Grupos Libres

Mariano Suárez-Alvarez

19 de marzo, 2007

Índice

1 Monoides libres 1

2 Grupos libres 4

3 Palabras reducidas 6

4 Presentaciones 13

5 Enumeración de coclases 17
Grafos de Cayley 17
Grafos de Cayley 17

6 Subgrupos: el teorema de Nielsen-Schreier 19

1. Monoides libres

1.1. Sea X un conjunto.

1.2. Una *palabra* sobre X es una sucesión finita $w = x_1 \cdots x_n$ de elementos de X con $n \in \mathbb{N}_0$. En particular, la palabra con cero letras es una palabra, que escribimos 1. Sea $\mathsf{M}(X)$ el conjunto de todas las palabras sobre X.

1.3. La *longitud* $|w|$ de una palabra $w \in \mathsf{M}(X)$ es la cantidad de letras que la componen. Así, $|1| = 0$ y $|x_1 \cdots x_n| = n$.

1.4. Cuando esto no introduzca confusiones, identificaremos los elementos de X con las palabras de $\mathsf{M}(X)$ de longitud 1.

1.5. Sobre $\mathsf{M}(X)$ definimos un producto $\cdot : \mathsf{M}(X) \times \mathsf{M}(X) \to \mathsf{M}(X)$ de la siguiente manera. Sean $a, b \in \mathsf{M}(X)$. Si $a = 1$, ponemos $a \cdot b = 1$; si $b = 1$, ponemos $a \cdot b = a$. Finalmente, si $a = x_1 \cdots x_n$ y $b = y_1 \cdots y_m$ son ambas no vacías, ponemos $a \cdot b = x_1 \cdots x_n y_1 \cdots y_m$.

1.6. Proposición. *$(\mathsf{M}(X), \cdot)$ es un monoide.*

Demostración. La definición misma del producto de $\mathsf{M}(X)$ implica que 1 es un elemento neutro. La asociatividad es clara. □

1.7. Es fácil verificar que la aplicación $|\cdot| : \mathsf{M}(X) \to \mathbb{N}_0$ es un morfismo de monoides.

1.8. Proposición. *Sea X un conjunto, G un monoide y sea $f : X \to G$ una función arbitraria. Entonces existe exactamente un homomorfismo de monoides $\bar{f} : \mathsf{M}(X) \to G$ tal que $\bar{f}(x) = f(x)$ para todo $x \in X$.*

Demostración. Definamos $\bar{f} : \mathsf{M}(X) \to G$ de la siguiente manera. Ponemos $\bar{f}(1) = 1$ y si $a = x_1 \cdots x_n \in \mathsf{M}(X)$ es una palabra no vacía, entonces ponemos

$$\bar{f}(a) = f(x_1) \cdots f(x_n).$$

Es fácil ver que esto define un homomorfismo de monoides. Dejamos la unicidad al lector. □

1.9. Si $u, v \in \mathsf{M}(X)$, decimos que u es un *prefijo* (*sufijo*) de v si existe $\lambda \in \mathsf{M}(X)$ tal que $v = u\lambda$ ($v = \lambda u$, respectivamente).

1.10. En lo que sigue haremos uso frecuente, sin mencionarlo, de las siguientes observaciones:

Proposición. *Sean $\alpha, \beta, \gamma, \delta \in \mathsf{M}(X)$ tales que $\alpha\beta = \gamma\delta$.*
(a) *Si $\alpha = \gamma$, entonces $\beta = \delta$.*
(b) *Si $|\alpha| = |\gamma|$, entonces $\alpha = \gamma$.*
(c) *Si $|\alpha| \leq |\gamma|$, entonces α es un prefijo de γ y δ es un sufijo de β.* □

1.11. Si $X = \emptyset$, es claro que $\mathsf{M}(X) = 1$ es el monoide trivial.

1.12. Si $X = \{x\}$, entonces $|\cdot| : \mathsf{M}(X) \to \mathbb{N}_0$ es un isomorfismo de monoides.

1.13. Si $X \neq \emptyset$, entonces $\mathsf{M}(X)$ es infinito. En efecto, toda palabra no vacía $w \in \mathsf{M}(X) \setminus 1$ tiene orden infinito.

1.14. En $\mathsf{M}(X)$ los elementos solo conmutan por razones triviales:

Proposición. *Sean $u, v \in \mathsf{M}(X)$ tales que $uv = vu \neq 1$. Entonces existen $w \in \mathsf{M}(X)$ y $k, l \in \mathbb{N}_0$ tales que $u = w^k$ y $v = w^l$.*

Demostración. Hagamos inducción sobre $|uv|$. Si $u = 1$, $v = 1$ ó $u = v$, el resultado es evidente. Supongamos entonces que no es ése el caso. Sin pérdida de generalidad, además, podemos suponer que $|u| < |v|$.

Existe entonces $\lambda \in \mathsf{M}(X)$ tal que $v = u\lambda$. Es $|\lambda| < |v|$; por otro lado, tenemos que $uu\lambda = uv = vu = u\lambda u$, así que $u\lambda = \lambda u$. Usando la hipótesis inductiva vemos que existen $w \in \mathsf{M}(X)$ y $k, l \in \mathbb{N}_0$ tales $u = w^k$ y $\lambda = w^l$. Esto implica que también $v = u\lambda = w^{k+l}$.

