{Z})$ y su reducción a un problema análogo en G

2.1 Motivación y enunciado del problema

Sea D^2 el disco cerrado $\{z \in \mathbb{C} : |z| \leqslant 1\}$ dotado de su orientación estándar.

Definición 27. Una *fibración elíptica topológica sobre el disco* es una función suave $f : X \to D^2$, tal que:

1. f es sobreyectiva;
2. X es una $4-$variedad suave con frontera compacta, orientada y conexa;
3. $f(intX) = intD^2$ y $f(\partial X) = \partial D^2$;
4. f tiene un número finito (posiblemente cero) de valores críticos $q_1, \ldots, q_k$, y todos están en $intD^2$;
5. f es localmente holomorfa, es decir, para cada $p \in intX$ existen cartas orientación preservantes alrededor de p y $f(p)$, que van a abiertos de $\mathbb{C}^2$ y de $\mathbb{C}$ (dotados de la orientación estándar) respecto a las cuales f es holomorfa;

6. la preimagen de cada valor regular es una 2−variedad suave cerrada, orientable y conexa, de género 1.

Definición 28. Dos fibraciones elípticas topológicas sobre el disco $f : X \to D^2$ y $g : Y \to D^2$ se dice que son *topológicamente equivalentes* si existen difeomorfismos $H : X \to Y$ y $h : D^2 \to D^2$ que preservan orientación, tales que $h \circ f = g \circ H$.

Definición 29. Una fibración elíptica topológica sobre el disco $f : X \to D^2$ se dice que es:

1. *Relativamente minimal* si ninguna de sus fibras contiene una esfera embebida cuya auto–intersección es -1.

2. *De Lefschetz estricta* si es relativamente minimal y para cada punto crítico p (necesariamente contenido en $intX$) de f existen cartas alrededor de p y $f(p)$ como en la condición 5 de la definición 27, en las que f toma la forma $(z_1, z_2) \to z_1^2 + z_2^2$ y, además, f es inyectiva cuando se restringe al conjunto de todos los puntos críticos. A una fibración elíptica topológica sobre el disco que es de Lefschetz estricta la abreviamos por FETLE.

Es importante observar que estas dos propiedades, la relativa minimalidad y el ser de Lefschetz estricta, son preservadas por la equivalencia topológica.

Consideremos ahora el grupo $SL(2,\mathbb{Z})$ formado por las matrices 2×2 con entradas enteras y determinante uno. Sea

$$\mathsf{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

y sea S el conjunto de todas las matrices conjugadas de T, es decir, el conjunto de todas las matrices de la forma $\mathsf{A}^{-1}\mathsf{T}\mathsf{A}$ con $\mathsf{A} \in SL(2,\mathbb{Z})$.

Definición 30. Llamaremos *factorización especial* a cada factorización en $SL(2,\mathbb{Z})$ cuyas entradas pertenecen a S, es decir, a cada elemento de

$$\mathcal{F} := \cup_{r \geqslant 0} S^r \,,$$

donde S^r denota el producto cartesiano de S consigo mismo r veces, y S^0 se toma, por definición, como el conjunto cuyo único elemento es $\emptyset$. Una factorización especial $(\mathsf{G}_1, \ldots, \mathsf{G}_r)$ se dice que es una *factorización especial de* $\mathsf{B} \in SL(2,\mathbb{Z})$ si además satisface $\mathsf{G}_1 \ldots \mathsf{G}_r = B$. Por definición, a $\emptyset$ se le considerará una factorización especial de la matriz identidad I_2.

Recordemos, por la proposicion 2, que en cualquier conjunto de factorizaciones de un grupo dado G se pueden definir dos relaciones de equivalencia, las cuales denotamos como $\equiv_H$ y $\equiv$. Entonces podemos considerar los conjuntos de clases de equivalencia $\mathcal{F}/\equiv_H$ y $\mathcal{F}/\equiv$.

Proposición 3. *Existe una regla que asigna a cada fibración elíptica topológica sobre el disco de Lefschetz estricta (FETLE) un único elemento de $\mathcal{F}/\equiv$. Dicha regla es sobreyectiva y tiene la propiedad de que dos FETLE son topológicamente equivalentes si y sólo si tienen la misma imagen en $\mathcal{F}/\equiv$.*

Lo que esto significa es que el problema de clasificación, excepto por equivalencia topológica de las FETLEs, es equivalente al problema de describir a $\mathcal{F}/\equiv$. Un subconjunto $\mathcal{R}$ de $\mathcal{F}$ con la propiedad de que cada elemento de $\mathcal{F}/\equiv$ es representado por exactamente un elemento de $\mathcal{R}$, junto con un mecanismo que, para cada elemento de $\mathcal{F}$ nos diga a cuál de los elementos de $\mathcal{R}$ es equivalente, sería una descripción completa de $\mathcal{F}/\equiv$. El problema correspondiente para el conjunto $\mathcal{F}/\equiv_H$ puede ser considerado como parte sustancial del problema de describir a $\mathcal{F}/\equiv$.

Consideremos ahora la *función producto* $p : \mathcal{F} \to SL(2,\mathbb{Z})$ definida por $p(\mathsf{G}_1,\ldots,\mathsf{G}_r) = \mathsf{G}_1 \ldots \mathsf{G}_r$ que le asigna cada factorización su producto, es decir, el elemento de $SL(2,\mathbb{Z})$ del cual es factorización. La función p es claramente constante en cada clase de equivalencia bajo $\equiv_H$. Esto hace que la función p determine una función $\overline{p} : \mathcal{F}/\equiv_H \to SL(2,\mathbb{Z})$. El problema de describir a $\mathcal{F}/\equiv_H$ puede entonces organizarce de la siguiente forma: para cada $\mathsf{B} \in SL(2,\mathbb{Z})$ se define $\mathcal{F}(\mathsf{B}) := p^{-1}(\mathsf{B})$ y entonces

$$\mathcal{F} \;=\; \coprod_{\mathsf{B}\in SL(2,\mathbb{Z})} \mathcal{F}(\mathsf{B})$$

y

$$\mathcal{F}/\equiv_H \;=\; \coprod_{\mathsf{B}\in SL(2,\mathbb{Z})} (\mathcal{F}(\mathsf{B})/\equiv_H) \ .$$

Esto significa que para describir a $\mathcal{F}/\equiv_H$ basta describir $\mathcal{F}(\mathsf{B})/\equiv_H$ para cada $\mathsf{B} \in SL(2,\mathbb{Z})$.

El problema al que damos solución en este trabajo es el de dar una descripción parcial de $\mathcal{F}(\mathsf{B})/\equiv_H$ para cada $\mathsf{B} \in SL(2,\mathbb{Z})$. Específicamente, se propone un algoritmo que para un $\mathsf{B} \in SL(2,\mathbb{Z})$ dado, encuentra una colección $\mathcal{R}(\mathsf{B})$

de factorizaciones especiales de B *con la propiedad de que toda factorización especial de* B *es Hurwitz equivalente a al menos una de las factorizaciones en* $\mathcal{R}(\mathsf{B})$.

El siguiente resultado, debido a Livne [4], provee una descripción completa de $\mathcal{F}(\mathsf{I}_2)/\equiv_H$, donde I_2 es la matriz identidad 2×2.

Teorema 6 (Livne)**.** *Sean*

$$\mathsf{V}=\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix} \quad y \quad \mathsf{T}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},$$

entonces toda factorización especial de I_2 *es Hurwitz equivalente a una, y sólo una, de las factorizaciones*

$$\mathcal{R}(\mathsf{I}_2):=\Big\{\underbrace{(\mathsf{V},\mathsf{T},\ldots,\mathsf{V},\mathsf{T})}_{6s \text{ pares } \mathsf{V},\mathsf{T}} : s\geqslant 0\Big\}.$$

Además, existe un algoritmo que toma una factorización especial de I_2 *y encuentra una secuencia de movimientos de Hurwitz que la transforma en una de estas factorizaciones especiales particulares.*

Para un conocimiento más profundo de lo tratado en las siguientes secciones, puede consultarse [3, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24].

2.2 El grupo $SL(2,\mathbb{Z})$

En álgebra, geometría y teoría de números, entre otras áreas de las matemáticas avanzadas, aparece de forma natural la necesidad de estudiar el grupo de matrices llamado *Lineal Especial de grado dos*, $SL(2,\mathbb{Z})$ (*Special linear*), que consiste en el conjunto de matrices invertibles de dimensión 2×2 con entradas en los enteros y determinante igual a uno.

Teorema 7. $SL(2,\mathbb{Z})$ *es un grupo bajo la operación multiplicación de matrices.*

Prueba. Sean $\mathsf{A},\mathsf{B},\mathsf{C}\in SL(2,\mathbb{Z})$, entonces:

① Puesto que $\det(\mathsf{AB})=\det(\mathsf{A})\det(\mathsf{B})=1\times 1=1$, y puesto que cada entrada de AB, que es de dimensión 2×2, es entera, entonces $\mathsf{AB}\in SL(2,\mathbb{Z})$.

② Por las propiedades de multiplicación de matrices, sabemos que $\mathsf{A}(\mathsf{BC}) = (\mathsf{AB})\mathsf{C}$.

③ $\exists$ un $1 \in SL(2,\mathbb{Z})$ tal que $\forall \mathsf{A} \in SL(2,\mathbb{Z})$ se cumple que $\mathsf{A}1 = 1\mathsf{A} = \mathsf{A}$. Tal elemento es $\mathsf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

④ $\forall \mathsf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}), \exists \mathsf{A}^{-1} \in SL(2,\mathbb{Z})$, tal que $\mathsf{A}\mathsf{A}^{-1} = \mathsf{A}^{-1}\mathsf{A} = \mathsf{I}_2$. Tal elemento es $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

□

Discutiremos ahora la estructura del grupo $SL(2,\mathbb{Z})$, mostrando que él es generado por dos elementos particulares.

Teorema 8. *Las matrices* $\mathsf{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *y* $\mathsf{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *generan a* $SL(2,\mathbb{Z})$. *Más aún, cada elemento en* $SL(2,\mathbb{Z})$ *puede expresarse como un producto de potencias positivas de* S *y* T.

Prueba. Sea G el subgrupo de $SL(2,\mathbb{Z})$ generado por S y T. Probaremos que $G = SL(2,\mathbb{Z})$.

① Si $\mathsf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ se tiene:
$\mathsf{SA} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$, $\quad \mathsf{T}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ y $\quad \mathsf{T}^n\mathsf{A} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$.
Observe que la premultiplicación por S intercambia las filas de A cambiando el signo de la primera fila para preservar el determinante; y la premultiplicación por T^n suma n veces la fila 2 a la fila 1 en A.

② Si $c = 0$ entonces $\mathsf{A} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \mathsf{T}^b$ ó $\mathsf{A} = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = \mathsf{S}^2\mathsf{T}^{-b}$ y queda probado.

③ Si $c \neq 0$ entonces ejecute el algoritmo de división de Euclides sobre la primera columna de A hasta obtener en ella $(\pm 1, 0)^t$, de la siguiente forma:
$i \leftarrow 0$ donde el símbolo $\leftarrow$ significa *asigne a*
$\mathsf{A}_i \leftarrow \mathsf{A}$ con $\mathsf{A}_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$

Si $|a_0| < |c_0|$ **entonces**
$\mathsf{A}_0 \leftarrow \mathsf{S}\mathsf{A}_0$
Fin **si**
Mientras que $\mathsf{A}_i(col1) \neq (\pm 1, 0)^t$ **haga**
Determine un q_i tal que $a_i = q_i c_i + r_i$, donde $0 \leqslant r_i < |c_i|$;
$\mathsf{A}_{i+1} \leftarrow \mathsf{T}^{-q_i}\mathsf{A}_i$;
$\mathsf{A}_{i+2} \leftarrow \mathsf{S}\mathsf{A}_{i+1}$;
$i \leftarrow i + 2$;
Fin **mientras que**

El algoritmo siempre termina en $(\pm 1, 0)^t$ en la primera columna puesto que si $x|a$ y $x|c$ entonces $x|ad - bc = 1$, luego $x = \pm 1$, es decir, el máximo común divisor entre a y c es ± 1 porque el algoritmo de Euclides produce el máximo común divisor de a y c. Esto se cumple no solamente en A sino también para cada A_i por haber sido obtenida mediante otra matriz con determinante igual a uno.

④ Al concluir el paso ③ se tienen las condiciones dadas en ②, es decir: $\mathsf{A}_i = \begin{pmatrix} 1 & b_i \\ 0 & 1 \end{pmatrix}$, luego $\mathsf{A}_{i+1} = \mathsf{T}^{-b_i}\mathsf{A}_i = \mathsf{I}_2$; ó $\mathsf{A}_i = \begin{pmatrix} -1 & b_i \\ 0 & -1 \end{pmatrix}$, en cuyo caso $\mathsf{A}_{i+1} = \mathsf{T}^{b_i}\mathsf{A}_i$ y $\mathsf{A}_{i+2} = \mathsf{S}^2\mathsf{A}_{i+1} = \mathsf{I}_2$.

Puesto que lo que se realizó fue transformar la matriz A en la matriz identidad mediante una serie de operaciones elementales fila, entonces, la multiplicación de los S, S^2 y T en orden inverso al que fueron determinados en el algoritmo, es igual a A^{-1}. Luego A es igual al inverso de dicha multiplicación.

Ahora, considerando que $\mathsf{S}^{-1} = \mathsf{S}^3$, y que $\mathsf{T}^{-1} = \mathsf{S}^3\mathsf{T}\mathsf{S}\mathsf{T}\mathsf{S}$, cualquier $\mathsf{A} \in SL(2,\mathbb{Z})$ puede ser expresada como un producto de potencias positivas de S y T. □

Ejemplo 21. Tomemos $\mathsf{A} = \begin{pmatrix} 5 & 2 \\ 17 & 7 \end{pmatrix}$ y expresémoslo en términos de potencias (positivas y negativas) de S, T.

