

# Capítulo 1

## Grupos virtualmente libres.

En este capítulo veremos como entran en juego las diferentes áreas de la matemática para definir de manera equivalente a los grupos virtualmente libres.

**DEFINICIÓN 1.0.1.** Un grupo  $G$  finitamente generado es **virtualmente libre** si existe un subgrupo libre  $F$  tal que su índice en  $G$  es finito.

Veamos algunas propiedades elementales que cumplen todos los grupos virtualmente libre. Antes probemos algunos lemas sobre grupos.

**DEFINICIÓN 1.0.2.** Sea  $G$  un grupo y  $H$  un subgrupo entonces el normalizador de  $H$  en  $G$  es el siguiente subgrupo

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

Denotaremos por  $S = \{g \in G : gHg^{-1} \neq H\}$  al conjunto de conjugados del subgrupo  $H$ .

**LEMA 1.0.3.** Si  $G$  es un grupo finitamente generado y  $H$  es un subgrupo de índice finito entonces  $N_G(H)$  tiene índice finito y más aún  $[G : N_G(H)] = |S|$ .

**Demostración.** Para ver que tiene índice finito notemos que  $H \leq N_G(H)$  por lo tanto tenemos que

$$[G : N_G(H)] \leq [G : H] < \infty.$$

Para probar la otra afirmación definimos la siguiente función hacia los cosets a derecha del normalizador desde el conjunto  $S$ ,

$$\begin{aligned} S &\rightarrow G/N_G(H) \\ sHs^{-1} &\mapsto N_G(H)s \end{aligned}$$

Veamos que es biyectiva.

Si  $N_G(H)s = N_G(H)t$  entonces tenemos que esto sucede si y solo si  $st^{-1} \in N_G(H)$ . Esto nos dice que por la definición del normalizador,

$$st^{-1}Hts^{-1} = H \iff s^{-1}Hs = t^{-1}Ht$$

y de esta manera obtenemos que la función está bien definida y es biyectiva. ■

**LEMA 1.0.4.** *Sea  $G$  un grupo finitamente generado y sean  $K, H$  subgrupos de índice finito entonces  $K \cap H$  es un subgrupo de índice finito.*

**Demostración.** Primero notemos que por el segundo teorema de isomorfismo para grupos tenemos que existe una biyección entre los siguientes conjuntos,

$$KH/K \simeq K/K \cap H$$

y en particular como  $|KH/K| \leq |G/K| < \infty$  por hipótesis obtenemos así que  $|K/K \cap H| < \infty$ .

Finalmente por una propiedad de índices de subgrupos obtenemos lo siguiente

$$[G : K \cap H] = [G : K][K : K \cap H]$$

y como ambos índices de la derecha son finitos por lo visto obtenemos que  $K \cap H$  es un subgrupo de índice finito también tal como queríamos ver. ■

**LEMA 1.0.5.** *Sea  $G$  un grupo finitamente generado y sea  $H$  subgrupo de índice finito entonces  $H$  es un grupo finitamente generado.*

**Demostración.** Sea  $A = \{g_1, \dots, g_n\}$  conjunto finito de generadores de  $G$ . Sea  $T = \{t_1, \dots, t_m\}$  conjunto transversal a derecha de  $H$ , esto es que  $Ht_1, \dots, Ht_k$  son todos los cosets a derecha de  $H$  sobre  $G$ . Supongamos que  $t_1 = 1$  dado que es el representante del coset  $H$ .

Dado  $g_j$  generador de  $G$  debe existir  $h_{ij} \in H$  tal que  $h_{ij}t_k = t_i g_j$  para cierto  $t_k$ . También debe existir  $h_i \in H$  de manera que  $h_i t_k = g_i$  para cierto  $t_k$ . Veamos que el conjunto finito

$$B = \{h_{ij}\}_{1 \leq i, j \leq n} \cup \{h_i\}_{1 \leq i \leq n}$$

genera a  $H$ .

Dado  $h \in H$  tenemos que

$$h = g_{i_1} \dots g_{i_r}$$

donde usamos el conjunto finito de generadores de  $G$ .