La proposición sigue entonces por inducción. □

1.15. Decimos que una palabra no vacía $u \in \mathsf{M}(X) \setminus 1$ es *primitiva* si no existen $k \in \mathbb{N}$ y $v \in \mathsf{M}(X)$ tales que $u = v^k$ y $k \geq 2$.

Proposición. *Sea $u \in \mathsf{M}(X) \setminus 1$. Entonces existen $k \in \mathbb{N}$ y $u_0 \in \mathsf{M}(X)$ tales que u_0 es primitiva y $u = u_0^k$. Tanto k como u_0 están unívocamente determinados por u. Además, si $v \in \mathsf{M}(X)$ y $l \in \mathbb{N}$ son tales que $u = v^l$, entonces $l \mid k$ y $v = u_0^{k/l}$.*

Demostración. Sea $k = \max\{i : \text{existe } v \in \mathsf{M}(X) \text{ tal que } v^i = k\}$; esto tiene sentido porque el conjunto considerado está acotado superiormente por $|u|$. Notemos que $k > 0$.

Sea $u_0 \in \mathsf{M}(X)$ tal que $u = u_0^k$. Si u_0 no es primitiva, entonces existe $w \in \mathsf{M}(X)$ y $l \geq 2$ tal que $u_0 = w^l$. Pero entonces es $u = u_0^k = w^{kl}$ y $kl \geq 2k > k$. Esto es imposible. Vemos así que u_0 debe ser primitiva.

Para terminar, supongamos que $v \in \mathsf{M}(X)$ y $l \in \mathbb{N}$ son tales que $u_0^k = v^l$. Esto implica, por supuesto, que $u_0 v^l = v^l u_0$, así que **1.14** nos dice que existen $w \in \mathsf{M}(X)$ y $s, t \in \mathbb{N}$ tales que $u_0 = w^s$ y $v^l = w^t$. Como u_0 es primitiva, debe ser $s = 1$ y $u_0 = w$. Entonces $v^l = u_0^t$ y $u = v^l = u_0^{lt}$; esto implica que $lt = k$, de manera que $l \mid k$ y $v = u_0^{k/l}$.

Si además v es primitiva, debe ser $k/l = 1$ y $v = u_0$. Esto demuestra la unicidad de k y u_0. □

1.16. Con estos dos resultados, es fácil describir el centro y los centralizadores de elementos en $\mathsf{M}(X)$:

Proposición. *Supongamos que $|X| > 1$. Entonces $\mathsf{Z}(\mathsf{M}(X)) = 1$. Además, si $u \in \mathsf{M}(X) \setminus 1$ y u_0 es la palabra primitiva tal que existe $k \in \mathbb{N}$ con $u = u_0^k$, entonces $\mathsf{C}(u) = \langle u_0 \rangle$*

Demostración. Supongamos que $u \in \mathsf{Z}(\mathsf{M}(X)) \setminus 1$ y sean $x, y \in X$ tales que $x \neq y$. Como $ux = xu$ y $uy = yu$, **1.14** nos dice que existen $w \in \mathsf{M}(X)$ y $k, l \in \mathbb{N}_0$ tales que $u = x^k = y^l$. Claramente esto es imposible. Esto prueba la primera afirmación.

Sea ahora $u \in \mathsf{M}(X) \setminus 1$ y supongamos que $v \in \mathsf{C}(u)$. Usando otra vez **1.14**, vemos que existen $w \in \mathsf{M}(X)$ y $k, l \in \mathbb{N}_0$ tales que $u = w^k$ y $v = w^l$. La proposición **1.15** implica entonces que existe $m \in \mathbb{N}$ tal que $w = u_0^m$. Pero esto nos dice que $v = w^l = u_0^{lm} \in \langle u_0 \rangle$. Así, $\mathsf{C}(u) \subset \langle u_0 \rangle$. La inclusión recíproca es evidente. □

1.17. Finalmente, es fácil describir $\mathsf{Aut}(\mathsf{M}(X))$.

Proposición. *Hay un isomorfismo $\mathsf{Aut}(\mathsf{M}(X)) \cong \mathsf{S}(X)$.*

Demostración. Sea $f \in \mathsf{Aut}(\mathsf{M}(X))$. Sea $x \in X$ y supongamos que $f(x) = uv$. Entonces $f^{-1}(u)f^{-1}(v) = x$, así que o bien $f^{-1}(u) = 1$ o bien $f^{-1}(v) = 1$. Esto implica que o $u = 1$ o $v = 1$, ya que f es inyectiva. Vemos así que $f(x) \in X$. Podemos definir entonces $\phi(f) = f|_X : X \to X$.

Es claro que $\phi(f^{-1}) \circ \phi(f) = \phi(f) \circ \phi(f^{-1}) = \mathsf{id}_X$, así que $\phi(f) \in \mathsf{S}(X)$. Vemos así que tenemos una aplicación $\phi : \mathsf{Aut}(\mathsf{M}(X)) \to \mathsf{S}(X)$ y es claro que se trata de un morfismo de grupos.