Solución. El algoritmo aplicado a A tomaría las siguientes acciones:

$$\mathsf{A}_0 = \mathsf{S}\mathsf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 2 \\ 17 & 7 \end{pmatrix} = \begin{pmatrix} -17 & -7 \\ 5 & 2 \end{pmatrix}$$

$$\mathsf{A}_1 = \mathsf{T}^4\mathsf{A}_0 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -17 & -7 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$$

$$\mathsf{A}_2 = \mathsf{S}\mathsf{A}_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} -5 & -2 \\ 3 & 1 \end{pmatrix}$$

$$\mathsf{A}_3 = \mathsf{T}^2\mathsf{A}_2 = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\begin{pmatrix}-5 & -2\\ 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}$$
$$\mathsf{A}_4 = \mathsf{S}\mathsf{A}_3 = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix} = \begin{pmatrix}-3 & -1\\ 1 & 0\end{pmatrix}$$
$$\mathsf{A}_5 = \mathsf{T}^3\mathsf{A}_4 = \begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}\begin{pmatrix}-3 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$
$$\mathsf{A}_6 = \mathsf{S}\mathsf{A}_5 = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$
$$\mathsf{A}_7 = \mathsf{S}^2\mathsf{A}_6 = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Lo anterior implica que

$$\begin{aligned}\mathsf{I}_2 &= \mathsf{S}^2\mathsf{A}_6\\ &= \mathsf{S}^2\mathsf{S}\mathsf{A}_5\\ &= \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{A}_4\\ &= \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{S}\mathsf{A}_3\\ &= \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{S}\mathsf{T}^2\mathsf{A}_2\\ &= \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{S}\mathsf{T}^2\mathsf{S}\mathsf{A}_1\\ &= \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{S}\mathsf{T}^2\mathsf{S}\mathsf{T}^4\mathsf{A}_0\\ &= \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{S}\mathsf{T}^2\mathsf{S}\mathsf{T}^4\mathsf{S}\mathsf{A}.\end{aligned}$$

Como $\mathsf{A}^{-1}\mathsf{A} = \mathsf{I}_2$, entonces $\mathsf{A}^{-1} = \mathsf{S}^2\mathsf{S}\mathsf{T}^3\mathsf{S}\mathsf{T}^2\mathsf{S}\mathsf{T}^4\mathsf{S} = \mathsf{S}^3\mathsf{T}^3\mathsf{S}\mathsf{T}^2\mathsf{S}\mathsf{T}^4\mathsf{S}$, luego $\mathsf{A} = \mathsf{S}^{-1}\mathsf{T}^{-4}\mathsf{S}^{-1}\ \mathsf{T}^{-2}\mathsf{S}^{-1}\mathsf{T}^{-3}\mathsf{S}^{-3}$. ◇

Corolario 1. *El grupo $SL(2,\mathbb{Z})$ es generado por dos matrices de orden finito.*

Prueba. $SL(2,\mathbb{Z}) = \langle \mathsf{S}, \mathsf{T}\rangle = \langle \mathsf{S}, \mathsf{S}\mathsf{T}\rangle$ donde

$$\mathsf{S} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \text{ es de orden cuatro y}$$
$$\mathsf{R} = \mathsf{S}\mathsf{T} = \begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix} \text{ es de orden seis.}$$ □

2.3 El grupo modular y reducción del problema a este grupo

El problema objeto de este trabajo será resuelto inicialmente no en $SL(2,\mathbb{Z})$, sino en un cociente muy simple de este grupo al cual se le llama grupo modular.

Definición 31 (Grupo modular)**.** Se llama grupo modular al cociente $SL(2,\mathbb{Z})/\{\mathsf{I}_2, -\mathsf{I}_2\}$. Al grupo modular se le denota usualmente como $PSL(2,\mathbb{Z})$, pero en el texto lo denotaremos como G_m.

Pasamos ahora a ver cómo el problema se puede reducir a un problema análogo en el grupo modular.

Denotemos por $\pi : SL(2,\mathbb{Z}) \to G_m$ al homomorfismo canónico, es decir, el que envía a cada elemento $\mathsf{A} \in SL(2,\mathbb{Z})$ en su clase de equivalencia $\bar{\mathsf{A}} = \{\mathsf{A}, -\mathsf{A}\}$.

Definición 32 (Levantamiento de una factorización especial)**.** Sea $\alpha = (g_1, \ldots, g_n)$ una factorización especial en G_m, es decir, tal que cada g_i es conjugado de $\bar{\mathsf{T}}$, con

$$\mathsf{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Una factorización especial $(\mathsf{A}_1, \ldots, \mathsf{A}_n)$ en $SL(2,\mathbb{Z})$ se dice que es un levantamiento de $(g_1, \ldots, g_n)$, si $\pi(\mathsf{A}_i) = g_i$ para cada i. Al levantamiento de una factorización especial α lo denotaremos como $lev(\alpha)$.

Observemos que si cada $g_i \in G_m$ es conjugado de $\bar{\mathsf{T}}$ entonces exactamente una de las dos preimágenes bajo π de g_i es conjugada de T. En efecto, supongamos que $g_i = h^{-1}\bar{\mathsf{T}}h$. Como π es sobreyectivo existe $\mathsf{B} \in SL(2,\mathbb{Z})$ tal que $\pi(\mathsf{B}) = h$. Por tanto $g = \pi(\mathsf{B})^{-1}\pi(\mathsf{T})\pi(\mathsf{B}) = \pi(\mathsf{B}^{-1}\mathsf{T}\mathsf{B})$ y vemos que g tiene al menos una preimagen que es un conjugado de T. La otra preimagen es $-\mathsf{B}^{-1}\mathsf{T}\mathsf{B}$, la cual no puede ser conjugado de T debido a que matrices conjugadas tienen trazas iguales, y

$$traza(-\mathsf{B}\mathsf{T}\mathsf{B}^{-1}) = -traza(\mathsf{B}\mathsf{T}\mathsf{B}^{-1}) = -traza(\mathsf{T}) = -2\,.$$

Esto nos permite hacer la siguiente afirmación.

Proposición 4. *Cada factorización especial en G_m tiene un único levantamiento.*

Teorema 9. *Sean $(\mathsf{T}_1, \ldots, \mathsf{T}_n)$ y $(\mathsf{T}'_1, \ldots, \mathsf{T}'_m)$ dos factorizaciones especiales en $SL(2,\mathbb{Z})$, es decir, tales que cada T_i y cada T'_j es conjugada de la matriz*

$$\mathsf{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Entonces estas factorizaciones son Hurwitz equivalentes si y sólo si $n = m$ y las factorizaciones $(\pi(\mathsf{T}_1), \ldots, \pi(\mathsf{T}_n))$ y $(\pi(\mathsf{T}'_1), \ldots, \pi(\mathsf{T}'_m))$ en G_m son Hurwitz equivalentes.

Prueba. Empecemos demostrando la necesidad de las dos condiciones. Si $(\mathsf{T}_1, \ldots, \mathsf{T}_n)$ y $(\mathsf{T}'_1, \ldots, \mathsf{T}'_m)$ son Hurwitz equivalentes, entonces, como se había observado inmediatamente después de la definición 25, se cumple la primera condición. Para ver que la segunda condición también se cumple basta observar que los cambios de Hurwitz conmutan con tomar la imagen bajo π. De manera precisa, si $(\mathsf{A}_1, \ldots, \mathsf{A}_n)$ es una factorización en $SL(2,\mathbb{Z})$, entonces se obtiene la misma factorización en G_m aplicando un movimiento de Hurwitz H y luego tomando π a cada entrada, que tomando primero π a cada entrada y luego aplicando el movimiento H. En efecto, si tomamos por ejemplo H como H_i, la primera manera transforma a $(\mathsf{A}_1, \ldots, \mathsf{A}_n)$ en

$$(\mathsf{A}_1, \ldots, \mathsf{A}_{i-1}, \mathsf{A}_{i+1}, \mathsf{A}_{i+1}^{-1}\mathsf{A}_i\mathsf{A}_{i+1}, \mathsf{A}_{i+2}, \ldots, \mathsf{A}_n)$$

y a ésta en

$$\begin{aligned}&(\pi(\mathsf{A}_1), \ldots, \pi(\mathsf{A}_{i-1}), \pi(\mathsf{A}_{i+1}), \pi(\mathsf{A}_{i+1}^{-1}\mathsf{A}_i\mathsf{A}_{i+1}), \pi(\mathsf{A}_{i+2}), \ldots, \pi(\mathsf{A}_n))\\ &\quad = (\pi(\mathsf{A}_1), \ldots, \pi(\mathsf{A}_{i-1}), \pi(\mathsf{A}_{i+1}), \pi(\mathsf{A}_{i+1})^{-1}\pi(\mathsf{A}_i)\pi(\mathsf{A}_{i+1}), \pi(\mathsf{A}_{i+2}), \ldots, \pi(\mathsf{A}_n))\,.\end{aligned}$$

La segunda manera transforma a $(\mathsf{A}_1, \ldots, \mathsf{A}_n)$ en $(\pi(\mathsf{A}_1), \ldots, \pi(\mathsf{A}_n))$ y a ésta en

$$(\pi(\mathsf{A}_1), \ldots, \pi(\mathsf{A}_{i-1}), \pi(\mathsf{A}_{i+1}), \pi(\mathsf{A}_{i+1})^{-1}\pi(\mathsf{A}_i)\pi(\mathsf{A}_{i+1}), \pi(\mathsf{A}_{i+2}), \ldots, \pi(\mathsf{A}_n))\,.$$

De manera similar se verifica en el caso en que H es un movimiento de Hurwitz izquierdo.

Pasamos ahora a demostrar la suficiencia de las condiciones. Supongamos que tenemos dos factorizaciones $\alpha = (\mathsf{T}_1, \ldots, \mathsf{T}_n)$ y $\alpha' = (\mathsf{T}'_1, \ldots, \mathsf{T}'_n)$ en $SL(2,\mathbb{Z})$, que suponemos tienen la misma longitud por la primera condición. Supongamos que $\beta = (\pi(\mathsf{T}_1), \ldots, \pi(\mathsf{T}_n))$ y $\beta' = (\pi(\mathsf{T}'_1), \ldots, \pi(\mathsf{T}'_n))$ son Hurwitz equivalentes. Entonces existe una sucesión de movimientos de Hurwitz $H_{i_1}^{\delta_1}, H_{i_2}^{\delta_2}, \ldots, H_{i_k}^{\delta_k}$ con cada $\delta_i \in \{-1, 1\}$, tal que $H_{i_k}^{\delta_k} \ldots H_{i_2}^{\delta_2} H_{i_1}^{\delta_1}(\beta) = \beta'$. Como vimos en la demostración de la necesidad de las condiciones, si hacemos un movimiento de Hurwitz H a una factorización $(\mathsf{A}_1, \ldots, \mathsf{A}_n)$ en $SL(2,\mathbb{Z})$, obtenemos una nueva factorización cuya imagen bajo π es precisamente la factorización que se obtiene haciendo el mismo movimiento de Hurwitz H a la imagen bajo π de $(\mathsf{A}_1, \ldots, \mathsf{A}_n)$. Esto nos dice que la imagen bajo π de la factorización $H_{i_k}^{\delta_k} \ldots H_{i_2}^{\delta_2} H_{i_1}^{\delta_1}(\alpha)$, es $\beta' = (\pi(\mathsf{T}'_1), \ldots, \pi(\mathsf{T}'_n))$. Si denotamos como $(\mathsf{T}''_1, \ldots, \mathsf{T}''_n)$ a $H_{i_k}^{\delta_k} \ldots H_{i_2}^{\delta_2} H_{i_1}^{\delta_1}(\alpha)$,

tenemos entonces que $\pi(\mathsf{T}_i'') = \pi(\mathsf{T}_i')$ para cada i. Esto a su vez dice que $\mathsf{T}_i'' \in \{\mathsf{T}_i', -\mathsf{T}_i'\}$ para cada i. Ahora, como cada una de las entradas de α es conjugada de la matriz T, y los movimientos de Hurwitz no alteran este hecho, cada una de las entradas de $(\mathsf{T}_1'', \ldots, \mathsf{T}_n'')$ es también conjugada de T. Pero se tiene que en el conjunto $\{\mathsf{T}_i', -\mathsf{T}_i'\}$ sólo la matriz T_i' es conjugada de T, debido a que $traza(-\mathsf{T}_i') = -traza(\mathsf{T}_i') = -traza(\mathsf{T}) = -2$. Concluimos que $\mathsf{T}_i'' = \mathsf{T}_i'$ para cada i, y por tanto que α y α' son Hurwitz equivalentes. □

Teorema 10. *Sea $\mathsf{B} \in SL(2,\mathbb{Z})$ arbitraria. Si $\mathcal{C}(\pi(\mathsf{B}))$ es una colección Hurwitz completa de factorizaciones especiales de $\pi(\mathsf{B})$, entonces la colección*

$$\mathcal{C}'(\mathsf{B}) := \{lev(\alpha) : \alpha \in \mathcal{C}(\pi(\mathsf{B}))\} \cap \mathcal{F}(\mathsf{B})$$

es una colección Hurwitz completa de factorizaciones especiales de B.

Prueba. Sea $\alpha = (\mathsf{T}_1, \ldots, \mathsf{T}_n)$ una factorización especial de B. Entonces $\alpha' = (\pi(\mathsf{T}_1), \ldots, \pi(\mathsf{T}_n))$ es una factorización especial de $\pi(\mathsf{B})$. Hay al menos una factorización β' en $\mathcal{C}(\pi(\mathsf{B}))$ que es Hurwitz equivalente a α'. Por el teorema 9 resulta que α es Hurwitz equivalente a $lev(\beta')$, y esta última claramente pertenece a $\mathcal{C}'(\mathsf{B})$ puesto que el producto de $lev(\beta')$ es B debido a que $lev(\beta')$ es Hurwitz equivalente a α y el producto de α es B. □

2.4 Presentación del grupo modular

Mostraremos ahora que G_m admite la presentación $\langle \omega, b | \omega^2, b^3 \rangle$.

Teorema 11. *El grupo modular G_m es isomorfo al grupo $\langle \omega, b | \omega^2, b^3 \rangle$.*

Prueba. Sean S y R las matrices definidas en la prueba del corolario 1, y sean $\bar{\mathsf{S}}$ y $\bar{\mathsf{R}}$ sus imágenes bajo el homomorfismo canónico $SL(2,\mathbb{Z}) \to G_m$. Resulta inmediato verificar que $\bar{\mathsf{S}}^2 = \bar{\mathsf{R}}^3 = \bar{\mathsf{I}}_2$, y $\langle \bar{\mathsf{S}}, \bar{\mathsf{R}} \rangle = G_m$.

Aplicando el teorema de Van Dyck, teorema 5, con $G = G_m$, $A = \{\bar{\mathsf{S}}, \bar{\mathsf{R}}\}$, $S = \{\omega, b\}$, donde ω y b se toman como símbolos, $\iota : S \to A$ definido como $\iota(\omega) = \bar{\mathsf{S}}$ y $\iota(b) = \bar{\mathsf{R}}$, y $R = \{\omega^2, b^3\}$, obtenemos la existencia de un epimorfismo $f : \langle \omega, b | \omega^2, b^3 \rangle \to G_m$, tal que $f(\omega N) = \bar{\mathsf{S}}$ y $f(bN) = \bar{\mathsf{R}}$.

A continuación demostramos que f es inyectiva y por tanto que es un isomorfismo, obteniendo así el resultado deseado.

En el resto de la demostración al elemento pN, donde p es una palabra en $\{\omega, b\}$ lo representaremos como $\bar{p}$. Observe que si $p, q \in F_S$, entonces $\overline{pq} = \bar{p}\bar{q}$.

Es fácil ver que todo elemento del grupo $\langle \omega, b | \omega^2, b^3 \rangle$ que no sea el elemento identidad se puede escribir como un producto $u_1 \dots u_n$ con $n \geqslant 1$, donde cada $u_i \in \{\bar{\omega}, \bar{b}, \bar{b}^2\}$ y, si $n \geqslant 2$, cada par $(u_i, u_{i+1}) \in \{(\bar{\omega}, \bar{b}), (\bar{\omega}, \bar{b}^2), (\bar{b}, \bar{\omega}), (\bar{b}^2, \bar{\omega})\}$. Al elemento identidad del grupo modular lo llamaremos *palabra vacía* y lo denotaremos como 1.