Por lo visto anteriormente podemos escribir  $g_{i_1} = h_{i_1} t_{k_1}$  y entonces nos queda la siguiente escritura de  $h$ ,

$$h = h_{i_1} t_{k_1} g_{i_2} \dots g_{i_r}$$

entonces usando que  $h_{k_1 i_2} t_{k_2} = t_{k_1} g_{i_2}$  llegamos a la siguiente escritura de  $h$ ,

$$h = h_{i_1} h_{k_1 i_2} t_{k_2} \dots g_{i_r}.$$

Repitiendo inductivamente este procedimiento llegamos a que  $h = h_{i_1} h_{k_1 i_2} \dots t_{k_r}$ . Este  $t_{k_r}$  tiene que ser 1 porque justamente  $h \in H$ , por lo tanto tenemos  $B$  es un conjunto finito de generadores de  $H$ . ■

Con esto podemos probar estos resultados elementales de grupos virtualmente libre.

**PROPOSICIÓN 1.0.6.** *Para todo grupo  $G$  virtualmente libre valen las siguientes propiedades.*

1. *Si  $F$  es un subgrupo libre de índice finito entonces podemos tomarnos otro subgrupo  $F'$  de manera que sea normal, libre y de índice finito.*
2. *Si  $H$  es un subgrupo de  $G$  de índice finito entonces  $H$  también resulta ser virtualmente libre.*

#### **Demostración.**

1. Si  $G$  es virtualmente libre y  $F$  es un subgrupo libre tenemos que la cantidad de conjugados de  $F$  es finita por el lema 1.0.3. Por lo tanto podemos considerar el siguiente subgrupo normal

$$F' = \bigcap_{g \in G} g F g^{-1}$$

donde la cantidad de grupos que estamos intersecando es finita y es normal por construcción. Veamos que  $F'$  nos sirve. Para ver que tiene índice finito nos alcanza con usar el lema 1.0.4 e inducción para que valga para una intersección finita arbitraria. Como tiene índice finito usando 1.0.5 sabemos entonces que es un grupo finitamente generado. Finalmente notemos que es libre por el resultado ?? que nos dice que todo subgrupo de un grupo libre es libre, en particular al ser  $F'$  subgrupo de  $F$  que es libre obtenemos que  $F'$  es libre tal como queríamos ver.

2. Por el lema 1.0.5 obtenemos directamente que  $H$  es grupo finitamente generado. Si  $F$  es un libre de índice finito en  $G$  podemos tomar  $H \cap F$  que es libre por ser subgrupo de un libre de acuerdo al resultado ?. El índice resulta ser finito puesto que

$$[H : F \cap H] \leq [G : F] < \infty.$$



OBSERVACIÓN 1.0.7. Dado  $G$  virtualmente libre vamos a construirnos una presentación en particular.

Como es un grupo virtualmente libre tenemos  $F$  subgrupo libre que podemos tomarlo normal y  $G/F$  grupo finito de manera que podemos escribir a  $G$  como una extensión de estos dos grupos por medio de la siguiente forma

$$1 \longrightarrow F \xrightarrow{\iota} G \xrightarrow{\pi} G/F \longrightarrow 1$$

Consideremos que  $F$  es libre generado por  $Y = \{y_1, \dots, y_n\}$ . Por otro lado sea  $G/F = \{b_i : 1 \leq i \leq m\}$  todos los elementos de este conjunto finito. Elegimos un transversal a derecha  $T = \{t_1, \dots, t_m\}$  de manera que  $\pi(t_i) = b_i$  y  $t_1 = 1$ .

Dado que es un transversal tenemos que se deben cumplir las siguientes dos relaciones para  $y_j \in Y$  y  $t_i, t_j, t_k \in T$ .

1.  $t_i y_j t_i^{-1} = u_{ij}$  donde  $u_{ij} \in F$  usando que  $F$  es normal.
2. Si tenemos que  $b_i b_j = b_k$  entonces  $t_i t_j = z_{ij} t_k$  donde  $z_{ij} \in F$  usando que  $(Ht_i)(Ht_j) = Ht_k$ .

Afirmamos que la siguiente es una presentación finita de  $G$ .

$$\langle W \mid R \rangle = \langle y_1, \dots, y_n, t_1, \dots, t_m \mid t_i y_j t_i^{-1} = u_{ij}, t_i t_j = z_{ij} t_k \rangle.$$

Sea el grupo que genera esta presentación  $H$  y sea  $F'$  el grupo libre sobre sus generadores.

Notemos que  $W = Y \cup T$  genera a  $G$  porque justamente  $F$  es libre y generado por  $Y$  y  $T$  es un conjunto transversal finito porque  $F$  tiene índice finito en  $G$ . Esto nos dice que tenemos un epimorfismo de grupos de  $F'$  en el grupo  $G$ .