Definimos ahora una aplicación $\psi : \mathsf{S}(X) \to \mathsf{Aut}(\mathsf{M}(X))$ de la siguiente manera. Sea $\pi \in \mathsf{S}(X)$. Entonces $\psi(\pi) : \mathsf{M}(X) \to \mathsf{M}(X)$ es la aplicación tal que

$$\psi(\pi)(x_1 \cdots x_n) = \pi(x_1) \cdots \pi(x_n).$$

Es claro que $\phi(\pi)$ es un automorfismos de $\mathsf{M}(X)$.

Para terminar, alcanza con mostrar que ϕ y ψ son aplicaciones inversas. Dejamos los detalles al lector. □

2. Grupos libres

2.1. Sea otra vez X un conjunto y considemos el conjunto de símbolos

$$X^{\pm} = \{x^{+1} : x \in X\} \cup \{x^{-1} : x \in X\}.$$

Sea, como antes, $\mathsf{M}(X^{\pm})$ el conjunto de palabras sobre $X^{\pm}$.

2.2. Definimos una relación $\prec$ sobre $\mathsf{M}(X^{\pm})$ de la siguiente manera: si $u, v \in \mathsf{M}(X^{\pm})$, ponemos $u \prec v$ sii existen $\alpha, \beta \in \mathsf{M}(X^{\pm})$, $x \in X$ y $\varepsilon \in \{\pm 1\}$ tales que

$$u = \alpha\beta \qquad \text{y} \qquad v = \alpha x^{\varepsilon} x^{-\varepsilon} \beta.$$

Si $u \prec v$, también escribimos $v \succ u$.

2.3. Si $u, v \in \mathsf{M}(X^{\pm})$, escribimos $u \preceq v$ si $u = v$ o $u \prec v$ y, por supuesto, tambien escribimos $v \succeq u$.

2.4. Es claro que si $u, u', v \in \mathsf{M}(X^{\pm})$ y $u \preceq u'$, entonces $uv \preceq u'v$ y $vu \preceq vu'$.

2.5. Definimos ahora una segunda relación $\sim$ sobre $\mathsf{M}(X^{\pm})$, poniendo $u \sim v$ sii hay elementos $c_0, \ldots, c_{2k+1} \in \mathsf{M}(X^{\pm})$ tales que

$$u \preceq c_0 \succeq c_1 \preceq c_2 \succeq \cdots \preceq c_{2k-1} \succeq c_{2k} \preceq c_{2k+1} \succeq v.$$

Dejamos al lector la tarea de mostrar que $\sim$ es una relación de equivalencia.

2.6. Un razonamiento inductivo a partir de **2.4** muestra que si $u, u', v \in \mathsf{M}(X^{\pm})$ son tales que $u \sim u'$, entonces $uv \sim u'v$ y $vu \sim vu'$.

2.7. Si $u \in \mathsf{M}(X)$, escribimos $[u]$ a la clase de equivalencia de u con respecto a $\sim$ en $\mathsf{M}(X)$.

2.8. Proposición. *Sea $\mathsf{L}(X) = \mathsf{M}(X^{\pm})/\!\sim$. Entonces es posible definir una aplicación $\cdot : \mathsf{L}(X) \times \mathsf{L}(X) \to \mathsf{L}(X)$ tal que*

$$[u] \cdot [v] = [uv]$$

para cada par de clases $[u], [v] \in \mathsf{L}(X)$. Más aún, $(\mathsf{L}(X), \cdot)$ es un grupo con $[1]$ como elemento neutro.

Demostración. El producto del enunciado está bien definido en vista de **2.6**. Que es asociativo y admite a $[1]$ como elemento neutro sigue inmediatamente de las afirmaciones correspondientes referidas a $\mathsf{M}(X^{\pm})$. Finalmente, si $[u] \in \mathsf{L}(X)$ con $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, es fácil ver que $[x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}]$ es un inverso para $[u]$. □

2.9. Proposición. *Sea X un conjunto, G un grupo y sea $f : X \to G$ una función arbitraria. Entonces existe exactamente un homomorfismo de grupos $\bar{f} : \mathsf{L}(X) \to G$ tal que $\bar{f}(x) = f(x)$ para todo $x \in X$.* □

2.10. Es fácil ver que, con las notaciones de la proposición, $\mathsf{im}\, \bar{f} = \langle \mathsf{im}\, f \rangle$.

2.11. Llamamos a $\mathsf{L}(X)$ el *grupo libre en X*. Un grupo isomorfo al grupo libre en algún conjunto se dice *libre*.

2.12. Si $X = \emptyset$, es claro que $\mathsf{L}(X) = 1$ es el grupo trivial. Esto se ve inmediatamente a partir de **1.11**.

2.13. Si $X = \{x\}$, entonces $\mathsf{L}(X) \cong \mathbb{Z}$. Para verlo, consideremos la aplicación $\bar{l} : \mathsf{M}(X^{\pm}) \to \mathbb{Z}$ dada por $\bar{l}(1) = 0$ y

$$\bar{l}(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = \sum_{i=1}^{n} \varepsilon_i.$$

Es inmediato verificar que $\bar{l}$ es un morfismo de monoides.