Para ver que f es inyectiva basta ver que $f(u_1 \dots u_n) \neq \bar{\mathsf{I}}_2$ para cada producto $u_1 \dots u_n$ de los descritos en el párrafo anterior. Esto equivale a verificar que un producto de la forma $U_1 \dots U_n$ con $n \geqslant 1$, donde cada $U_i \in \{\bar{\mathsf{S}}, \bar{\mathsf{R}}, \bar{\mathsf{R}}^2\}$, y si $n \geqslant 2$, cada par $(U_i, U_{i+1}) \in \{(\bar{\mathsf{S}}, \bar{\mathsf{R}}), (\bar{\mathsf{S}}, \bar{\mathsf{R}}^2), (\bar{\mathsf{R}}, \bar{\mathsf{S}}), (\bar{\mathsf{R}}^2, \bar{\mathsf{S}})\}$, no puede ser igual a $\bar{\mathsf{I}}_2$. Como $\bar{\mathsf{R}}, \bar{\mathsf{R}}^2 \neq \bar{\mathsf{I}}_2$ basta verificar que ningún producto de la forma

$$\mathsf{P} = \bar{\mathsf{R}}^{\lambda_1} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_n} \tag{2.1}$$

donde $n \geqslant 2$, $\lambda_1, \lambda_n \in \{0, 1, 2\}$ y $\lambda_i \in \{1, 2\}$ para $1 < i < n$, es igual a $\bar{\mathsf{I}}_2$. Entonces:

- Si $n = 2$ las posibilidades son $\bar{\mathsf{R}}^0 \bar{\mathsf{S}} \bar{\mathsf{R}}^0, \bar{\mathsf{R}}^0 \bar{\mathsf{S}} \bar{\mathsf{R}}^1, \bar{\mathsf{R}}^0 \bar{\mathsf{S}} \bar{\mathsf{R}}^2, \bar{\mathsf{R}}^1 \bar{\mathsf{S}} \bar{\mathsf{R}}^0, \bar{\mathsf{R}}^1 \bar{\mathsf{S}} \bar{\mathsf{R}}^1, \bar{\mathsf{R}}^1 \bar{\mathsf{S}} \bar{\mathsf{R}}^2$, $\bar{\mathsf{R}}^2 \bar{\mathsf{S}} \bar{\mathsf{R}}^0, \bar{\mathsf{R}}^2 \bar{\mathsf{S}} \bar{\mathsf{R}}^1$ ó $\bar{\mathsf{R}}^2 \bar{\mathsf{S}} \bar{\mathsf{R}}^2$. Se ve directamente que ninguno es igual a $\bar{\mathsf{I}}_2$.

- Supongamos ahora que existe algún producto $\bar{\mathsf{R}}^{\lambda_1} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_n}$ como en (2.1) con $n > 2$ necesariamente, que es igual a $\bar{\mathsf{I}}_2$. Supongamos que n es mínimo con esta propiedad, es decir, que no existe un producto $\bar{\mathsf{R}}^{\lambda_1} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_k}$ como en (2.1) y que sea igual a $\bar{\mathsf{I}}_2$, con $k < n$.

  Así

  $$\bar{\mathsf{R}}^{\lambda_1} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_n} = \bar{\mathsf{I}}_2 \,,$$

  con $n > 2$. Tenemos que

  $$\bar{\mathsf{R}}^{-\lambda_1} \left(\bar{\mathsf{R}}^{\lambda_1} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_n} \right) \bar{\mathsf{R}}^{\lambda_1} = \bar{\mathsf{R}}^{-\lambda_1} \bar{\mathsf{I}}_2 \bar{\mathsf{R}}^{\lambda_1} \,,$$
  $$\bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_n + \lambda_1} = \bar{\mathsf{I}}_2 \,.$$

Ahora, $\lambda_n + \lambda_1$ debe de ser diferente de cero módulo tres, puesto que si lo fuera se tendría que $\bar{\mathsf{S}} \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} \bar{\mathsf{S}} \bar{\mathsf{S}} = \bar{\mathsf{S}} \bar{\mathsf{I}}_2 \bar{\mathsf{S}}$, luego $\bar{\mathsf{R}}^{\lambda_2} \bar{\mathsf{S}} \dots \bar{\mathsf{S}} \bar{\mathsf{R}}^{\lambda_{n-1}} = \bar{\mathsf{I}}_2$, lo cual contradice la suposición acerca de la minimalidad de n. Concluimos que $\lambda_n + \lambda_1$ es igual a 1 o a 2. En ambos casos resulta que $\bar{\mathsf{I}}_2$ se puede escribir como un producto de la forma

$$g_1 \dots g_r \tag{2.2}$$

con $r > 1$ en el que cada $g_i \in \{\bar{\mathsf{S}} \bar{\mathsf{R}}, \bar{\mathsf{S}} \bar{\mathsf{R}}^2\}$. Veamos que esto también es imposible. El que exista un producto como en (2.2) es equivalente a que algún producto de

la forma $\mathsf{G}_1 \dots \mathsf{G}_r$ con $r > 1$ en el que cada $\mathsf{G}_i \in \{\mathsf{SR}, \mathsf{SR}^2\}$, sea igual a la matriz I_2 o a la matriz $-\mathsf{I}_2$.

Recordemos que las matrices S y R son

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

respectivamente, y por tanto

$$\mathsf{SR} = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \mathsf{SR}^2 = -\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Tenemos entonces que $\mathsf{G}_1 \dots \mathsf{G}_r = (-1)^r \mathsf{G}'_1 \dots \mathsf{G}'_r$ donde cada matriz G'_i es

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{ó} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Concluimos la demostración observando que el producto $\mathsf{G}'_1 \dots \mathsf{G}'_r$ no puede ser igual ni a I_2 ni a $-\mathsf{I}_2$. Esto se debe a que si

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

es una matriz cuyas entradas son enteros no negativos, y en la que las entradas que no están en la diagonal principal no son ambas cero, entonces los dos productos

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+a \\ c & d+c \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}$$

son también matrices cuyas entradas son no negativas y en que las entradas que no están en la diagonal principal no son ambos cero.

Se concluye que G_m tiene presentación $\langle \omega, b | \omega^2, b^3 \rangle$. □

2.5 Replanteamiento del problema en $G = \langle \omega | \omega^2 \rangle * \langle b | b^3 \rangle$

El grupo $\langle \omega, b | \omega^2, b^3 \rangle$ es isomorfo al producto libre $\langle \omega | \omega^2 \rangle * \langle b | b^3 \rangle$. Al grupo $\langle \omega | \omega^2 \rangle * \langle b | b^3 \rangle$ lo denotaremos, de acá en adelante, como G. El grupo $\langle \omega | \omega^2 \rangle$ consta de dos elementos, $\bar{\omega}$ y $\bar{\omega}^2$. Si denotamos a estos como ω y 1, respectivamente, su tabla de multiplicación es

$*$	1	ω
1	1	ω
ω	ω	1

De forma similar, el grupo $\langle b|b^3\rangle$ consta de tres elementos, $\bar{b}$, $\bar{b}^2$ y $\bar{b}^3$. Si denotamos a estos como b, b^2 y 1, respectivamente, su tabla de multiplicación es

$*$	1	b	b^2
1	1	b	b^2
b	b	b^2	1
b^2	b^2	1	b

De la definición de producto libre, definición 23, resulta que cada elemento de G *es* una palabra de la forma $t_1 \dots t_n$ con $n \geqslant 0$, donde cada $t_i \in \{\omega, b, b^2\}$ y, si $n \geqslant 2$, cada par $t_i t_{i+1} \in \{\omega b, \omega b^2, b\omega, b^2\omega\}$. Cuando $n = 0$ se tiene la palabra vacía que es el elemento identidad de G.

El isomorfismo $f : \langle \omega, b|\omega^2, b^3\rangle \to G_m$ obtenido en el teorema 11, induce un isomorfismo $\tilde{f} : G = \langle \omega|\omega^2\rangle * \langle b|b^3\rangle \to G_m$ vía el isomorfismo obvio entre $\langle \omega, b|\omega^2, b^3\rangle$ y G. Como f envía a $\bar{\omega}$ en $\bar{\mathsf{S}}$ y a $\bar{b}$ en $\bar{\mathsf{R}}$, entonces $\tilde{f}$ envía a ω en $\bar{\mathsf{S}}$ y a b en $\bar{\mathsf{R}}$. Como $\bar{\mathsf{T}} = \bar{\mathsf{S}}\bar{\mathsf{R}}$, entonces $\tilde{f}$ envía a ωb en $\bar{\mathsf{T}}$. Esto nos dice que el problema de encontrar una colección Hurwitz completa de factorizaciones especiales de un elemento de G_m dado es equivalente al problema de encontrar una colección Hurwitz completa de factorizaciones en términos de conjugados de ωb de un elemento de G dado.

Ahora, por razones técnicas, el problema en G debe ser traducido de nuevo en otro problema equivalente en G. Específicamente, sea $\phi : G \to G$ el automorfismo que envía a ω en ω y a b en b^2, y sea $c_b : G \to G$ el automorfismo que envía a cada elemento $g \in G$ en $bgb^{-1} = bgb^2$. La composición $h = c_b \circ \phi$ de estos automofismos es un automorfismo que envía a ωb en $b\omega b$. Entonces el problema de encontrar una colección Hurwitz completa de factorizaciones, en términos de conjugados de ωb, equivale al problema de encontrar una colección Hurwitz completa de factorizaciones en términos de conjugados de $b\omega b$. Es este último problema el que abordaremos a continuación.

2.6 Estudio del problema en G

Definición 33 (Longitud de g)**.** Si $g = t_1 \dots t_n$, entonces decimos que la longitud de g, denotada por $\ell(g)$, es n. Por definición, la longitud para la palabra vacía es $\ell(1) = 0$.

Ejemplo 22. Si $g = \omega b\omega b^2\omega b^2\omega$ entonces $\ell(g) = 7$.

De la definición de producto libre, definición 23, resulta que si $g = t_k \dots t_1$ y $g' = t'_1 \dots t'_l$ son elementos de G, entonces su *multiplicación* $g * g'$ es la expresión reducida

$$gg' = t_k \dots t_{m+1} r t'_{m+1} \dots t'_l \,,$$

donde $m \geqslant 0$ es la cantidad de sílabas, definición 19, de g que intervienen en la multiplicación, es decir, $t_i = t'^{-1}_i$ para $0 < i < m$, y $r = b^\delta$, $\delta \in \{0,1,2\}$. $\delta = 0$ cuando no ocurren cancelaciones ($b^0 = 1$), es decir, $gg' = t_k \dots t_1 t'_1 \dots t'_l$, o cuando $m = \text{mín}\{\ell(g), \ell(g')\}$, en cuyo caso $gg' = t_k \dots t_{l+1}$ ó $gg' = t'_{k+1} \dots t'_l$.

Definición 34. Cuando $m = 0$ se dice de cada elemento del conjunto $\{t_k, \dots, t_1, t'_1, \dots, t'_k\}$ que *no interviene en la multiplicación*. Si $0 < m < \text{mín}\{\ell(g), \ell(g')\}$, se dice de cada elemento del conjunto $\{t_k, \dots, t_{m+1}, t'_{m+1}, \dots, t'_l\}$ que *no interviene en la multiplicación*. Si $m = \text{mín}\{\ell(g), \ell(g')\}$ decimos de cada elemento del conjunto $\{t'_{m+1}, \dots, t'_l\}$ cuando $\ell(g) < \ell(g')$, y del conjunto $\{t_k, \dots, t_{m+1}\}$ cuando $\ell(g) > \ell(g')$, que *no interviene en la multiplicación*.

Ejemplo 23. Veamos algunas posibles situaciones:

- Sea $g = b^2\omega b\omega b\omega b^2\omega$ y $g' = \omega b\omega b^2\omega b\omega b\omega$. En este caso $m = 6$, $\ell(g) = 8$, $\ell(g') = 9$. Entonces $0 < m < \text{mín}\{\ell(g), \ell(g')\} = 8$. Tenemos entonces que

$$\begin{aligned} g * g' &= (b^2\omega b\omega b\omega b^2\omega) * (\omega b\omega b^2\omega b\omega b\omega) \\ &= b^2\omega(b * b)\omega b\omega \\ &= b^2\omega(b^2)\omega b\omega \,. \end{aligned}$$

  En este caso $r = b^2$.

- Sean $g = \omega b^2\omega$ y $g' = \omega b\omega b^2\omega$.

  En este caso $m = 3$, $\ell(g) = 3$, $\ell(g') = 5$. Entonces ocurre que $m = \text{mín}\{\ell(g), \ell(g')\}$ y $\ell(g) < \ell(g')$, y por tanto $g * g' = b^2\omega$.

- Sean $g = \omega b^2\omega$ y $g' = b\omega b$.

  En este caso $m = 0$ y entonces $g * g' = \omega b^2\omega b\omega b$. ◇

Afirmación 1. *Si se multiplican $g, g' \in G$, entonces su longitud es*

$$\ell(g * g') = \ell(g) + \ell(g') - 2m + \ell(r) \,,$$

donde m y r se definen como en la discusión anterior.

Prueba. Sean $g = t_k \dots t_1$ y $g' = t'_1 \dots t'_l$. Hay tres posibilidades:

- $m = 0$: ocurre cuando no hay alguna cancelación. En este caso $r = 1$ y entonces $\ell(r) = 0$. Por un lado $\ell(g * g') = k + l$ y $\ell(g) + \ell(g') - 2m + \ell(r) = k + l - 2(0) + 0 = k + l$.

- $m = \text{mín}\{k, l\}$: si $k < l$ entonces $m = k$ y $r = 1$. De aquí que $\ell(g) + \ell(g') - 2m + \ell(r) = k + l - 2k + 0 = l - k = \ell(g * g') = \ell(t_{k+1} \dots t_l)$. Si $k = l$ entonces $m = k$ y $r = 1$. Se tiene que $\ell(g) + \ell(g') - 2m + \ell(r) = k + l - 2k + 0 = l - k = 0 = \ell(g * g')$. Finalmente, si $l < k$ la demostración es similar a la del caso $k < l$.

- $1 < m < \text{mín}\{k, l\}$: en este caso $g * g' = t_k \dots t_{m+1} b^\delta t'_{m+1} \dots t'_l$, con $\delta \in \{1, 2\}$. En este caso $\ell(r = b^\delta) = 1$ y por tanto $\ell(g * g') = k + l - 2m + 1 = \ell(g) + \ell(g') - 2m + \ell(r)$. □

Definición 35 (Junta bien)**.** Un producto $g_1 * \cdots * g_n$ (o una factorización $(g_1, \dots, g_n)$) de elementos de G, se dice que junta bien, si para todo $1 \leqslant i \leqslant n-1$ se tiene que $\ell(g_i * g_{i+1}) \geqslant \text{máx}\{\ell(g_i), \ell(g_{i+1})\}$. Los productos (o factorizaciones) con $n = 1$ ó $n = 0$ (producto vacío o factorización vacía) se declaran como que juntan bien. En caso contrario, se dice que el producto (o la factorización) *junta mal*.