Toda relación de  $G'$  la cumple el grupo  $G$  por la elección que tomamos, de esta manera tenemos un epimorfismo de grupos  $\bar{\varphi}$  tal que hace conmutar al siguiente diagrama,

$$\begin{array}{ccc} F' & \xrightarrow{\varphi} & G \\ \downarrow & \nearrow \bar{\varphi} & \\ H & & \end{array}$$

El grupo  $G$  es tal que a toda palabra  $w$  en sus generadores la podemos llevar a que sea de la pinta

$$w = yt$$

donde  $y \in F$  reducida y  $t \in T$  es alguno de los transversales. Para llegar a esto hacemos el mismo procedimiento que hicimos en la demostración del lema 1.0.5.

De esta manera una palabra es trivial si y solamente si  $y = 1$  y  $t = 1$ . Esto nos dice que  $\bar{\varphi}(w) = 1$  si y solamente si  $w = 1$ . Concluimos así que  $\bar{\varphi}$  es un isomorfismo de grupos tal como queríamos ver y por lo tanto  $\langle W \mid R \rangle$  resultó ser una presentación de  $G$ .

Veamos ahora unos ejemplos y contraejemplos de grupos virtualmente libres.

**EJEMPLO 1.0.8.** Veamos algunos ejemplos elementales de grupos que son de esta familia y algunos que no lo sean.

1. Cualquier extensión de un grupo libre por un grupo finito es un grupo virtualmente libre,

$$1 \rightarrow F \rightarrow G \rightarrow K \rightarrow 1$$

donde  $K$  es un grupo finito y  $F$  es un grupo finitamente generado libre. En particular esto nos da los casos más elementales de productos directos y semidirectos, esto es  $G = F \times K$  o bien  $G = F \rtimes K$ . En este capítulo veremos que todo grupo virtualmente libre podemos considerarlo como un subgrupo de una extensión de este tipo.

2. El ejemplo más sencillo de un grupo que no es virtualmente libre es  $\mathbb{Z} \times \mathbb{Z}$ . La primera observación es que al ser abeliano si tiene un subgrupo libre necesariamente tiene que ser isomorfo a  $\mathbb{Z}$ .

Nos alcanza con ver que no es virtualmente  $\mathbb{Z}$ . Sea  $F$  un subgrupo que es isomorfo a  $\mathbb{Z}$ . Sea  $(n, m) \in \mathbb{Z} \times \mathbb{Z}$  el generador de  $F$ . Probaremos que  $\mathbb{Z} \times \mathbb{Z}/F$  tiene orden infinito. Para eso consideraremos  $(p, q) \in \mathbb{Z} \times \mathbb{Z}$  tal que  $p, q$  son primos distintos y ambos coprimos con  $m, n$ . Veamos que  $[(p, q)] \in \mathbb{Z} \times \mathbb{Z}/F$  tiene orden infinito. Si no lo fuera deberían existir  $\alpha, \beta \in \mathbb{Z}$  de manera que

$$\alpha(p, q) = \beta(n, m)$$

como todos son coprimos entre sí esto nos dice que  $p \mid \beta$  y similarmente que  $q \mid \beta$ , por lo que tenemos que  $q \mid \alpha$  y  $p \mid \alpha$ . Esto nos dice que se pueden escribir de esta manera

$$\begin{aligned}\alpha &= p^{r_1} q^{s_1} \gamma_1 \\ \beta &= p^{r_2} q^{s_2} \gamma_2\end{aligned}$$

con  $r_i, s_i \geq 1$  para  $i = 1, 2$ .

Finalmente como

$$\alpha p = \beta n$$

tenemos que  $r_1 + 1 = r_2$  pero por otro lado como

$$\alpha q = \beta m$$

acá tenemos que al ser  $m$  coprimo con  $p$  luego la multiplicidad de  $p$  en la descomposición en primos de lo que está a la izquierda es  $r_2 - 1$  mientras que lo que está a la derecha es  $r_2$ .

Esto es una contradicción que vino de suponer que  $[(p, q)] \in \mathbb{Z} \times \mathbb{Z}/F$  tenía orden finito por lo tanto tenemos que  $\mathbb{Z} \times \mathbb{Z}$  no puede ser virtualmente libre.