Si $u, v \in \mathsf{M}(X^{\pm})$ son tales que $u \preceq v$, entonces es claro que $\bar{l}(u) = \bar{l}(v)$. Una inducción permite mostrar, más generalmente, que si $u, v \in \mathsf{M}(X^{\pm})$ son tales que $u \sim v$, entonces $\bar{l}(u) = \bar{l}(v)$. Esto nos dice que podemos definir una aplicación $l : \mathsf{L}(X) \to \mathbb{Z}$ tal que $l([u]) = \bar{l}(u)$. Se trata evidentemente de un morfismo de grupos. Si $n \in \mathbb{N}$,

$$l([\underbrace{x^{+1} \cdots x^{+1}}_{n \text{ factores}}]) = n$$

y

$$l([\underbrace{x^{-1} \cdots x^{-1}}_{n \text{ factores}}]) = -n,$$

así que el morfismo l es sobreyectivo. Para terminar, basta mostrar que l es inyectivo.

Supongamos que $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ es una palabra no vacía tal que $l([u]) = 0$. Queremos mostrar que $u \sim 1$.

Hagamos inducción sobre n. Es $\sum_{i=1}^{n} \varepsilon_i = 0$, así que existe $j \in \{1, \ldots, n-1\}$ tal que $\varepsilon_j = -\varepsilon_{j+1}$. Sea $u' = x_1^{\varepsilon_1} \cdots x_{j-1}^{\varepsilon_{j-1}} x_{j+2}^{\varepsilon_{j+2}} \cdots x_n^{\varepsilon_n}$ Entonces $l([u']) = 0$; nuestra hipótesis inductiva nos dice entonces que $u' \sim 1$. Como claramente $u \sim u'$, vemos que $u \sim 1$, como queríamos.

2.14. Si $X \neq \emptyset$, entonces todo elemento de la forma $[x]$ con $x \in X$ tiene orden infinito en $\mathsf{L}(X)$. En particular, $\mathsf{L}(X)$ es infinito.

Para verlo, consideremos la aplicación $f : X \to \mathbb{Z}$ tal que $f(y) = 1$ para todo $y \in X$ y sea $\bar{f} : \mathsf{L}(X) \to \mathbb{Z}$ la extensión a $\mathsf{L}(X)$. Entonces $\bar{f}$ es un morfismo de grupos y $\bar{f}([x]) = 1$. Si $[x]^n = [1]$ en $\mathsf{L}(X)$, entonces $0 = \bar{f}([x]^n) = nf([x]) = n$ en $\mathbb{Z}$. Vemos así que $[x]$ tiene orden infinito.

3. Palabras reducidas

3.1. La siguiente proposición es una recíproca de la afirmación de **2.4**:

Proposición. *Sean $u, u', v \in \mathsf{M}(X^{\pm})$. Si $uv \preceq u'v$ ó $vu \preceq vu'$, entonces $u \preceq u'$.*

Demostración. Supongamos que $uv \preceq u'v$; el otro caso se trata de exactamente la misma manera. Además, hagamos inducción sobre $|v|$. Notemos que cuando $|v| = 0$ no hay nada que probar, así que supongamos que $|v| > 0$.

Si $uv = u'v$, entonces claramente $u = u'$ y por supuesto es $u \preceq u'$. Supongamos entonces que $uv \prec u'v$.

En ese caso, existen $\alpha, \beta \in \mathsf{M}(X^{\pm})$, $x \in X$ y $\varepsilon \in \{\pm 1\}$ tales que $uv = \alpha\beta$ y $u'v = \alpha x^{\varepsilon} x^{-\varepsilon}\beta$.

Claramente es $0 \leq |\alpha| \leq |uv|$. Distinguimos tres casos:

- Si $|\alpha| \leq |u|$, existe $\lambda \in \mathsf{M}(X^{\pm})$ tal que $u = \alpha\lambda$. Entonces $\alpha\beta = uv = \alpha\lambda v$, de manera que $\beta = \lambda v$. Usando esto, vemos que $u'v = \alpha x^{\varepsilon} x^{-\varepsilon}\beta = \alpha x^{\varepsilon} x^{-\varepsilon}\lambda v$, así que $u' = \alpha x^{\varepsilon} x^{-\varepsilon}\lambda$. Concluimos que en este caso $u \prec u'$.
- Si $|u| < |\alpha| < |uv|$, entonces $\beta \neq 1$ y existe $\lambda \in \mathsf{M}(X^{\pm})$ tal que $\alpha = u\lambda$. Esto nos dice que $uv = \alpha\beta = u\lambda\beta$, así que $v = \lambda\beta$. Usando esta igualdad, $\alpha x^{\varepsilon} x^{-\varepsilon}\beta = u'v = u'\lambda\beta$ y entonces $u'\lambda = \alpha x^{\varepsilon} x^{-\varepsilon}$. En definitiva, $u\lambda \prec u'\lambda$. Es $|\lambda| = |\alpha| - |u| = |v| - |\beta| < |v|$, así que la hipótesis inductiva nos permite concluir que $u \prec u'$.
- Supongamos finalmente que $|\alpha| = |uv|$. Debe ser $u'v = \alpha x^{\varepsilon} x^{-\varepsilon}$ y $uv = \alpha$.