Ejemplo 24. En el ejemplo 23, en el tercer caso $\ell(g*g') = 6 \geqslant \text{máx}\{l(g), l(g')\} = 3$; por lo tanto el producto $g * g'$ junta bien. En cualquiera de los otros dos casos $g * g'$ junta mal. ◇

Denotemos como s_1 a $b\omega b \in G$ y como S al conjunto $\{g^{-1} * s_1 * g : g \in G\}$ formado por todos los conjugados de s_1. Tres conjugados especiales de s_1 son $s_0 = b^2 * s_1 * b = \omega b^2$, s_1 mismo, y $s_2 = b * s_1 * b^2 = b^2\omega$.

Definición 36. Los conjugados s_0, s_1 y s_2 son llamados *cortos*. Cualquier otro conjugado de s_1 es llamado *largo*.

Note que $\ell(s_0) = \ell(s_2) = 2$ y $\ell(s_1) = 3$.

Proposición 5. *Todo conjugado largo se puede escribir de manera única en la forma $Q^{-1} * s_1 * Q$ donde Q empieza por ω.*

Prueba. Dado un $g = g_1 \dots g_n \in G$, entonces:

① Sea $s = g^{-1} s_1 g$.

② Si $\ell(g) = 0$ entonces $g = 1 = Q$ y $s = s_1$, así queda probado.

③ Ahora, si $\ell(g) \geqslant 1$, observe los posibles conjugados de s_j, $j \in \{1,2,3\}$, $g_i \in \{\omega, b, b^2\}$, $1 \leqslant i \leqslant n$:

$$\begin{array}{lll} \omega s_0\omega = s_2 & b^2 s_0 b = s_2 & bs_0b^2 = s_1 \\ \omega s_1\omega = \omega s_1\omega & b^2 s_1 b = s_0 & bs_1b^2 = s_2 \\ \omega s_2\omega = s_0 & b^2 s_2 b = s_1 & bs_2b^2 = s_0\,, \end{array}$$

es decir, los posibles conjugados de $g_i^{-1} s_j g_i \in \{s_j\}$, excepto si $s_j = s_1$ y $g_i = \omega$.

④ De esta forma, si tenemos $s_j = s_1$ y $g_i = \omega$ entonces $Q = g_i \dots g_n$. Así, $s = Q^{-1}s_1Q$ y queda demostrada. Si no ocurre esto, entonces obtenemos un nuevo s_j y si $i = n$, queda demostrado; pero si $i < n$ se vuelve a ejecutar el paso ③ con el nuevo s_j y el siguiente g_i. Puesto que n es finito, el proceso acaba en algún s_j o con $s = Q^{-1}s_1Q$.

Para probar la unicidad, suponga que s puede ser escrito en forma reducida de dos formas diferentes de igual longitud, es decir, $s = Q^{-1}s_1Q = R^{-1}s_1R$ con $Q \neq R$, entonces $1 = ss^{-1} = (Q^{-1}s_1Q)(R^{-1}s_1R)^{-1} = (Q^{-1}s_1Q)(R^{-1}s_1^{-1}R)$. Lo que implica que $QR^{-1} = 1$, es decir, $Q = R$. Luego, la forma reducida de s es única. □

Ejemplo 25. Si $g = b^2\omega b\omega b^2\omega b$ entonces $g^{-1} = b^2\omega b\omega b^2\omega b$, luego

$$\begin{aligned} s &= g^{-1}s_1g \\ &= b^2\omega b\omega b^2\omega b s_1 b^2\omega b\omega b^2\omega b \\ &= b^2\omega b\omega b^2\omega s_2\omega b\omega b^2\omega b \\ &= b^2\omega b\omega b^2 s_0 b\omega b^2\omega b \\ &= b^2\omega b\omega s_2\omega b^2\omega b \\ &= b^2\omega b s_0 b^2\omega b \\ &= b^2\omega s_1\omega b\,. \end{aligned}$$

De esta forma $Q = \omega b$ y se verifica que $s = Q^{-1}s_1Q$. ◇

Esto nos dice que

$$S = \{s_0, s_1, s_2\} \cup \{Q^{-1} * s_1 * Q : Q \in G, \text{ donde } Q \text{ empieza por } \omega\}\,.$$

Note que cuando el conjugado largo está escrito de esta manera, su longitud es $2\ell(Q)+3$. En particular, la longitud de cualquier conjugado largo es un impar no menor que 5.

Definición 37 (Factorización especial)**.** Una factorización $(g_1,\dots,g_n)$ de g (o un producto $g_1 * \cdots * g_n = g$) es especial si cada $g_i \in S$.

La factorización vacía es entonces una factorización especial de 1.

Ejemplo 26. La 3−tupla $(b^2\omega,\ \omega b\omega b\omega,\ \omega b^2\omega b\omega b\omega b\omega)$ es una factorización especial de $g = b\omega b\omega b\omega$, pues $(b^2\omega) * (\omega b\omega b\omega) * (\omega b^2\omega b\omega b\omega b\omega) = g$. ◇

Observe que $s_2 * s_2 = b^2\omega b^2\omega$, $s_1 * s_1 = b\omega b^2\omega b$, $s_0 * s_0 = \omega b^2\omega b^2$, $s_2 * s_1 = b^2\omega b\omega b$, $s_1 * s_0 = b\omega b\omega b^2$ y $s_0 * s_2 = \omega b\omega$, lo que muestra que estos productos juntan bien; y que $s_0 * s_1 = s_1 * s_2 = s_2 * s_0 = b$, lo que muestra que estos productos juntan mal. Veamos a continuación otros casos donde (g, g'), con $g, g' \in S$, también juntan bien.

Proposición 6. *Dados $g, g' \in S$, si $\ell(g) = \ell(g') = k$, con k impar, entonces $g * g'$ junta bien.*

Prueba. Sean $g = P^{-1}s_1P$ y $g' = Q^{-1}s_1Q$, puesto que $\ell(g) = \ell(g') = k$ entonces $\ell(P) = \ell(Q) = \frac{k-3}{2}$. Se pueden presentar dos casos:

- Si $P = Q$ entonces $PQ^{-1} = 1$ y $gg' = (P^{-1}s_1P)(Q^{-1}s_1Q) = P^{-1}b\omega b^2\omega bQ$; luego $\ell(gg') = \frac{k-3}{2} + 5 + \frac{k-3}{2} = k+2$. Así, $\ell(gg') > k = \max\{\ell(g), \ell(g')\}$.
- Si $P \neq Q$ entonces $PQ^{-1} = t_1 \dots t_n \neq 1$, con $t_1 = t_n = \omega$; luego $gg' = (P^{-1}s_1P)(Q^{-1}s_1Q) = P^{-1}s_1t_1\dots t_ns_1Q$ con $\ell(t_1\dots t_n) > 2$; luego $\ell(gg') = \frac{k-3}{2} + 3 + \ell(t_1\dots t_n) + 3 + \frac{k-3}{2} = k + 3 + \ell(t_1\dots t_n) > k+5$. Así, $\ell(gg') > k = \max\{\ell(g), \ell(g')\}$. □

Corolario 2. *Sea $(g_1, g_2, \dots, g_n)$ con cada $g_i \in S$, si $\ell(g_1) = \ell(g_2) = \cdots = \ell(g_n) = k$, con k impar, entonces cada par (g_i, g_{i+1}), $i \in [1\dots n-1]$, junta bien.*

Ejemplo 27. Dados $g_1 = b\omega b^2\omega\underline{b\omega b}\omega b\omega b^2$, $g_2 = b\omega b\omega\underline{b\omega b}\omega b^2\omega b^2$ y $g_3 = b^2\omega b^2\omega\underline{b\omega b}\omega b\omega b$, tenemos que $g_1g_2 = b\omega b^2\omega\underline{b\omega b}\omega b^2\omega\underline{b\omega b}\omega b^2\omega b^2$ y $g_2g_3 = b\omega b\omega\underline{b\omega b}\omega b^2\omega b\omega b^2\omega\underline{b\omega b}\omega b\omega b$, y que $g_1g_2g_3 = b\omega b^2\omega\underline{b\omega b}\omega b^2\omega\underline{b\omega b}\omega b^2\omega b\omega b^2\omega\underline{b\omega b}\omega b\omega b$. Para una mejor lectura, se ha subrayado s_1 en cada g_i. ◇

Definición 38 (Centro de un conjugado)**.** Para cada $g \in S$ de la forma $Q^{-1}s_1Q$, donde $\ell(Q) \geqslant 0$, es decir, $\ell(g)$ impar, diremos que su centro es la sílaba $\omega \in s_1$. Los conjugados s_0 y s_2 se considerarán sin centro. Note que si $\ell(g) = k$, entonces la posición del centro en g es $\frac{k+1}{2}$.

Proposición 7. *Dados $g, g' \in S$ con $\ell(g)$ y $\ell(g')$ impares. Los conjugados g, g' juntan bien si y sólo si ninguno de sus centros intervienen en la multiplicación gg'.*

Prueba. Sean $\ell(g) = k$ y $\ell(g') = l$, $g = P^{-1}s_1P$ y $g' = Q^{-1}s_1Q$ donde $\ell(P) = \frac{k-3}{2}$ y $\ell(Q) = \frac{l-3}{2}$.

$\Rightarrow$

① $\ell(gg') \geqslant \text{máx}\{k, l\}$ por hipótesis.

② Suponga que $k \leqslant l$ y que, por contradicción, el centro de g interviene en la multiplicación de g y g'.

③ Sea m la cantidad de sílabas que intervienen en la multiplicación, entonces $m \geqslant \frac{k+3}{2}$.

④ Si $m = \frac{k+3}{2}$ entonces $\ell(gg') = k + l - 2\left(\frac{k+3}{2}\right) + 1 = l - 2 < \text{máx}\{k, l\} = l$ (en el caso $m < k$), ó $\ell(gg') = k + l - 2\left(\frac{k+3}{2}\right) = l - 3 < \text{máx}\{k, l\} = l$ (en el caso $m = k$), lo que, en ambos casos, implica una contradicción.

Se concluye que el centro de g no interviene en la multiplicación, y con mayor razón el centro de g' tampoco interviene puesto que $\frac{k+1}{2} \leqslant \frac{l+1}{2}$. Si $k > l$, el análisis es similar.

$\Leftarrow$

⑤ Por hipótesis los centros de g y g' no intervienen.

⑥ Suponga que $k < l$, entonces, si m es la cantidad de sílabas que intervienen en la multiplicación, $m \leqslant \frac{k-1}{2}$.

⑦ Si $m = \frac{k-1}{2}$ entonces $\ell(gg') = k + l - 2\left(\frac{k-1}{2}\right) + 1 = l + 2 > l = \text{máx}\{k, l\}$.

Se concluye que g y g' juntan bien. Si $k > l$ el análisis es similar. Si $k = l$, en la proposición 6 se probó que juntan bien. □

Corolario 3. *Sean $g_1, g_2, \ldots, g_n \in S$ cuyas longitudes $\ell(g_1), \ell(g_2), \ldots, \ell(g_n)$ son todas impares. El producto $g_1 * g_2 * \ldots * g_n$ junta bien si y sólo si ninguno de los centros de los g_i intervienen en la multiplicación.*

Ejemplo 28. Dados $g_1 = b\omega b^2\omega\underline{b\omega b}\omega b\omega b^2$, $g_2 = b\omega\underline{b\omega b}\omega b^2$ y $g_3 = \omega b^2\omega\underline{b\omega b}\omega b\omega$, tenemos que $g_1 * g_2 * g_3 = b\omega b^2\omega b\underline{\omega} b\omega b^2\underline{\omega} b\omega b^2\omega b^2\omega b\underline{\omega} b\omega b\omega$. Para una mejor lectura, se ha subrayado s_1 en cada g_i y el centro de cada uno en $g_1 * g_2 * g_3$. ◇

Proposición 8. *Dados $g, g' \in S$ con al menos uno de ellos de longitud par, $g * g'$ junta bien si y sólo si $m \in \{0, 1\}$, siendo m la cantidad de sílabas en g que intervienen en el producto $g * g'$.*

Prueba. Sean $g, g' \in S$ con $\ell(g) = k$ y $\ell(g') = l$, entonces:

$\Rightarrow$

① $g * g'$ junta bien por hipótesis

② Suponga que k es par y que $g' = t_1 t_2 \dots t_l$, entonces máx$\{k, l\} = l$:

- Si $g = s_0 = \omega b^2$, entonces $t_1 t_2 \neq b\omega$ puesto que si lo fuera, $g * g' = (\omega b^2)(b\omega t_3 \dots t_n) = t_3 \dots t_n$, luego $\ell(g * g') = l - 2$, lo cual contradice ① y ② (en este caso $m = 2$). Luego, $t_1 t_2 \in \{\omega b, \omega b^2\}$ ó $t_1 t_2 = b^2\omega$. En el primer caso $\ell(g*g') = l+2$ y $m = 0$; y en el segundo $\ell(g*g') = l+1$ y $m = 1$.
- Si $g = s_2 = b^2\omega$, entonces $t_1 \neq \omega$ puesto que si lo fuera, $\ell(g*g') = l-1$ ó $\ell(g*g') = l-2$, lo cual contradice ① y ② ($m = 2$). Luego, $t_1 \in \{b, b^2\}$ en cuyo caso $\ell(g * g') = l + 2$ y $m = 0$.

③ Suponga que l es par y que $g = t_1 t_2 \dots t_k$, entonces máx$\{k, l\} = k$: el análisis es similar.

$\Leftarrow$

④ $m = 0$ ó $m = 1$ por hipótesis

⑤ Suponga que k es par y que $g' = t_1 t_2 \dots t_l$, entonces máx$\{k, l\} = l$:

- Si $g = s_0 = \omega b^2$ y $m = 0$, entonces $t_1 = \omega$ ($t_1 \notin \{b, b^2\}$ puesto que, entonces $m > 0$), luego $\ell(g * g') = 2 + l > l$.
- Si $g = s_0 = \omega b^2$ y $m = 1$, entonces $t_1 = b^2$ ($t_1 \neq \omega$ puesto que, entonces $m = 0$; y $t_1 \neq b$ puesto que, entonces $m = 2$), luego $\ell(g*g') = 1 + l > l$.
- Si $g = s_2 = b^2\omega$ y $m = 0$, entonces $t_1 \in \{b, b^2\}$ ($t_1 \neq \omega$ puesto que, entonces $m = 2$), luego $\ell(g * g') = 2 + l > l$.
- Si $g = s_2 = b^2\omega$ y $m = 1$ no es posible puesto que se requiere $t_1 = \omega$, lo que implica $m = 2$.

⑥ Suponga que l es par y que $g = t_1 t_2 \dots t_k$, entonces máx$\{k, l\} = k$: el análisis es similar. □

Corolario 4. *Bajo las condiciones de la proposición 8, se deduce que el centro del conjugado de longitud impar no interviene en la multiplicación.*

Corolario 5. *Bajo las condiciones de la proposición 8, g y g' juntan mal si y sólo si $m = 2$.*

Definición 39 (Extremo izquierdo)**.** Para cada $s \in S$ definimos su extremo izquierdo, el cual denotaremos por $izq(s)$, de la forma: $izq(s_0) = \omega$, $izq(s_1) = b$, $izq(s_2) = b^2$ y si s es largo y de la forma $Q^{-1}s_1Q$, entonces $izq(s) = Q^{-1}b$.