### §1.1. Grupos independientes de contexto.

OBSERVACIÓN 1.1.1. Si tenemos un grupo  $G$  tal que es independiente de contexto consideremos  $\mathcal{G}$  gramática que genera al lenguaje del problema de la palabra,  $WP(G, \Sigma) = L(\mathcal{G})$ . Si  $A$  es una de las variables de esta gramática podemos obtener el lenguaje  $L_A$  de palabras generadas a partir de esta variable, donde

$$L_A = \{w \in \Sigma^* \mid A \xRightarrow{*}_{\mathcal{G}} w\}.$$

Veamos que si  $v, v' \in L_A$  entonces  $v =_G v'$ , es decir son el mismo elemento vistos en el grupo  $G$ . Para eso si tenemos una derivación que en algún momento llega a  $S \xRightarrow{*}_{\mathcal{G}} \beta A \gamma \xRightarrow{*}_{\mathcal{G}} uvw$  también tenemos otra derivación que deriva en  $S \xRightarrow{*}_{\mathcal{G}} \beta A \gamma \xRightarrow{*}_{\mathcal{G}} uv'w$ . Es decir que  $uvw, u'v'w' \in WP(G, \Sigma)$  por lo tanto

$$uvw =_G 1 =_G uv'w \implies v =_G v'$$

tal como queríamos ver.

Una pregunta natural es intentar entender la relación entre la clasificación del lenguaje del problema de la palabra de un grupo dado y las distintas familias de grupos que le corresponden. La siguiente demostración generaliza la construcción del ejemplo del problema de la palabra de un grupo libre.

|| **TEOREMA 1.1.2.** *[?] Todo grupo virtualmente libre es independiente de contexto.*

**Demostración.** Sea  $G$  grupo virtualmente libre y consideremos una presentación  $\langle W \mid R \rangle$  como la que construimos en la observación 1.0.7. Veamos de construir un autómata de pila de manera que acepte al lenguaje  $WP(G, W)$ . Antes de definirlo consideremos algunos conjuntos finitos que nos van a servir para definir al autómata.

Si tenemos que  $t_j y_i = u_{ij} t_j$  y que  $t_i t_j = z_{ijk} t_k$  luego consideremos la siguiente definición. El conjunto finito  $U = \{u_{ij}, z_{ijk} : 1 \leq i, j, k \leq n\}$ . Consideremos  $\text{Pre}(U) =$

$\{u' \in Y^* : u'v \in U\}$  el conjunto de los prefijos de las palabras en  $U$  que sabemos es finito también. Sea entonces el conjunto finito  $Q = T \times T \cup Y \times \text{Pre}(U)$ .

Con estas definiciones ahora nuestro autómata lo definimos así:

$$\mathcal{M} = (Q, W, Y, \delta, (1, 1, 1), \{(1, 1, 1)\})$$

El conjunto  $Q$  van a ser nuestros estados. El alfabeto de entrada es  $W$  que es el conjunto de generadores del grupo. El alfabeto de la pila es  $Y$  que es el conjunto de generadores del subgrupo libre  $F$ . Nuestro estado inicial que también es el final corresponde a  $(1, 1, 1)$ .

Ahora podemos definir la función de transición. Sea  $w_i \in W$  algún generador del grupo luego tenemos que

$$\begin{aligned}\delta(y_i w', (t_j, 1, 1), v) &= (w', (t_j, y_i, 1), v) \\ \delta(t_i w', (t_j, 1, 1), v) &= (w', (t_k, t_i, 1), v)\end{aligned}$$

de manera que si estamos en  $T \times \{1\} \times \{1\}$  podemos pasar a la segunda coordenada correspondiente a la letra de  $W$  que hayamos leído. Ahora en esta instancia lo que vamos a hacer es la reducción del producto de  $u_{ij} \cdot v$  o bien el de  $z_{ijk} \cdot v$  respectivamente una letra a la vez. Para esto tenemos

$$\delta(w', (t_j, w_i, u), v) = (w', (t_j, w_i, y_i u), y_i \cdot v).$$

siempre y cuando  $y_i u$  sea un prefijo de la palabra de  $U$  correspondiente. Notemos que sigue siendo determinístico porque fijamos de antemano alguna escritura única en los generadores  $Y$  para cada palabra  $u \in U$ . En la pila hacemos la reducción en el grupo libre de multiplicar por una letra. Finalmente la función de transición la definimos para que podamos volver una vez que ya reducimos toda la palabra  $u \in U$ . Para eso tenemos

$$\delta(w', (t_j, w_i, u), v) = (w', (t_j, 1, 1), v).$$

en el caso que  $u \in U$ , es decir que ya hicimos toda la reducción.