  Existen $k \in \mathbb{N}_0$ y $w \in \mathsf{M}(X^{\pm})$ tales que $v = w(x^{\varepsilon} x^{-\varepsilon})^k$ y w no tiene a $x^{\varepsilon} x^{-\varepsilon}$ como sufijo. Tenemos que

  $$uw(x^{\varepsilon} x^{-\varepsilon})^{k+1} = uvx^{\varepsilon} x^{-\varepsilon} = \alpha x^{\varepsilon} x^{-\varepsilon} = u'v = u'w(x^{\varepsilon} x^{-\varepsilon})^k,$$

  así que

  $$uwx^{\varepsilon} x^{-\varepsilon} = u'w. \tag{1}$$

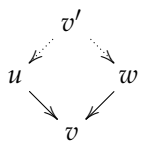
  Como w no tiene a $x^{\varepsilon} x^{-\varepsilon}$ como sufijo, esto nos dice que $|w| < 2$ y, más precisamente, que o bien $w = 1$ o bien $w = x^{-\varepsilon}$.

  Si $w = x^{-\varepsilon}$, entonces (1) nos dice que $ux^{-\varepsilon} x^{\varepsilon} x^{-\varepsilon} = u'x^{-\varepsilon}$ y deducimos que $ux^{-\varepsilon} x^{\varepsilon} = u'$ y, en consecuencia, que $u \prec u'$.

  Si, por el contrario, $w = 1$, $v = (x^{\varepsilon} x^{-\varepsilon})^k$. Como $|v| > 0$, es $k > 0$. Usando esto y la igualdad $u'(x^{\varepsilon} x^{-\varepsilon})^k = u'v = \alpha x^{\varepsilon} x^{-\varepsilon}$, vemos que $u'(x^{\varepsilon} x^{-\varepsilon})^{k-1} = \alpha = uv = u(x^{\varepsilon} x^{-\varepsilon})^k$. Así, es $u' = ux^{\varepsilon} x^{-\varepsilon}$ y, otra vez, vemos que $u \prec u'$.

En cualquiera de los tres casos, obtenemos la afirmación del enunciado, así que hemos probado la proposición. □

3.2. Proposición. *Sean u, v, $w \in \mathsf{M}(X^{\pm})$ y supongamos que $u \succeq v \preceq w$. Entonces existe $v' \in \mathsf{M}(X^{\pm})$ tal que $v' \succeq u$ y $v' \succeq w$.*



Demostración. Si $v = u$, podemos tomar $v' = w$; análogamente, si $v = w$, podemos tomar $v' = u$. Supongamos entonces que $u \neq v \neq w$.

En ese caso, existen $\alpha, \beta, \gamma, \delta \in \mathsf{M}(X^{\pm})$, $x, y \in X$, $\varepsilon, \eta \in \{\pm 1\}$ tales que

$$u = \alpha x^{\varepsilon} x^{-\varepsilon} \beta \qquad v = \alpha\beta$$
$$w = \gamma y^{\eta} y^{-\eta} \delta \qquad v = \gamma\delta$$

Supongamos que es $|\alpha| \geq |\gamma|$. Como $\alpha\beta = \gamma\delta$, existe $\lambda \in \mathsf{M}(X^{\pm})$ tal que $\alpha = \gamma\lambda$. Entonces $\gamma\delta = \alpha\beta = \gamma\lambda\beta$ y vemos que $\delta = \lambda\beta$. Pongamos $v' = \gamma y^{\eta} y^{-\eta} \lambda x^{\varepsilon} x^{-\varepsilon} \beta$. Vale ahora que $v' \succ \gamma\lambda x^{\varepsilon} x^{-\varepsilon}\beta = \alpha x^{\varepsilon} x^{-\varepsilon}\beta = u$ y $v' \succ \gamma y^{\eta} y^{-\eta} \lambda\beta = \gamma y^{\eta} y^{-\eta}\delta = w$, que es precisamente lo que queríamos.

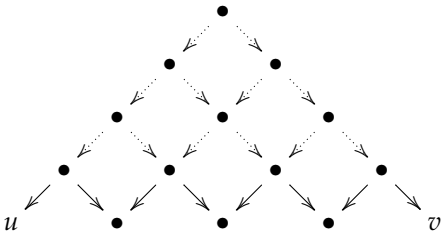
El caso en el que $|\alpha| < |\gamma|$ puede tratarse de manera similar. □

3.3. Corolario. *Si $u, v \in \mathsf{M}(X^{\pm})$ son tales que $u \sim v$, entonces existen $k, l \in \mathbb{N}$ y $w, c_1, \ldots, c_k, d_1, \ldots, d_l \in \mathsf{M}(X^{\pm})$ tales que*

$$u \prec c_1 \prec c_2 \prec \cdots \prec c_{k-1} \prec c_k \prec w$$

y

$$v \prec d_1 \prec d_2 \prec \cdots \prec d_{l-1} \prec d_l \prec w$$



Demostración. Esto sigue de **3.2**. Dejamos los detalles al lector. □

3.4. Una palabra $u \in \mathsf{M}(X^{\pm})$ es *reducible* si existen $\alpha, \beta \in \mathsf{M}(X^{\pm})$, $x \in X$ y $\varepsilon \in \{\pm 1\}$ tales que $u = \alpha x^{\varepsilon} x^{-\varepsilon} \beta$. Una palabra es *reducida* si no es reducible.

3.5. Si $u, v \in \mathsf{M}(X^{\pm})$ son tales que existen $\alpha, \beta \in \mathsf{M}(X^{\pm})$, $x \in X$ y $\varepsilon \in \{\pm 1\}$ tales que $u = \alpha\beta$, $u = \alpha x^{\varepsilon} x^{-\varepsilon}\beta$ y además αx^{ε} es reducida, escribimos $u \prec_l v$.