Definición 40 (Extremo derecho)**.** Para cada $s \in S$ definimos su extremo derecho, el cual denotaremos por $der(s)$, de la forma: $der(s_0) = b^2$, $der(s_1) = b$, $der(s_2) = \omega$ y si s es largo y de la forma $Q^{-1}s_1Q$, entonces $der(s) = bQ$.

Proposición 9. *Sean $g, g' \in S$, si g y g' juntan bien entonces gg' tiene la forma reducida $izq(g_1)t_1 \dots t_n der(g')$ donde cada $t_i \in \{\omega, b, b^2\}$.*

Prueba. Sean $g, g' \in S$, entonces

- Si $\ell(g)$ y $\ell(g')$ son impares, entonces, por la proposición 7, sus centros no intervienen en la multiplicación, luego gg' tiene la forma $P^{-1}b\omega b^2\omega bQ$ ó $P^{-1}s_1t_1 \dots t_n s_1Q$; en ambos casos se cumple la proposición.

- Si $\ell(g)$ y $\ell(g')$ son pares, entonces, debido a que g y g' juntan bien, se presentan únicamente los siguientes tres casos: $s_0s_0 = \omega b^2\omega b^2$, $s_0s_2 = \omega b\omega$ y $s_2s_2 = b^2\omega b^2\omega$; se observa que se cumple la proposición.

- Si $\ell(g)$ es par y $\ell(g')$ es impar, entonces, por la proposición 8 y porque juntan bien, si m es la cantidad de sílabas del elemento corto que intervienen en la multiplicación, $m \in \{0, 1\}$, luego la parte izquierda de g no interviene y con mayor razón el extremo derecho de g' tampoco interviene porque $2 < \ell(g')$. Otra forma de analizar esta situación es la siguiente:
  i) si $g = s_0$, por hipótesis, g' debe comenzar con ω ó b^2; por lo tanto $gg' = \omega t_1 \dots t_n s_1Q$. Se cumple la proposición.
  ii) si $g = s_2$, por hipótesis, g' debe comenzar con b ó b^2; por lo tanto $gg' = b^2\omega Q^{-1}s_1Q$. Se cumple la proposición.

- Si $\ell(g)$ es impar y $\ell(g')$ es par, se analiza en forma similar al caso anterior. □

Proposición 10. *La forma reducida de un producto $g_1 \dots g_n$ de elementos de S, que junta bien, tiene la forma $izq(g_1)t_1 \dots t_m der(g_n)$ donde cada $t_i \in \{\omega, b, b^2\}$.*

Prueba. Para todo g_i de longitud impar, por la proposición 7 y por los corolarios 3 y 4, se cumple que su centro no interviene en la multiplicación por la izquierda y tampoco en la multiplicación por la derecha. Pero si g_i es de longitud par, entonces, por la proposición 8, si alguna sílaba de g_i interviene en la multiplicación, es aquella igual a b^2 convirtiéndose en b; la otra sílaba, ω, no interviene porque contradeciría la hipótesis; en partícular, lo anterior ocurre con g_1 y g_n. De esta forma se concluye que la forma reducida de $g_1 \dots g_n$ es $izq(g_1)t_1 \dots t_m der(g_n)$. □

Proposición 11. *Dados $g, g' \in S$ tales que $\ell(g)$ y $\ell(g')$ son impares, si g y g' juntan mal, entonces el centro del más corto interviene en la multiplicación de ambos.*

Prueba. De la proposición 7 se desprende que si el centro de g y el centro de g' no intervienen, entonces juntan bien. Luego, si g y g' no juntan bien, entonces el centro de g interviene o el centro de g' interviene.

Ahora, suponga que $\ell(g) = k < l = \ell(g')$, entonces si el centro de g' interviene, con mayor razón interviene el centro de g, puesto que $\frac{k+1}{2} < \frac{l+1}{2}$. Esto implica que cuando menos, el centro de g interviene. Si $\ell(g) = k > l = \ell(g')$ entonces el análisis es similar.

Se concluye que el centro del más corto interviene en la multiplicación. □

Afirmación 2. *Dados $g, g' \in S$ tales que $\ell(g)$ y $\ell(g')$ son impares, si g y g' juntan mal, entonces el centro del más largo no interviene en la multiplicación de ambos.*

Proposición 12. *Dados $g, g' \in S$ tales que $\ell(g)$ y $\ell(g')$ son impares con $\ell(g) < \ell(g')$, si g y g' juntan mal y m es la cantidad de sílabas de g que intervienen en la multiplicación gg' y si m' es la cantidad de sílabas de g^{-1} que intervienen en la multiplicación $(gg')g^{-1}$, entonces $m' \geqslant m$.*

Prueba. Si $g = t_k \dots t_1$ y $g' = t'_1 \dots t'_l$ entonces $t_i^{-1} = t'_i$ para $i \in [1 \dots m-1]$; puesto que, por la afirmación 2, el centro de g' no interviene en la multiplicación de gg', entonces, ya que las últimas $m-1$ sílabas de g' son iguales a las de g y las primeras $m-1$ sílabas de g^{-1} son iguales a las de g', las cancelaciones m' en $(gg')g^{-1}$ son, cuando menos, m. Luego, $m' \geqslant m$. □

Afirmación 3. *Dados $g, g' \in S$ tales que $\ell(g)$ y $\ell(g')$ son impares con $\ell(g) > \ell(g')$, si g y g' juntan mal y m es la cantidad de sílabas de g que intervienen en*

la multiplicación gg' y si m' es la cantidad de sílabas de g'^{-1} que intervienen en la multiplicación $g'^{-1}(gg')$, entonces $m' \geqslant m$.

Proposición 13. *Dados $g, g' \in S$ tales que $\ell(g)$ y $\ell(g')$ son impares, si g y g' juntan mal, entonces existen $h, h' \in S$ tales que $hh' = gg'$ y $\ell(h) + \ell(h') < \ell(g) + \ell(g')$.*

Prueba. Sean $g, g' \in S$, tales que $\ell(g) = k$ y $\ell(g') = l$, entonces:

① Si $k < l$, entonces, por la proposición 11, el centro de g interviene en la multiplicación.

② Sean $h = (gg')g^{-1}$ y $h' = g$. Se verifica que $hh' = \left((gg')g^{-1}\right) g = gg'$.

③ Si m es la cantidad de sílabas de g que intervienen en la multiplicación de gg', entonces, por ①, $m \geqslant \frac{k+3}{2}$ (pues si el centro, que se encuentra en la posición $\frac{k+1}{2}$, interviene, también interviene la sílaba siguiente que es b).

④ Si m' es la cantidad de sílabas de g^{-1} que intervienen en la multiplicación $(gg')g^{-1}$, entonces, por ① y por la proposición 12, $m' \geqslant m$.

⑤ Si $m = \frac{k+3}{2}$ y $m' = \frac{k+3}{2}$ (son los valores mínimos que pueden tomar), y asumiendo que $\ell(r_1) = \ell(r_2) = 1$, (recuerde que $\ell(r_i) \in \{0, 1\}$, entonces, por la afirmación 1, $\ell((gg')g^{-1}) = \left[k + l - 2\left(\frac{k+3}{2}\right) + \ell(r_1)\right] + k - 2\left(\frac{k+3}{2}\right) + \ell(r_2) = l - 4$; lo que en realidad implica que $\ell((gg')g^{-1}) \leqslant l - 4$.

⑥ Se concluye que $\ell(h) + \ell(h') \leqslant (l-4) + k < k + l = \ell(g) + \ell(g')$.

Observe que lo realizado fue un cambio de Hurwitz a la izquierda, definición 25. Ahora, si $l < k$, entonces hacemos $h = g'$ y $h' = (g')^{-1}(gg')$ y cálculos equivalentes: así queda probado.

No se analiza el caso $k = l$, puesto que, por la proposición 6, g y g' juntarían bien □

Proposición 14. *Si $g, g' \in S$ son tales que $g*g'$ junta mal y a lo más uno de ellos tiene longitud par, entonces existe un movimiento de Hurwitz que transforma el par (g, g') en un par (h, h') tal que $\ell(h) + \ell(h') < \ell(g) + \ell(g')$.*

Prueba. Sean $g, g' \in S$ con $\ell(g) = k$ y $\ell(g) = l$, entonces:

① Sean $k = 2$, l impar, $h = (gg')g^{-1}$ y $h' = g$. Se verifica que $hh' = \left((gg')g^{-1}\right) g = gg'$.

② Si m es la cantidad de sílabas de g que intervienen en la multiplicación gg' y m' es la cantidad de sílabas de g^{-1} que intervienen en la multiplicación $(gg')g^{-1}$, tenemos entonces dos casos:

- Si $g = s_0 = \omega b^2$ entonces, por el corolario 5, $m = 2$ y $r_1 = 0$; $m' = 1$ y $r_2 = 1$ si $l = 3$ ($m' = 2$ y $r_2 = 0$ si $l \geqslant 5$). Entonces, por la afirmación 1, $\ell((gg')g^{-1}) = [k + l - 2m + \ell(r_1)] + k - 2m' + \ell(r_2) = l - 1$ si $l = 3$ ($l - 4$ si $l \geqslant 5$); lo que en realidad implica que $\ell((gg')g^{-1}) \leqslant l - 1$. Se concluye que $\ell(h) + \ell(h') \leqslant (l - 1) + k < k + l = \ell(g) + \ell(g')$.
- Si $g = s_2 = b^2\omega$ entonces por el corolario 5, $m = 2$ y $\ell(r_1) \in \{0, 1\}$; $m' = 2$ y $\ell(r_2) \in \{0, 1\}$. Entonces, por la afirmación 1, $\ell((gg')g^{-1}) = [k + l - 2m + \ell(r_1)] + k - 2m' + \ell(r_2) = l - 2$ ó $l - 4$; lo que en realidad implica que $\ell((gg')g^{-1}) \leqslant l-2$. Se concluye que $\ell(h)+\ell(h') \leqslant (l - 2) + k < k + l = \ell(g) + \ell(g')$.

Observe que lo realizado fue un cambio de Hurwitz a la izquierda, definición 25.

③ Si k es impar, $l = 2$, $h = g'$ y $h' = (g')^{-1}(gg')$ y realizamos cálculos equivalentes, vemos que $hh' = \left((gg')g^{-1}\right) g = gg'$ y que $\ell(h) + \ell(h') < \ell(g) + \ell(g')$. □

Definición 41 (Factorización en cortos)**.** Una factorización de un elemento $g \in G$ es en cortos si todos sus factores son cortos; esto incluye a la factorización vacía.

Proposición 15. *Toda factorización $(g_1, \ldots, g_r)$ en cortos de un $g \in G$ es Hurwitz equivalente a otra en cortos de la forma $(g'_1, \ldots, g'_s, s_0, s_1, \ldots, s_0, s_1)$, donde $0 \leqslant s \leqslant r$ y $(g'_1, \ldots, g'_s)$ junta bien.*

Prueba. Supongamos que $(g_1, \ldots, g_r)$ es una factorización en cortos de $g \in G$ donde ningún par junta mal, $r = s$ y queda probado.

Suponga que existe al menos un par $g_i g_{i+1}$ tal que juntan mal. Como se vio antes de la proposición 6, los únicos pares de cortos que juntan mal son $s_0 s_1 = s_1 s_2 = s_2 s_0 = b$, los cuales son Hurwitz equivalentes. Por simplicidad en la explicación de la prueba, convirtamos los $s_1 s_2$ a $s_0 s_1$ mediante Hurwitz a la izquierda y los $s_2 s_0$ a $s_0 s_1$ mediante Hurwitz a la derecha, entonces, entre los varios pares $g_i g_{i+1}$ que juntan mal, escojamos el par $s_0 s_1$ de la derecha. Si este par $g_i g_{i+1}$ es $g_{r-1} g_r$, es decir, ya están al final, entonces no hay nada que hacer, sino lo es, proceda de la siguiente forma:

- Si $g_{i+2} = s_0$, entonces, mediante Hurwitz a la derecha, convirtamos $s_0 s_1$ en $s_1 s_2$, de esta forma tendremos $g_{i+1} g_{i+2} = s_2 s_0$, es decir, un par que junta mal más a la derecha. Convierta este par a $s_0 s_1$.

- Si $g_{i+2} = s_1$, entonces, mediante Hurwitz a la izquierda, convirtamos $s_0 s_1$ en $s_2 s_0$, de esta forma tendremos $g_{i+1} g_{i+2} = s_0 s_1$, es decir, un par que junta mal más a la derecha.

Repita el anterior paso hasta situar el par que junta mal en las posiciones $r-1$ y r o hasta que esté contiguo a otro par que junta mal situado al final.

Cuando sitúe un par que junta mal, en el extremo derecho, continúe con el anterior par de más a la derecha y así sucesivamente hasta que todos los pares que juntan mal estén situados en el extremo derecho. Así queda probado. □

Proposición 16. *Toda factorización especial $(g_1, \ldots, g_n)$, de un elemento $g \in G$, puede ser transformada, aplicando una secuencia de movimientos de Hurwitz, en una factorización (necesariamente especial y con el mismo número de factores) $(g'_1, \ldots, g'_n)$, que satisface al menos una de las siguientes dos propiedades:*

i) cada g'_i es corto

ii) junta bien.