Una vez definido este autómata consideremos ahora el lenguaje aceptado por pila vacía y estado final a la vez,

$$\mathcal{L}(\mathcal{M}) = \{w \in W^* \mid (w, 1, 1) \vdash^* (1, 1, 1)\}$$

Debemos ver que el autómata acepta justamente al lenguaje que queremos. Esto es que  $\mathcal{L}(\mathcal{M}) = \text{WP}(G, W)$

Dada una palabra  $w \in W^*$  por como es esta presentación sabemos que se puede escribir como  $w = vt$  donde  $v \in F$  reducida y  $t \in T$ . De esta manera  $w \in \text{WP}(G, W)$

si y solo si  $v = 1, t = 1$ . Notemos que el autómata en toda transición no hace más que reescribir la cadena de izquierda a derecha tal como hicimos en la observación 1.0.7. Esto es que cuando termina de consumir la cadena de entrada llegamos a la configuración  $(1, t_i, v)$  es decir que  $w = vt_i$ . Por lo tanto como aceptamos por estado final y pila vacía esto nos dice que  $w \in \text{WP}(G, W)$  si y solo si  $w \in \mathcal{L}(M)$ .

Con esto probamos que los grupos virtualmente libres son independiente de contexto usando la equivalencia ??.

■

El siguiente resultado es un teorema de Muller–Schupp demostrado en [?]. La demostración sigue la exposición del paper [?].

**TEOREMA 1.1.3.** [?] *Todo grupo independiente de contexto es tal que su grafo de Cayley tiene treewidth finito.*

**Demostración.** La descomposición que hicimos en ?? es válida para todo grafo de Cayley. Veamos que esta descomposición para un grupo independiente de contexto tiene treewidth finito. Buscamos  $k \in \mathbb{N}$  tal que nos permita acotar  $|\beta C| \leq k$  para todo  $\beta C \in V(T)$ . Alcanza con ver que los diámetros de los bolsones  $\beta C$  están acotados uniformemente, esto es que exista  $M \in \mathbb{N}$  tal que

$$\text{diam}(\beta C) = \sup_{g, h \in \beta C} d(g, h) \leq M$$

para todo  $\beta C$  de la descomposición de árboles. Si esto sucede, al ser el grupo finitamente generado por  $\Sigma$  entonces  $|\beta C| \leq |\Sigma|^M < \infty$ .

Dado que  $G$  es un grupo independiente de contexto entonces el lenguaje del problema de la palabra para estos generadores  $\text{WP}(G, \Sigma)$  tiene una gramática  $\mathcal{G}$  independiente de contexto que lo genera. Consideremos que está en la forma normal de Chomsky.

Para cada variable  $A$  de nuestra gramática podemos considerar el siguiente lenguaje

$$L_A = \{w \in \Sigma^* : A \Rightarrow_{\mathcal{G}}^* w\}.$$

Para este lenguaje introduzcamos un número natural  $k_A \in \mathbb{N}$  definido por  $k_A = \min_{w \in L_A} |w|$ . Como tenemos finitas variables en nuestra gramática  $\mathcal{G}$  podemos considerar  $k = \max_{A \in V} k_A$ . Veamos que  $\text{diam}(\beta C) \leq 3k$  para todo  $\beta C \in V(T)$ .

Sean  $g, h \in \beta C$  para cierta  $C$  componente conexa de  $V_n$ , acotemos  $d(g, h)$ . Para eso consideremos una geodésica  $\alpha$  que una 1 con  $g$  y análogamente otra  $\gamma$  que una 1 con  $h$ . Como  $C \cup \beta C$  es conexo podemos tomar un arco  $\tau$  que una  $g$  con  $h$  dentro de  $C \cup \beta C$ . De esta manera tenemos un triángulo tal que si leemos las letras que están en la etiqueta del arco empezando desde 1 y moviéndonos por  $\alpha$  leemos la etiqueta  $u$ . Cuando nos movemos por  $\tau$  leemos la etiqueta  $v$ . Consideremos que esta etiqueta



$v$  es tal que  $|v| > 1$  caso contrario ya tenemos la cota probada. Finalmente leemos la etiqueta  $w$  cuando regresamos al 1 por medio de  $\gamma$ . Como  $uvw$  está en un ciclo en el grafo de Cayley entonces  $uvw \in \text{WP}(G, \Sigma)$  y por lo tanto tenemos alguna derivación  $S \Rightarrow_G^* uvw$ .