3.6. Es evidente que si u, $v \in \mathsf{M}(X^{\pm})$ son tales que $u \prec_l v$, entonces $u \prec v$.

3.7. Por otro lado, si $v \in \mathsf{M}(X^{\pm})$ es reducible, existe $u \in \mathsf{M}(X^{\pm})$ tal que $u \prec_l v$.

3.8. Proposición. *Sean $u, u', v \in \mathsf{M}(X^{\pm})$. Si $u \prec_l v$ y $u' \prec_l v$, entonces $u = u'$.*

Más generalmente, si $u, u', w, c_1, \ldots, c_k, d_1, \ldots, d_r \in \mathsf{M}(X^{\pm})$ son tales que

$$u \prec_l c_1 \prec_l c_2 \prec_l \cdots \prec_l c_{k-1} \prec_l c_k \prec_l w$$

y

$$u' \prec_l d_1 \prec_l d_2 \prec_l \cdots \prec_l d_{r-1} \prec_l d_r \prec_l w,$$

y o bien $l = r$ o bien u y u' son reducidas, entonces $u = u'$.

Demostración. Por hipótesis, existen α, β, γ, $\delta \in \mathsf{M}(X^{\pm})$, $x, y \in X$, $\varepsilon, \eta \in \{\pm 1\}$ tales que $u = \alpha\beta$, $u' = \gamma\delta$,

$$v = \alpha x^{\varepsilon} x^{-\varepsilon} \beta = \gamma y^{\eta} y^{-\eta} \delta \tag{2}$$

y αx^{ε} y γy^{η} son reducidas.

Supongamos que $|\alpha| < |\gamma|$. De (2) vemos que $\alpha x^{\varepsilon} x^{-\varepsilon}$ es un prefijo de γy^{η}. Pero esto es imposible porque γy^{η} es reducida.

De la misma forma vemos que no puede ser $|\alpha| < |\gamma|$ y concluimos que $|\alpha| = |\gamma|$. Usando otra vez (2), esto implica que de hecho $\alpha = \gamma$ y $\beta = \delta$. Luego $u = u'$, como queríamos mostrar.

La última afirmación sigue de la primera mediante un razonamiento inductivo que dejamos al lector. □

3.9. Proposición. *Sean $u, v \in \mathsf{M}(X^{\pm})$. Supongamos que u es reducida y que existen $c_1, \ldots, c_k \in \mathsf{M}(X^{\pm})$ tales que*

$$u \prec c_1 \prec c_2 \prec \cdots \prec c_{k-1} \prec c_k \prec v.$$

Entonces existen $c'_1, \ldots, c'_k \in \mathsf{M}(X^{\pm})$ tales que

$$u \prec_l c'_1 \prec_l c'_2 \prec_l \cdots \prec_l c'_{k-1} \prec_l c'_k \prec_l v.$$

Demostración. Hagamos inducción sobre k. Si $c_k \not\prec_l v$, entonces el resultado sigue inmediatamente de la hipótesis inductiva. Supongamos entonces que $c_k \not\prec_l v$. Entonces basta mostrar que existe una cadena de la forma

$$u \prec c'_1 \prec c'_2 \prec \cdots \prec c'_{k-1} \prec c'_k \prec_l v,$$

en la que la *primera* reducción es de tipo $\prec_l$.

Sea $c'_k \in \mathsf{M}(X^{\pm})$ tal que $c'_k \prec_l v$. Sean $\alpha, \beta \in \mathsf{M}(X^{\pm})$, $x \in X$ y $\varepsilon \in \{\pm 1\}$ tales que $v = \alpha x^{\varepsilon} x^{-\varepsilon} \beta$, $c'_k = \alpha\beta$ y αx^{ε} es reducida.

Como $c_k \prec v$, existen $\gamma, \delta \in \mathsf{M}(X^{\pm})$, $y \in X$ y $\eta \in \{\pm 1\}$ tales que $v = \gamma y^{\eta} y^{-\eta} \delta$ y $c_k = \gamma\delta$. Observemos que

$$\gamma y^{\eta} y^{-\eta} \delta = v = \alpha x^{\varepsilon} x^{-\varepsilon} \beta, \tag{3}$$

Consideremos las posibles relaciones entre $|\gamma|$ y $|\alpha|$:

- Si $|\gamma| < |\alpha|$, entonces de (3) vemos que $\gamma y^{\eta} y^{-\eta}$ es un prefijo de αx^{ε}, lo que contradice la irreducibilidad de αx^{ε}.
- Sabemos que no es $|\gamma| = |\alpha|$ porque $c_k \not\prec_l v$.
- Si $|\gamma| = |\alpha| + 1$, entonces (3) implica que $\gamma = \alpha x^{\varepsilon}$, $y = x$, $\eta = -\varepsilon$ y $y^{-\eta}\delta = \beta$. Usando estas igualdades, vemos que $c_k = \gamma\delta = \alpha x^{\varepsilon}\delta = \alpha y^{-\eta}\delta = \alpha\beta = c'_k$ y, en particular, $c_k \prec_l v$, otra vez contradiciendo nuestra hipótesis.