Prueba. La demostración será por inducción sobre la cantidad

$$L(g_1, \ldots, g_n) = \sum_{i=1}^{n} \text{máx}\{0, \ell(g_i) - 3\}\,.$$

Si $L(g_1, \ldots, g_n) = 0$, entonces se tiene que $\ell(g_i) - 3 \leqslant 0$ para cada i. Pero esto equivale al hecho de que cada g_i es corto. Concluimos que en este caso $(g_1, \ldots, g_n)$ ya satisface la propiedad i). Supongamos ahora que $L(g_1, \ldots, g_n) > 0$, y que el resultado es cierto para toda factorización cuya L es menor que $L(g_1, \ldots, g_n)$. Si $(g_1, \ldots, g_n)$ junta bien, no hay nada que probar. Supongamos entonces que $(g_1, \ldots, g_n)$ junta mal, es decir, que existe i tal que (g_i, g_{i+1}) junta mal. Por otro lado, que $L(g_1, \ldots, g_n) > 0$ nos dice que existe j tal que $\ell(g_j) - 3 > 0$, es decir, g_j es un conjugado largo de s_1. Si g_i es largo o g_{i+1} es largo, entonces sabemos que haciendo un cambio de Hurwitz adecuado logramos cambiar el par (g_i, g_{i+1}) por un par (g'_i, g'_{i+1}) tal que $\ell(g_i) + \ell(g_{i+1}) > \ell(g'_i) + \ell(g'_{i+1})$. Entonces $L(g_1, \ldots, g_i, g_{i+1}, \ldots, g_n) > L(g_1, \ldots, g'_i, g'_{i+1}, \ldots, g_n)$, por las proposiciones 13 y 14. Tenemos entonces que $(g_1, \ldots, g_i, g_{i+1}, \ldots, g_n)$ se transforma

por un movimiento de Hurwitz en $(g_1,\ldots,g_i',g_{i+1}',\ldots,g_n)$, y como esta última satisface la hipótesis de inducción, existe $(g_1'',\ldots,g_n'')$ Hurwitz equivalente a $(g_1,\ldots,g_i',g_{i+1}',\ldots,g_n)$, y que satisface i) o ii). Entonces $(g_1,\ldots,g_n)$ es Hurwitz equivalente a $(g_1'',\ldots,g_n'')$, la cual satisface i) o ii). Podemos entonces suponer que g_i y g_{i+1} son cortos. Supongamos que $j>i$, y que j es tomado de tal manera que todos los elementos $g_i,g_{i+1},\ldots,g_{j-1}$ son cortos. Ahora, los únicos pares de conjugados cortos que juntan mal son $(s_0,s_1),(s_1,s_2)$ y (s_2,s_0), y existen movimientos de Hurwitz que transforman el par (s_1,s_2) en (s_0,s_1) y a (s_2,s_0) en (s_0,s_1). Ahora, se verifica directamente que $g^{-1}*h*g\in\{s_0,s_1,s_2\}$ siempre que $h\in\{s_0,s_1,s_2\}$ y $g\in\{s_0,s_0^{-1},s_1,s_1^{-1},s_2,s_2^{-1}\}$. Esto hace posible hacer $j-i-2$ movimientos de Hurwitz que llevan a g_{i+1} hasta la posición $j-1$. Luego se pueden hacer otros $j-i-2$ movimientos de Hurwitz que llevan a g_i a la posición $j-2$. Obtenemos así una nueva factorización $(g_1',\ldots,g_n')$ tal que g_j' es largo, $g_{j-2}=s_0$, $g_{j-1}=s_1$ y $L(g_1',\ldots,g_n')=L(g_1,\ldots,g_n)$. Ahora, es fácil ver que existe al menos un conjugado corto s_α tal que (s_α,g_j) junta mal. Entonces, haciendo, si fuera necesario, un movimiento de Hurwitz extra al par (g_{j-2}',g_{j-1}'), se obtiene una factorización $(g_1'',\ldots,g_n'')$ tal que $g_j''=g_j$ y $g_{j-1}''=s_\alpha$. Note que $L(g_1'',\ldots,g_n'')=L(g_1',\ldots,g_n')=L(g_1,\ldots,g_n)$. Entonces el par (g_{j-1}'',g_j'') satisface las condiciones de la proposición 14. Entonces se puede hacer un movimiento de Hurwitz a este par, de tal manera que el nuevo par (g_{j-1}''',g_j''') satisfaga $\ell(g_{j-1}''')+\ell(g_j''')<\ell(g_{j-1}'')+\ell(g_j'')$, y entonces

$$L(g_1'',\ldots,g_{j-1}''',g_j''',\ldots,g_n'')<L(g_1'',\ldots,g_{j-1}'',g_j'',\ldots,g_n'')=L(g_1,\ldots,g_n)\,.$$

De acuerdo a la hipótesis de inducción, la factorización $(g_1'',\ldots,g_{j-1}''',g_j''',\ldots,g_n'')$ puede ser transformada por medio de movimientos de Hurwitz en otra que es en cortos o que junta bien. Esto concluye la demostración. □

Definición 42 (Colección Hurwitz completa)**.** Una colección de factorizaciones especiales de $g\in G$ se dice que es Hurwitz completa si por cada clase de equivalencia existe por lo menos una factorización en la colección que representa a dicha clase. Esto es equivalente a decir que por cada factorización especial de g, hay al menos una en la colección que es equivalente a ella.

Por las proposiciones 15 y 16, para obtener una colección Hurwitz completa de factorizaciones especiales de un $g\in G$, basta encontrar todas las factorizaciones especiales de g que juntan bien, y todas las factorizaciones especiales de g en cortos de la forma $(g_1,\ldots,g_s,s_0,s_1,\ldots,s_0,s_1)$, con $s\geqslant 0$ y en la que $(g_1,\ldots,g_s)$ junta bien.

Unidad 3

Algoritmo, código en Maple y ejemplo

A continuación se presenta un algoritmo modular recursivo tal que dado un $g \in G$, determina todas sus posibles factorizaciones especiales de la forma

$$(h_1, \ldots, h_r)(s_0, s_1)^{j+3k},$$

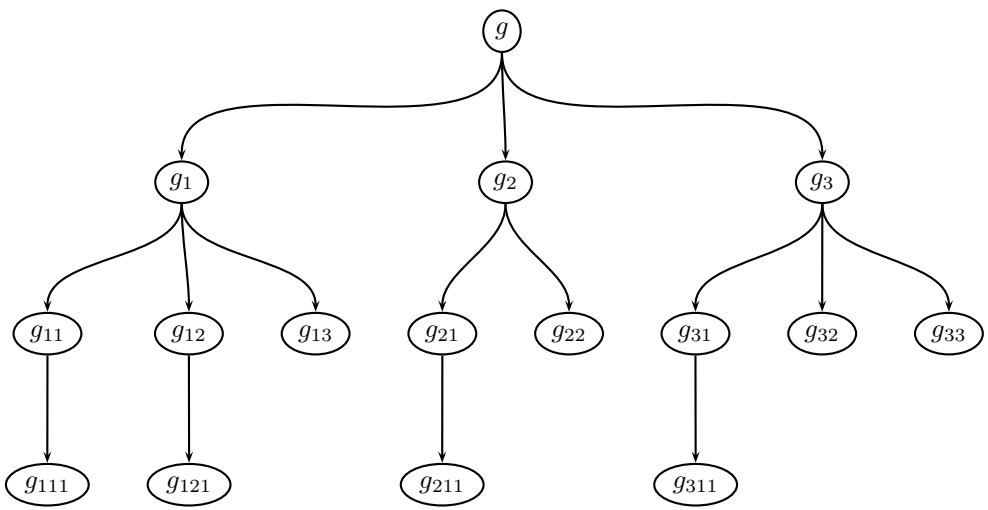
donde $j \in \{0, 1, 2\}$, $k \geqslant 0$, $r \geqslant 0$, y si $r \geqslant 2$ cada par (h_i, h_{i+1}), $1 \leqslant i \leqslant r-1$, junta bien. Según lo discutido en las últimas secciones de la unidad 2, estas factorizaciones forman una colección Hurwitz completa de factorizaciones especiales de g. Algunas de estas factorizaciones pueden ser Hurwitz equivalentes entre sí.

Para comprender el funcionamiento del algoritmo suponga que construiremos un árbol n–ario donde el nodo raíz, numerado como 0, está compuesto por el $g \in G$ a factorizar. El siguiente nivel, nivel 1, está compuesto por n_1 nodos donde el primer nodo contiene a $s_i^{-1}g = g_0$, $i \in [0, 1, 2]$; el segundo posible nodo contiene a $h_1^{-1}g = g_1$, el tercero contiene $h_2^{-1}g = g_2$, y así sucesivamente. Cada h_i es un posible factor especial largo de g. La cantidad de factores especiales largos es determinada por la longitud de g. El algoritmo busca todos los posibles hasta la mitad de dicha longitud. Entonces, en el nivel 1 se ha determinado un número finito de nuevos g_i, cada uno de los cuales es de menor longitud que el g contenido en el nodo padre.

Con cada g_i obtenido en el nivel 2, se genera el nivel 3 tal como se obtuvo el nivel 2 y así se avanza sucesivamente de nivel en nivel hasta que la longitud del elemento a factorizar en un nodo es cero, uno o dos.

Cada ruta desde el nodo raíz hasta cada hoja del árbol indica una factorización de g compuesta por los s_i y los h_j empleados para reducir g a longitud cero, uno o dos. Cuando en una hoja su longitud es cero, ello indica que todos los factores juntan bien; si es diferente de cero, entonces los factores no juntan bien y esa factorización es ignorada en la ejecución del algoritmo, excepto si todos los factores son cortos, tal como se puede observar en el ejemplo dado luego del código.

El siguiente árbol ejemplariza la anterior descripción.



Notas: el g a factorizar es generado aleatoriamente; por cada nodo en cada nivel, el algoritmo se invoca a sí mismo, por ello es recursivo; y el algoritmo funciona para un g de longitud mayor o igual a cero, la longitud está limitada sólo por la capacidad de la máquina donde se ejecute.

```
Algoritmo Factorizar
   Generar(g ∈ ⟨ω, b : ω^2, b^3⟩);
   FactorizaciónCortosLargos (g, [], []);
Fin Factorizar


FactorizaciónCortosLargos(CadenaAnálisis, ÚltimoFactor, Factorización)
   Si CadenaAnálisis = [] entonces
      Factorización ← Factorización+(s0 s1)^3k;
      Escriba(Factorización);
    sino
      # Primero suponemos que hay un factor corto
```

```
    Dependiendo de long(CadenaAnálisis) haga
      1: Dependiendo de CadenaAnálisis[1] haga
           ω: Factorización ← Factorización+s_0 + (s_0 s_1)^{1+3k};
           b^i: Factorización ← Factorización+(s_0 s_1)^{i+3k};
         Fin dependiendo
         Escriba(Factorización);
      2: Dependiendo de CadenaAnálisis[1, 2] haga
           ωb: Factorización ← Factorización+s_0 + (s_0 s_1)^{2+3k};
           ωb^2: Factorización ← Factorización+s_0 + (s_0 s_1)^{3k};
           bω: Factorización ← Factorización+s_1 + (s_0 s_1)^{2+3k};
           b^2ω: Factorización ← Factorización+s_2 + (s_0 s_1)^{3k};
         Fin dependiendo
         Escriba(Factorización);
      ⩾3: FactorCorto ← DeterminarFactorCorto(CadenaAnálisis);
         Si PeganBien(ÚltimoFactor, FactorCorto) entonces
           Factorización ← Factorización+FactorCorto;
           InversoFactorCorto ← Inverso(FactorCorto);
           NuevaCadena ← Multiplicar(InversoFactorCorto, CadenaAnálisis);
           FactorizaciónCortosLargos(NuevaCadena, FactorCorto, Factorización)
         Fin si

    # Ahora suponemos que hay uno o varios factores largos
      ⩾ 5 : ListaFactoresLargos ← DeterminarFactoresLargos(CadenaAnálisis);
         Para i ← 1 hasta ℓ(ListaFactoresLargos) haga
           FactorLargo ← ListaFactoresLargos [i];
           Si PeganBien (ÚltimoFactor, FactorLargo) entonces
             Factorización ← Factorización+FactorLargo;
             InversoFactorLargo ← Inverso (FactorLargo);
             NuevaCadena ← Multiplicar(InversoFactorLargo, CadenaAnálisis);
             FactorizaciónCortosLargos(NuevaCadena, FactorLargo,Factorización);
           Fin si
         Fin para
    Fin dependiendo
  Fin si
Fin FactorizaciónCortosLargos


DeterminarFactorCorto(Cadena)
  Dependiendo de Cadena[1] haga
    ω : Retorne (s_0);
    b : Retorne (s_1);
    b^2 : Retorne (s_2);
  Fin dependiendo
Fin DeterminarFactorCorto


PeganBien(g_1, g_2)
```

$g \leftarrow$ Multiplicar(g_1, g_2)
Si $\ell(g) \geqslant \ell(g_1) \wedge \ell(g) \geqslant \ell(g_2)$ **entonces**
Retorne(verdadero);
sino
Retorne (falso);
Fin **si**
Fin **PeganBien**

Multiplicar(g_1, g_2)
Terminar←falso;
Mq $\ell(g_1) \neq 0 \ \wedge \ \ell(g_2) \neq 0 \wedge \sim$Terminar **haga**
Si $(g_1[\ell(g_1)] = \omega \wedge g_2[1] = \omega) \vee \big(g_1[\ell(g_1)] = b \wedge g_2[1] = b^2\big) \vee \big(g_1[\ell(g_1)] = b^2 \wedge g_2[1] = b\big)$ **entonces**
$g_1 \leftarrow g_1 - g_1[\ell(g_1)]$;
$g_2 \leftarrow g_2 - g_2[1]$;
sino
Si $g_1[\ell(g_1)] = b \wedge g_2[1] = b$ **entonces**
$g_1[\ell(g_1)] \leftarrow b^2$;
$g_2 \leftarrow g_2 - g_2[1]$;
sino
Si $g_1[\ell(g_1)] = b^2 \wedge g_2[1] = b^2$ **entonces**
$g_1[\ell(g_1)] \leftarrow b$;
$g_2 \leftarrow g_2 - g_2[1]$;
Fin **si**
Fin **si**
Terminar←verdadero;
Retorne $(g_1 + g_2)$;
Fin **si**
Fin **mq**
Si $\sim$Terminar **entonces**
Retorne $(g_1 + g_2)$;
Fin **si**
Fin **Multiplicar**

Inverso(g);
Tamaño $\leftarrow \ell(g)$;
$g^{-1} \leftarrow []$;
Para $i \leftarrow 1$ hasta Tamaño **haga**
Dependiendo de g[Tamaño$-i+1$] **haga**
ω: $g^{-1}[i] \leftarrow \omega$;
b: $g^{-1}[i] \leftarrow b^2$;
b^2: $g^{-1}[i] \leftarrow b$;
Fin **dependiendo**
Fin **para**
Retorne (g^{-1});

Fin **Inverso**

DeterminarFactoresLargos(Cadena)
LongitudCadena ← *long*(Cadena);
ListaFactoresLargos ← [];
ContadorFactoresLargos ← 0;
$i \leftarrow 2$;
Mientras que $i <$ (LongitudCadena/2) **haga**
Si Cadena$[i] = b \wedge$ Cadena$[i+1] = \omega$ **entonces**
ContadorFactoresLargos ← ContadorFactoresLargos+1;
ListaFactoresLargos [ContadorFactoresLargos] ← ArmarFactorLargo(Cadena, $i-1$);
Fin **si**
$i \leftarrow i+1$;
Fin **mientras que**
Retorne(ListaFactoresLargos);
Fin **DeterminarFactoresLargos**

ArmarFactorLargo(Cadena, i)
$Q^{-1} \leftarrow []$;
Para $j \leftarrow 1$ hasta i **haga**
$Q^{-1}[j] \leftarrow$ Cadena$[j]$;
Fin **para**
$Q \leftarrow$ Inverso(Q^{-1});
Retorne $(Q^{-1}s_1Q)$;
Fin **ArmarFactorLargo**