Ya que tenemos esta derivación  $S \Rightarrow_G^* uvw$  miremos la primer variable que deriva a  $v$  como subpalabra. Esto es que para la subpalabra  $v$  sabemos que existe alguna variable  $A$  tal que  $A \Rightarrow_G^* v'v''$  donde  $v$  es a su vez una subpalabra de  $v'v''$ . Tomamos la última variable que aparece en la derivación. Ésta debe existir porque en particular  $S$  cumple lo pedido de ser una variable que deriva a una palabra que contiene a  $v$  como subpalabra.

Como está en la forma normal de Chomsky sabemos que al ser  $|v| \geq 2$  entonces tenemos que la derivación tiene la siguiente pinta

$$S \Rightarrow_G^* u'Aw' \Rightarrow_G u'BCw' \Rightarrow_G^* u'v'v''w'$$

donde  $B, C$  son otras variables. En particular notemos que  $A \Rightarrow_G^* v'v''$ ,  $B \Rightarrow_G^* v'$  y  $C \Rightarrow_G^* v''$ .

Si miramos la geodésica  $\alpha$  sabemos que cuando leímos  $u'$  habremos llegado a un vértice del grafo  $x$ , y al estar sobre la geodésica misma tenemos la siguiente igualdad,

$$d(x, g) = d(1, g) - d(1, x).$$

Análogamente cuando miramos la geodésica  $\gamma$  en la instancia que ya leímos  $w'$  saliendo desde  $h$  llegamos a cierto vértice  $z$  y por la misma razón que en el caso anterior obtenemos

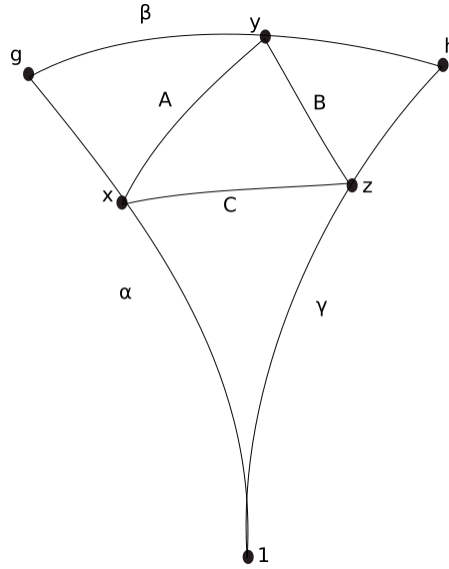
$$d(z, h) = d(1, h) - d(1, z).$$

Por otro lado si consideramos el vértice  $y$  al que llegamos después de leer  $u'v'$  que sabemos que está en el arco  $\tau$  dado que  $v$  es subpalabra de  $v'v''$ . Usando que  $y \in \tau \subseteq C \cup \beta C$  tenemos que  $d(1, y) \leq n + 1 = d(1, g)$  por ser  $C$  una componente conexa de  $V_n$ , entonces vale la siguiente desigualdad

$$d(x, g) = d(1, g) - d(1, x) \leq d(1, y) - d(1, x) = d(x, y)$$

y análogamente tenemos que  $d(z, h) \leq d(z, y)$ .

Por la observación 1.1.1 notemos que si reemplazamos  $v'$  por la palabra de menor tamaño del lenguaje  $L_B$  seguimos teniendo un ciclo pero de longitud idéntica o más chica. La palabra  $v'$  la leemos justamente cuando vamos del vértice  $x$  al vértice  $y$ , así la distancia  $d(x, y)$  está acotada por la mayor de todas las palabras que puedan derivarse de  $B$ . Idénticamente hacemos esto para las variables  $A$  y  $C$ . Por como definimos a  $k$  tenemos las siguientes cotas  $d(x, y), d(y, z), d(x, z) \leq k$ .



Ahora estamos listos para ver que  $d(g, h) \leq 3k$ . Usamos la desigualdad triangular tres veces,

$$\begin{aligned} d(g, h) &\leq d(g, x) + d(x, z) + d(h, z) \\ &\leq d(x, y) + d(x, z) + d(y, z) \leq 3k \end{aligned}$$

tal como queríamos ver. ■

**EJEMPLO 1.1.4.** Ejemplo de  $PSL(2, \mathbb{Z})$  o de algún otro grupo que sea un producto libre de grupos finitos.