Concluimos que debe ser $|\gamma| \geq |\alpha| + 2$ y, en particular, que $\alpha x^{\varepsilon} x^{-\varepsilon}$ es un prefijo de c_k. Esto nos permite definir

$$t = \min \left\{ i : \alpha x^{\varepsilon} x^{-\varepsilon} \text{ es prefijo de } c_j \text{ si } j \in \{i, \ldots, k\} \right\}.$$

ya que el conjunto al que tomamos el mínimo no es vacío.

La elección de t implica que para cada $i \in \{t, \dots, k\}$ existe $d_i \in \mathsf{M}(X^{\pm})$ tal que $c_i = \alpha x^{\varepsilon} x^{-\varepsilon} d_i$.

Ahora bien, como $c_t \succ c_{t-1}$, existen $\mu, \nu \in \mathsf{M}(X^{\pm})$, $z \in X$ y $\sigma \in \{\pm 1\}$ tales que $c_t = \mu z^{\sigma} z^{-\sigma} \nu$ y $c_{t-1} = \mu\nu$. Tenemos que

$$\alpha x^{\varepsilon} x^{-\varepsilon} d_t = c_t = \mu z^{\sigma} z^{-\sigma} \nu, \tag{4}$$

Analizamos ahora la relación entre $|\alpha|$ y $|\mu|$:

- Si $|\alpha| > |\mu|$, entonces $\mu z^{\sigma} z^{-\sigma}$ es un prefijo de αx^{ε}, lo que es imposible.
- Si $|\alpha| + 1 < |\mu|$, entonces $\alpha x^{\varepsilon} x^{-\varepsilon}$ es un prefijo de μ y, por lo tanto, también de c_{t-1}, lo que otra vez es imposible.
- Si $|\alpha| = |\mu|$, la igualdad (4) implica que $\alpha = \mu$ y $d_r = \nu$. Luego $c_{t-1} = \mu\nu = \alpha d_t$.
- Si $|\alpha| + 1 = |\mu|$, la misma ecuación nos dice que $\mu = \alpha x^{\varepsilon}$, $x = z$, $\sigma = -\varepsilon$ y $d_t = z^{-\sigma\nu}$. Estas igualdades implican que $c_{t-1} = \mu\nu = \alpha x^{\varepsilon}\nu = \alpha z^{-\sigma}\nu = \alpha d_t$.

En cualquier caso, vemos que tenemos $c_{t-1} = \alpha d_t$.

Sabemos que

$$\begin{array}{ccccccccc} c_t & \prec & c_{t+1} & \prec & \cdots & \prec & c_k & \prec & v \\ \| & & \| & & & & \| & & \| \\ \alpha x^{\varepsilon} x^{-\varepsilon} d_t & & \alpha x^{\varepsilon} x^{-\varepsilon} d_{t-1} & & & & \alpha x^{\varepsilon} x^{-\varepsilon} d_k & & \alpha x^{\varepsilon} x^{-\varepsilon} \beta \end{array}$$

así que la proposición **3.1** nos permite concluir que $d_t \prec d_{t-1} \prec \cdots \prec d_k \prec \beta$. Usando ahora **2.4**, vemos que $\alpha d_t \prec \alpha d_{t-1} \prec \cdots \prec \alpha d_k \prec \alpha\beta$.

Con todo lo hecho, obtenemos una cadena

$$u \prec c_1 \prec \cdots \prec c_{t-1} = \alpha d_t \prec \alpha d_{t-1} \prec \cdots \prec \alpha d_k \prec \alpha\beta \prec_l \alpha x^{\varepsilon} x^{-\varepsilon} \beta = v$$

que tiene longitud l. Esto prueba la proposición. □

3.10. Proposición. *Sea $u \in \mathsf{M}(X^{\pm})$. Entonces existe exáctamente una palabra reducida $\bar{u} \in \mathsf{M}(X^{\pm})$ tal que $u \sim \bar{u}$.*

Demostración. Bastará mostrar que si u y u' son palabras reducidas de $\mathsf{M}(X^{\pm})$ tales que $u \sim u'$, entonces $u = u'$.

Sean entonces u, u' palabras reducidas tales que $u \sim u'$. La proposición **3.3** nos dice que existen $k, r \in \mathbb{N}$ y $w, c_1, \dots, c_k, d_1, \dots, d_r \in \mathsf{M}(X^{\pm})$ tales que

$$u \prec c_1 \prec c_2 \prec \cdots \prec c_{k-1} \prec c_k \prec w$$

y

$$u' \prec d_1 \prec d_2 \prec \cdots \prec d_{r-1} \prec d_r \prec w$$

Usando **3.9**, vemos entonces que existen $c'_1, \dots, c'_k, d'_1, \dots, d'_r \in \mathsf{M}(X^{\pm})$ tales que

$$u \prec_l c'_1 \prec_l c'_2 \prec_l \cdots \prec_l c'_{k-1} \prec_l c'_k \prec_l w$$

y

$$u' \prec_l d'_1 \prec_l d'_2 \prec_l \cdots \prec_l d'_{r-1} \prec_l d'_r \prec_l w$$

Podemos ahora concluir que $u = u'$ usando **3.8**. □

3.11. Si $u \in \mathsf{M}(X^{\pm})$, escribimos $\mathsf{red}(u)$ a la palabra reducida equivalente a u.

3.12. Notemos que si $u \in \mathsf{M}(X^{\pm})$, es fácil contruir la palabra reducida $\mathsf{red}(u)$ eqivalente a u: basta simplemente hacer reducciones mientras esto sea posible. Este proceso debe arribar a una palabra reducida en un número finito de pasos, porque cada reducción disminuye la longitud. Por otro lado, que la palabra reducida obtenida depende solamente de u es precisamente el contenido de **3.10**.