El algoritmo fue implementado en Maple 12. A continuación el código.

```
> DeterminarFactorCorto := proc (Cadena::list)

description "Procedimiento que determina el primer factor corto de un
g=g[1]...g[r] \in <w,b| w^(2)=b^(3)= 1>, recibido en el parámetro 'Cadena',
de acuerdo a g[1]. El proceso retorna el correspondiente s[0],s[1] ó s[2],
indicado como ['w','b^2'], ['b','w','b'] ó['b^2','w'], respectivamente.";

 if nops(Cadena) = 0 then
   return "La cadena está vacía"
  else
    if Cadena[1] = "w" then
      return ["w", "b^2"]
     elif Cadena[1] = "b" then
      return ["b", "w", "b"]
     elif Cadena[1] = "b^2" then
```

```
      return ["b^2", "w"]
     else
      printf("El dato %s es malo", Cadena[1])
    end if
 end if

end proc;

-------------------------------------------------------------

> GenerarG := proc (longitud::integer)

local i, g, anterior, generado;
description "Construye un g reducido \in <w,b| w^(2)=b^(3)= 1>, de la longitud
indicada en la variable de entrada 'longitud'. ";
i := 0; g := [];

 if 0 < longitud then
   anterior := `mod`(rand(), 3);
   while i < longitud do
     generado := `mod`(rand(), 3);
     if anterior = 0 and generado = 1 or anterior = 0 and generado = 2 or
      anterior = 1 and generado = 0 or anterior = 2 and generado = 0 then
       i := i+1;
       g := [op(g), generado];
       anterior := generado
     end if
   end do
 end if;

 for i to longitud do
   if g[i] = 0 then
     g[i] := "w"
    elif g[i] = 1 then
     g[i] := "b"
    elif g[i] = 2 then
     g[i] := "b^2"
   end if
 end do;

 return g

end proc;

-------------------------------------------------------------

> Multiplicar := proc (g::list, h::list)
local Terminar, g1, g2;
```

```
description "Dados g,h \in <w,b| w^(2)=b^(3)= 1>, se multiplican estos de
tal forma que se obtiene un g=gh el cual es retornado. ";

 g1 := g;
 g2 := h;
 Terminar := "falso";

 while nops(g1) <> 0 and nops(g2) <> 0 and Terminar = "falso" do
   if g1[nops(g1)] = "w" and g2[1] = "w" or g1[nops(g1)] = "b" and
    g2[1] = "b^2" or g1[nops(g1)] = "b^2" and g2[1] = "b" then
      g1 := [op(1 .. nops(g1)-1, g1)];
      if 1 < nops(g2) then
        g2 := [op(2 .. nops(g2), g2)]
       else g2 := []
      end if
     else
      if g1[nops(g1)] = "b" and g2[1] = "b" then
        g1[nops(g1)] := "b^2";
        if 1 < nops(g2) then
          g2 := [op(2 .. nops(g2), g2)]
         else g2 := []
        end if
       else
        if g1[nops(g1)] = "b^2" and g2[1] = "b^2" then
          g1[nops(g1)] := "b";
          if 1 < nops(g2) then
            g2 := [op(2 .. nops(g2), g2)]
           else
            g2 := []
          end if
        end if
      end if;

      Terminar := "verdadero";
      return [op(g1), op(g2)]
    end if
  end do;

  if Terminar = "falso" then
    return [op(g1), op(g2)]
  end if
end proc;

-------------------------------------------------------------

> PeganBien := proc (g1::list, g2::list)
local g;
```

```
description "Verifica si g1, g2 \in <w,b| w^(2)=b^(3)= 1> juntan bien. Retorna
'verdadero' en caso afirmativo. Retorna 'falso' en caso negativo.";

 g := Multiplicar(g1, g2);

 if nops(g1) <= nops(g) and nops(g2) <= nops(g) then
   return "verdadero"
  else
   return "falso"
 end if
end proc;

----------------------------------------------------------------

> Inverso := proc (g)
local Tamaño, i, Inv;

description "Recibido un 'g' \in  <w,b| w^(2)=b^(3)= 1> el procedimiento
retorna el correspondiente inverso. ";

 Tamaño := nops(g);
 Inv := [];

 for i to Tamaño do
   if g[Tamaño-i+1] = "w" then
     Inv := [op(Inv), "w"]
    elif g[Tamaño-i+1] = "b" then
     Inv := [op(Inv), "b^2"]
    elif g[Tamaño-i+1] = "b^2" then
     Inv := [op(Inv), "b"]
   end if
 end do;

 return Inv

end proc;

----------------------------------------------------------------

> DeterminarFactoresLargos := proc (Cadena)

local LongitudCadena, ListaFactoresLargos, ContadorFactoresLargos, i;

description "Dado un g \in <w,b| w^(2)=b^(3)= 1> recibido  en el parámetro
Cadena, se determina una lista de posibles factores largos de dicho g.
Cada factor largo \in S. ";
```

```
 LongitudCadena := nops(Cadena);
 ListaFactoresLargos := [];
 ContadorFactoresLargos := 0;
 i := 2;

 while i < (1/2)*LongitudCadena do
   if Cadena[i] = "b" and Cadena[i+1] = "w" then
     ListaFactoresLargos := [op(ListaFactoresLargos), ArmarFactorLargo(Cadena, i)]
   end if;
   i := i+1
 end do;

 return ListaFactoresLargos

end proc;

-----------------------------------------------------------------

> ArmarFactorLargo := proc (g::list, i::integer)

local Qi, j, Q;

description "Recibido un g=g_1...g_n \in G, se toman los primeros i-1 componentes
de g, y se determina que g_1...g_{i-1}=Qi. Luego se construye un s=QiS_1Q \in S.
Se retorna s. ";

 Qi := [];

 for j to i-1 do
   Qi := [op(Qi), g[j]]
 end do;

 Q := Inverso(Qi);
 return [op(Qi), "b", "w", "b", op(Q)]

end proc;

-----------------------------------------------------------------

> Convertir := proc (Factores::list)

local i, Conversion;

description "Dado un g=g[1]...g[n] \in <w,b| w^(2)=b^(3)= 1>, recibido en
'Factores', donde cada g[i]\in [[w, b^2],[b,w,b],[b^2,w],
(s[0]s[1])^(j+3k),largo], se convierte cada factor a [s[0],s[1],s[2],
(s[0]s[1])^(j+3 k),largo], respectivamente. ";
```

```
 Conversion := [];

 if 0 < nops(Factores) then
   for i to nops(Factores) do
     if Factores[i] = ["w", "b^2"] then
       Conversion := [op(Conversion), s[0]]
      elif Factores[i] = ["b", "w", "b"] then
       Conversion := [op(Conversion), s[1]]
      elif Factores[i] = ["b^2", "w"] then
       Conversion := [op(Conversion), s[2]]
      else Conversion := [op(Conversion), Factores[i]]
     end if
   end do
 end if;

 return Conversion

end proc;

-----------------------------------------------------------------

> VerificarRespuesta := proc (Factores::list)

local Concatenacion, i;
global gOriginal;

description "Se compara el parámetro 'Factores' con el g original que fue
dado a factorizar, el cual está contenido en la variable 'gOriginal' que
es global. El procedimiento informa si son diferentes";

 Concatenacion := [];

 if nops(Factores) = 0 then
   print("Error: la factorización está vacía")
  else
   for i to nops(Factores)-1 do
     Concatenacion := Multiplicar(Concatenacion, Factores[i])
   end do;
   if Factores[nops(Factores)] = (s[0]*s[1])^(1+3*k) then
     Concatenacion := Multiplicar(Concatenacion, ["b"])
   end if;
   if Factores[nops(Factores)] = (s[0]*s[1])^(2+3*k) then
     Concatenacion := Multiplicar(Concatenacion, ["b^2"])
   end if;
   if nops(Concatenacion) <> nops(gOriginal) then
     print("Error: La cantidad de factores es diferente");
     return
    else
```

```
     for i to nops(Concatenacion) do
       if gOriginal[i] <> Concatenacion[i] then
         print("Error: la factorización es diferente del g original");
         return
       end if
     end do
   end if
 end if

end proc;

-----------------------------------------------------------------

> FactorizacionCortosLargos := proc (CadenaAnalisis::list, UltimoFactor::list,
   ResultadoAnterior::list)

local FactorCorto, InversoFactorCorto, NuevaCadena, ListaFactoresLargos, i,
 FactorLargo, InversoFactorLargo, Resultado;
global YaImprimioCortos;

description "Algoritmo recursivo que recibe un g=g[1]...g[n] \in G=<w,b|
w^(2)=b^(3)= 1> en el parámetro 'CadenaAnalisis', y detemina su primer
factor corto y posibles primeros factores largos. El factor encontrado es
agregado a la variable Resultado junto con la factorización recibida en el
parámetro ResultadoAnterior. El llamado a este proceso es finalizado luego
que se ha determinado que  la longitud del parámetro 'CadenaAnalisis' es
menor que tres. Entonces la factorización se convierte a forma legible, se
imprime y se verifica el resultado con el g original contenido en la variable
global gOriginal.  ";

 if CadenaAnalisis = [] then
   Resultado := [op(ResultadoAnterior), (s[0]*s[1])^(3*k)];
   if YaImprimioCortos = "falso" then
     print(Convertir(Resultado), nops(Resultado)-1);
     YaImprimioCortos := "verdadero"
    else
     print(Convertir([op(1 .. nops(Resultado)-1, Resultado)]), nops(Resultado)-1)
   end if;
   VerificarRespuesta(Resultado)
  else
   if nops(CadenaAnalisis) = 1 then
     if CadenaAnalisis[1] = "w" then
       Resultado := [op(ResultadoAnterior), ["w", "b^2"], (s[0]*s[1])^(1+3*k)]
      elif CadenaAnalisis[1] = "b" then
       Resultado := [op(ResultadoAnterior), (s[0]*s[1])^(1+3*k)]
      elif CadenaAnalisis[1] = "b^2" then
       Resultado := [op(ResultadoAnterior), (s[0]*s[1])^(2+3*k)]
      else
```

```
    print(Error*en*la*determinación*del*último*factor*corto*del*g*de*entrada)
  end if;

  if YaImprimioCortos = "falso" then
    print(Convertir(Resultado), nops(Resultado)-1);
    VerificarRespuesta(Resultado);
    YaImprimioCortos := "verdadero"
  end if
end if;

if nops(CadenaAnalisis) = 2 then
  if CadenaAnalisis[1] = "w" and CadenaAnalisis[2] = "b" then
    Resultado := [op(ResultadoAnterior), ["w", "b^2"], (s[0]*s[1])^(2+3*k)]
   elif CadenaAnalisis[1] = "w" and CadenaAnalisis[2] = "b^2" then
    Resultado := [op(ResultadoAnterior), ["w", "b^2"], (s[0]*s[1])^(3*k)]
   elif CadenaAnalisis[1] = "b" and CadenaAnalisis[2] = "w" then
    Resultado := [op(ResultadoAnterior), ["b", "w", "b"], (s[0]*s[1])^(2+3*k)]
   elif CadenaAnalisis[1] = "b^2" and CadenaAnalisis[2] = "w" then
    Resultado := [op(ResultadoAnterior), ["b^2", "w"], (s[0]*s[1])^(3*k)]
   else
    return Error*en*la*determinación*del*último*factor*corto*del*g*de*entrada
  end if;

  if Resultado[nops(Resultado)] = (s[0]*s[1])^(3*k) or YaImprimioCortos = "falso" then
    if YaImprimioCortos = "falso" then
      print(Convertir(Resultado), nops(Resultado)-1); YaImprimioCortos := "verdadero"
     else
      print(Convertir([op(1 .. nops(Resultado)-1, Resultado)]), nops(Resultado)-1)
    end if;
    VerificarRespuesta(Resultado)
  end if
end if;

if 3 <= nops(CadenaAnalisis) then
  FactorCorto := DeterminarFactorCorto(CadenaAnalisis);
  if PeganBien(UltimoFactor, FactorCorto) = "verdadero" then
    Resultado := [op(ResultadoAnterior), FactorCorto];
    InversoFactorCorto := Inverso(FactorCorto);
    NuevaCadena := Multiplicar(InversoFactorCorto, CadenaAnalisis);
    FactorizacionCortosLargos(NuevaCadena, FactorCorto, Resultado)
  end if
end if;

if 5 <= nops(CadenaAnalisis) then
  ListaFactoresLargos := DeterminarFactoresLargos(CadenaAnalisis);
  for i to nops(ListaFactoresLargos) do
    FactorLargo := ListaFactoresLargos[i];
    if PeganBien(UltimoFactor, FactorLargo) = "verdadero" then
```

```
        Resultado := [op(ResultadoAnterior), FactorLargo];
        InversoFactorLargo := Inverso(FactorLargo);
        NuevaCadena := Multiplicar(InversoFactorLargo, CadenaAnalisis);
        FactorizacionCortosLargos(NuevaCadena, FactorLargo, Resultado)
      end if
    end do
  end if
end if

end proc;

-----------------------------------------------------------------

> Factorizar := proc ()

global gOriginal, YaImprimioCortos;

description "Algoritmo que genera un g=g[1]...g[n] \in G=<w,b| w^(2)=b^(3)= 1>,
lo factoriza en  g=g'[1]...g'[n],con cada g'[i] \in S={s[i]: s[i]=Q^(-1)hQ,
Q \in G},  de tal forma que cada par  g'[i]g'[i+1] junte bien, excepto
posiblemente al final de cada factorización. A cada factorización se le agrega
al final (s[0]s[1])^(j+3 k), representando así un conjunto de clases de
factorizaciones de g. Si al final de cada factorización se obtiene 'b' ó 'b^(2)',
quiere decir que la factorización no junta bien. Solamente son mostradas
aquellas factorizaciones que juntan bien, excepto la primera factorización
encontrada que corresponde a aquella que es en cortos y que tal vez junte mal.";

 YaImprimioCortos := "falso";
 gOriginal := GenerarG(35);
 lprint("Las factorizaciones de g = ");
 print(gOriginal);
 lprint("donde la primera es en cortos (que consiste en el conjunto de representantes
 de todas las clases de factorizaciones posibles en cortos de g, k>=0), y las
 siguientes son las que juntan bien, que contienen al menos un factor largo, son:");

 FactorizacionCortosLargos(gOriginal, [], [])

end proc;

-----------------------------------------------------------------
```

A continuación un ejemplo de un g de longitud 35 generado aleatoriamente

```
> Factorizar();
"Las factorizaciones de g = "
["w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w",
  "b", "w", "b^2", "w", "b^2", "w", "b^2", "w", "b^2", "w", "b", "w", "b",
```

```
  "w", "b^2", "w", "b", "w", "b", "w"]
"donde la primera es en cortos (que consiste en el conjunto de representantes
de todas las clases de factorizaciones posibles en cortos de g, k>=0), y las
siguientes son las que juntan bien, que contienen al menos un factor largo, son:"
[
[s_0, s_2, s_1, s_0, s_2, s_1, s_0, s_0, s_2, s_2, s_2, s_2, s_2,
  s_1, s_0, s_0, s_2, s_1, (s_0 s_1)^(2 + 3 k)], 18

[s_0, s_2, s_1, s_0, s_2, s_1, s_0, s_0, s_2, s_2, s_2, s_2, s_2,
  s_1, s_0, ["w", "b", "w", "b", "w"]], 16

[s_0, s_2, s_1, s_0, s_2, s_1, s_0, s_0, s_2, s_2, s_2, s_2, s_2,
  ["b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 16

  [s_0, s_2, s_1, s_0, s_2, s_1, s_0, s_0, s_2, s_2, s_2, s_2,
    ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2], 16

[s_0, s_2, s_1, s_0, s_2, s_1, s_0, ["w", "b", "w", "b", "w"],
  ["w", "b", "w", "b", "w"], ["w", "b", "w", "b", "w"],
  ["w", "b", "w", "b", "w"], ["w", "b", "w", "b", "w"], s_1, s_1, s_0, s_2
  ], 16

[s_0, s_2, s_1, s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_0, s_0, s_0, s_0, s_2, s_1,
  s_1, s_0, s_2], 16

[s_0, s_2, s_1, s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
    ["b", "w", "b", "w", "b", "w", "b^2"], s_0,
    ["w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w"],
    ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 10

[s_0, s_2, s_1, s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0,
  s_0, s_0, s_0, s_0, s_2, s_1, s_1, s_0, s_2], 16

[s_0, s_2, s_1, s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0,
  s_0, ["w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 10

[s_0, s_2, s_1, s_0,
   ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"],
   ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], s_1, s_1,
   ["b", "w", "b", "w", "b", "w", "b^2"], ["w", "b", "w", "b", "w"]], 10

[s_0, s_2, s_1, s_0,
      ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"],
      ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], s_1,
      ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
```

```
      ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, s_2, s_1, ["w", "b", "w", "b", "w"], s_1, s_1, s_0, s_0, s_0,
  s_0, s_0, s_2, s_1, s_1, s_0, s_2], 16

[s_0, s_2, s_1, ["w", "b", "w", "b", "w"], s_1, s_1, s_0, s_0,
    ["w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w"],
    ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 10

[s_0, s_2, s_1, ["w", "b", "w", "b", "w"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["w", "b", "w", "b", "w"]], 10

[s_0, s_2, s_1, ["w", "b", "w", "b", "w"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"], ["b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b", "w", "b^2"], s_2
  ], 10

[s_0, s_2, s_1, ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_1,
   s_1, s_1, s_1, ["b", "w", "b", "w", "b", "w", "b^2"],
   ["w", "b", "w", "b", "w"]], 10
[s_0, s_2, s_1, ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_1,
   s_1, s_1, ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
   ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, s_2, s_1,
  ["w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w"],
  ["w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w"], s_2,
  s_2, s_1, s_0, ["w", "b", "w", "b", "w"]], 10

[s_0, s_2, s_1,
  ["w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w"],
  ["w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w"], s_2,
  s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, s_2, s_1,
  ["w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w"],
  ["w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w"], s_2,
  ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2], 10
```

```
[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"], s_2, s_1, s_1, s_0,
  s_0, s_0, s_0, s_0, s_2, s_1, s_1, s_0, s_2], 16

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"], s_2, s_1, s_1, s_0,
  s_0, ["w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"], s_2,
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["w", "b", "w", "b", "w"]], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"], s_2,
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"], ["b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b", "w", "b^2"], s_2
  ], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
     ["b^2", "w", "b", "w", "b", "w", "b"],
     ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_1, s_1,
     ["b", "w", "b", "w", "b", "w", "b^2"], ["w", "b", "w", "b", "w"]], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
         ["b^2", "w", "b", "w", "b", "w", "b"],
         ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_1,
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b^2"], ["b^2", "w", "b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], ["b^2", "w",
  "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], [
  "b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w",
  "b"], ["b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w",
  "b^2", "w", "b"], ["b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w",
  "b", "w", "b^2", "w", "b"], s_0, s_2], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2"], [
  "b", "w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w",
  "b^2"], ["b", "w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w",
  "b", "w", "b^2"], ["b", "w", "b^2", "w", "b^2", "w", "b", "w", "b", "w",
  "b", "w", "b", "w", "b^2"], ["b", "w", "b^2", "w", "b^2", "w", "b", "w",
  "b", "w", "b", "w", "b", "w", "b^2"], ["b", "w", "b^2", "w", "b^2", "w",
```

```
  "b", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, s_2, ["b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w",
  "b^2", "w", "b^2", "w", "b^2", "w", "b^2"], ["b", "w", "b", "w", "b", "w",
  "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2", "w", "b^2", "w", "b^2"],
  s_0, s_2, s_1, s_1, s_0, s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0, s_2, s_1, s_1, s_0,
  s_0, s_0, s_0, s_0, s_2, s_1, s_1, s_0, s_2], 16

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0, s_2, s_1, s_1, s_0,
  s_0, ["w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0, s_2,
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["w", "b", "w", "b", "w"]], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0, s_2,
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"], ["b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b", "w", "b^2"], s_2
  ], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0,
     ["b^2", "w", "b", "w", "b", "w", "b"],
     ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_1, s_1,
     ["b", "w", "b", "w", "b", "w", "b^2"], ["w", "b", "w", "b", "w"]], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0,
         ["b^2", "w", "b", "w", "b", "w", "b"],
         ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_1,
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], s_0, ["b^2", "w", "b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], ["b^2", "w",
  "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], [
  "b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w",
  "b"], ["b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w",
  "b^2", "w", "b"], ["b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w",
```

```
  "b", "w", "b^2", "w", "b"], s_0, s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], ["w", "b", "w", "b", "w"], s_2,
  s_1, s_1, s_1, s_1, ["b", "w", "b", "w", "b", "w", "b^2"],
  ["w", "b", "w", "b", "w"]], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], ["w", "b", "w", "b", "w"], s_2,
  s_1, s_1, s_1,
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], ["w", "b", "w", "b", "w"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"], s_0, ["w", "b", "w", "b", "w"]], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"], ["w", "b", "w", "b", "w"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], s_0, s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"],
   ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
   ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_2, s_2, s_2, s_1,
   s_0, ["w", "b", "w", "b", "w"]], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"],
      ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
      ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_2, s_2, s_2,
      ["b", "w", "b", "w", "b", "w", "b^2"],
      ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b"],
         ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
         ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_2, s_2,
         ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2], 10

[s_0, ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"], s_0, ["w", "b", "w", "b", "w"]], 10
```

```
[s_0, ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], s_0, s_2], 10

[["w", "b", "w", "b", "w"], s_1, s_0, s_2, s_1, s_1, s_0, s_0, s_0,
  s_0, s_0, s_2, s_1, s_1, s_0, s_2], 16

[["w", "b", "w", "b", "w"], s_1, s_0, s_2, s_1, s_1, s_0, s_0,
    ["w", "b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b", "w"],
    ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], s_1, s_0, s_2,
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
         ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], s_1, s_0, s_2,
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"], ["b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b", "w", "b^2"], s_2
  ], 10

[["w", "b", "w", "b", "w"], s_1, s_0, ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_1, s_1,
  ["b", "w", "b", "w", "b", "w", "b^2"], ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], s_1, s_0, ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_1,
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[["w", "b", "w", "b", "w"], s_1, s_0, ["b^2", "w", "b", "w", "b^2", "w",
  "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], ["b^2", "w", "b", "w",
  "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], ["b^2", "w",
  "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], [
  "b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w",
  "b"], ["b^2", "w", "b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w",
  "b^2", "w", "b"], s_0, s_2], 10
```

```
[["w", "b", "w", "b", "w"], s_1, ["w", "b", "w", "b", "w"], s_2, s_1, s_1,
  s_1, s_1, ["b", "w", "b", "w", "b", "w", "b^2"], ["w", "b", "w", "b", "w"]
  ], 10

[["w", "b", "w", "b", "w"], s_1, ["w", "b", "w", "b", "w"], s_2, s_1, s_1,
  s_1, ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[["w", "b", "w", "b", "w"], s_1, ["w", "b", "w", "b", "w"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"], s_0, ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], s_1, ["w", "b", "w", "b", "w"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], s_0, s_2], 10

[["w", "b", "w", "b", "w"], s_1,
   ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
   ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_2, s_2, s_2, s_1,
   s_0, ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], s_1,
      ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
      ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_2, s_2, s_2,
      ["b", "w", "b", "w", "b", "w", "b^2"],
      ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[["w", "b", "w", "b", "w"], s_1,
        ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
        ["w", "b", "w", "b", "w", "b", "w", "b^2", "w"], s_2, s_2,
        ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2], 10

[["w", "b", "w", "b", "w"], ["b", "w", "b", "w", "b", "w", "b^2"], s_2, s_2,
  s_1, s_1, s_1, s_1, ["b", "w", "b", "w", "b", "w", "b^2"],
  ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], ["b", "w", "b", "w", "b", "w", "b^2"], s_2, s_2,
  s_1, s_1, s_1,
  ["b", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10
```

```
[["w", "b", "w", "b", "w"], ["b", "w", "b", "w", "b", "w", "b^2"], s_2,
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"], s_0, ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"], ["b", "w", "b", "w", "b", "w", "b^2"], s_2,
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b"], s_0, s_2], 10

[["w", "b", "w", "b", "w"], ["b", "w", "b", "w", "b", "w", "b^2"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"],
  ["b^2", "w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2
  ], 10

[["w", "b", "w", "b", "w"],
   ["b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2"], s_2, s_2,
   s_2, s_2, s_2, s_1, s_0, ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w"],
   ["b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2"], s_2, s_2,
   s_2, s_2, s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
   ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10

[["w", "b", "w", "b", "w"],
   ["b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b^2"], s_2, s_2,
   s_2, s_2, ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2], 10

[["w", "b", "w", "b", "w"], ["b", "w", "b", "w", "b", "w", "b", "w", "b", "w",
  "b^2", "w", "b^2", "w", "b^2"], ["b", "w", "b", "w", "b", "w", "b", "w",
  "b", "w", "b^2", "w", "b^2", "w", "b^2"], s_0, s_0, s_2, s_1, s_1,
  s_0, s_2], 10

[["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"], ["w", "b", "w", "b", "w"],
  s_2, s_2, s_2, s_2, s_1, s_0, ["w", "b", "w", "b", "w"]], 10

[["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"], ["w", "b", "w", "b", "w"],
  s_2, s_2, s_2, s_2, ["b", "w", "b", "w", "b", "w", "b^2"],
  ["b", "w", "b", "w", "b", "w", "b^2"], s_2], 10
```

```
[["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"], ["w", "b", "w", "b", "w"],
  s_2, s_2, s_2, ["b^2", "w", "b", "w", "b", "w", "b"], s_1, s_0, s_2],
  10

[["w", "b", "w", "b", "w", "b", "w", "b^2", "w"],
    ["w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b", "w"],
    ["w", "b^2", "w", "b", "w", "b", "w", "b", "w", "b^2", "w", "b", "w"],
    ["w", "b", "w", "b", "w"], ["w", "b", "w", "b", "w"],
    ["w", "b", "w", "b", "w"], s_1, s_1, s_0, s_2], 10

[["w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w",
  "b^2", "w", "b^2", "w", "b^2", "w", "b^2", "w", "b^2", "w"], ["w", "b", "w",
  "b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b", "w", "b^2", "w",
  "b^2", "w", "b^2", "w", "b^2", "w", "b^2", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"],
  ["w", "b^2", "w", "b", "w", "b", "w", "b", "w"]], 4
>
```

Bibliografía

[1] D. Auroux. *Mapping class group factorizations and symplectic 4-manifolds: some open problems*. Problems on Mapping Class Groups and Related Topics, B. Farb Ed., Amer. Math. Soc., Proc. Symp. Pure Math., 74, 123–132 (2006). Referenciado en v, vi

[2] Robert E. Gompf. *Locally holomorphic maps yield symplectic structures*. Communications in analysis and geometry, ISSN 1019–8385, **13**(3), 511–525 (2005). Referenciado en v

[3] Yukio Matsumoto. *Diffeomorphism types of elliptic surfaces*. Proceedings of the Japan Academy, **61**(2), 55–58 (1985). Referenciado en vi, 22

[4] Boris Moishezon. *Complex surfaces and connected sums of complex projective planes*, ISBN 0387083553, Springer–Verlag, 1977. Referenciado en vi, 22

[5] Wikipedia. *Operación matemática*. http://es.wikipedia.org/wiki/Operaci%C3%B3n_matem%C3%A1tica, enero de 2008. Referenciado en 1

[6] Tomas W. Hungerford. *Algebra*, ISBN 0–387–90518–9. USA: Springer, 1974. Referenciado en 1

[7] John B. Fraleigh. *A first course in Abstract algebra*, fifth edition, ISBN 0–201–53467–3. USA: Addison–Wesley Publishing Company, Inc., 1967. Referenciado en 1

[8] Pierre Antoine Grillet. *Abstract Algebra*, second edition, eISBN 978-0-387-71568-1. USA: Springer Science + Business Media, LLC, 2007. Referenciado en 1

[9] PlanethMath.org. http://planetmath.org/encyclopedia/FinitelyGeneratedSubgroup.html y http://planetmath.org/encyclopedia/ScheierIndexFormula.html, junio de 2009. Referenciado en 1

[10] Wikipedia. *Group theory*. http://en.wikipedia.org/wiki/Group_theory, junio de 2009. Referenciado en 1

[11] José F. Caicedo C. *Teoría de grupos*, ISBN 958–701–348–4. Colombia: Pro–Offset Editorial Ltda, 2004. Referenciado en 1

[12] Wikipedia. *Free product*. http://en.wikipedia.org/wiki/Free_product, enero de 2010. Referenciado en 1

[13] Joseph J. Rotman *An Introduction to the Theory of Groups*, fourth edition, ISBN 978–0–387–94285–8. New York: Springer–Verlag, 1995. Referenciado en 1

[14] Keith Conrad. $SL(2,\mathbb{Z})$. http://www.math.uconn.edu/ kconrad/blurbs/group theory/SL(2,Z).pdf, febrero de 2010. Referenciado en 22

[15] Svetlana Katok. Fuchsian groups, ISBN 0–226–42583–5, The University of Chicago Press, USA, 1992. Referenciado en 22

[16] Roger C. Alperin. $PSL(2,\mathbb{Z}) = \mathbb{Z}_2 * \mathbb{Z}_3$. The American Mathematical Monthly, ISSN 0002–9890, **100**(4), 385–386 (1993). Referenciado en 22

[17] Carlos A. Cadavid and Juan D. Vélez. On a minimal factorization conjecture. Topology and its Applications, ISSN 0166–8641, **154**(15), 2786—2794 (2007). Referenciado en 22

[18] Wikipedia. *Modular group*. http://en.wikipedia.org/wiki/Modular_group, febrero de 2010. Referenciado en 22

[19] Eric W. Weisstein. *CRC Concise encyclopedia of mathematics*, 2 edition, ISBN 978–1584883470, Chapman & Hall/CRC, 2002. Referenciado en 22

[20] Carlos Prieto. *Topología básica*, ISBN 968–16–7093–0. México, D.F.: Fondo de Cultura Económica, 2003. Referenciado en 22

[21] Marcel Berger. *Encounter with a geometer, part I*. Notices of the AMS, ISSN 0002–9920, **47**(2), February 2000. Referenciado en 22

[22] John G. Ratcliffe. Foundations of hyperbolic manifolds, ISBN 978-0-387-47322-2, Springer–Verlag, New York, 2006. Referenciado en 22

[23] Robert Friedman and John W. Morgan. Smooth Four-Manifolds and Complex Surfaces, ISBN 978-3-540-57058-5, Springer, 1994. Referenciado en 22

[24] A. G. Khovanskii and Smilka Zdravkovska. Branched covers of S^2 and braid groups, 1996. Referenciado en 22