3.13. Los resultados de esta sección permiten dar un algoritmo para comparar elementos del grupo libre $\mathsf{L}(X)$:

Proposición. *Sean $u, v \in \mathsf{M}(X^{\pm})$. Entonces $[u] = [v]$ en $\mathsf{L}(X)$ sii $\mathsf{red}(u) = \mathsf{red}(v)$.* □

3.14. Si $u, v \in \mathsf{M}(X^{\pm})$ son reducidas, entonces

$$|\mathsf{red}(uv)| \geq \mathsf{mín}\{|u| - |v|, |v| - |u|\}.$$

Esto puede verse por inducción sobre $|uv|$. En efecto, si uv es reducida, el resultado es claro; si no, existen $u', v' \in \mathsf{M}(X^{\pm})$, $x \in X$ y $\varepsilon \in \{\pm 1\}$ tales que $u = u'x^{\varepsilon}$ y $v = x^{-\varepsilon}v'$. Entonces $\mathsf{red}(uv) = \mathsf{red}(u'v')$ y la hipótesis inductiva implica que

$$\begin{aligned} |\mathsf{red}(uv)| &= |\mathsf{red}(u'v')| \geq \mathsf{mín}\{|u'| - |v'|, |v'| - |u'|\} \\ &= \mathsf{mín}\{|u| - |v|, |v| - |u|\}. \end{aligned}$$

3.15. Una palabra $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \mathsf{M}(X^{\pm})$ es *cíclicamente reducida* si es reducida y si o bien $x_1 \neq x_n$ o bien $\varepsilon_1 = \varepsilon_n$.

3.16. Es evidente que si $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \mathsf{M}(X^{\pm})$ es cíclicamente reducida, entonces $x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} x_1^{\varepsilon_1}$ también lo es. Notemos que $[x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}]$ y $[x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} x_1^{\varepsilon_1}]$ son conjugados en $\mathsf{L}(X)$:

$$[x_1^{\varepsilon_1}] \cdot [x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} x_1^{\varepsilon_1}] \cdot [x_1^{\varepsilon_1}]^{-1} = [x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}].$$

3.17. Si $u \in \mathsf{M}(X^{\pm})$ es cíclicamente reducida, entonces cualquiera sea $k \in \mathbb{N}$, la palabra u^k también lo es.

3.18. Si $[u] \in \mathsf{L}(X)$, existe $v \in \mathsf{M}(X^{\pm})$ cíclicamente reducida tal que $[u]$ y $[v]$ son conjugados en $\mathsf{L}(X)$.

En efecto, supongamos que $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ es reducida pero no cíclicamente reducida y razonemos inductivamente sobre n. Entonces $x_1 = x_n$ y $\varepsilon_1 = -\varepsilon_n$. Sea $u' = x_2^{\varepsilon_2} \cdots x_{n-1}^{\varepsilon_{n-1}}$. Entonces $u = x_1^{\varepsilon_1} u' x_1^{-\varepsilon_1}$ así que $[u]$ y $[u']$ son conjugados es $\mathsf{L}(X)$. Obtenemos el resultado deseado observando que la hipótesis inductiva implica que existe $v \in \mathsf{M}(X^{\pm})$ cíclicamente reducida tal que $[u']$ y $[v]$ son conjugados en $\mathsf{L}(X)$.

3.19. La razón por la que generalmente estamos interesados en la propiedad de reducción cíclica es la siguiente proposición:

Proposición. *Una palabra reducida u es cíclicamente reducida sii, siempre que $v \in \mathsf{M}(X^{\pm})$ es tal que $[u]$ y $[v]$ son conjugados en $\mathsf{L}(X)$, es $|v| \geq |u|$.*

Demostración. Sea $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \mathsf{M}(X^{\pm})$ cíclicamente reducida. Para probar la proposición, basta mostrar que si $w = y_1^{\eta_1} \cdots y_m^{\eta_m} \in \mathsf{M}(X^{\pm})$ es reducida, entonces $|\mathsf{red}(wuw^{-1})| \geq |u|$.

Si $v = wuw^{-1}$ es reducida, esto es evidente. Supongamos entonces que v no es reducida. En ese caso o *(i)* $y_m = x_1$ y $\eta_m = -\varepsilon_1$ o *(ii)* $y_m = x_n$ y $\eta_m = \varepsilon_n$. Como u es cíclicamente reducida, *(i)* y *(ii)* no pueden ocurrir simultáneamente. Esto nos dice que de wu y uw^{-1}, una de las dos es reducida y, como w y w^{-1} son reducidas, concluimos que $|\mathsf{red}(wuw^{-1})| \geq |u|$, como queríamos. □

3.20. Proposición. *Si* $|X| > 1$, *entonces* $\mathsf{Z}(\mathsf{L}(X)) = 1$.

Demostración. Supongamos que $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ es una palabra reducida de longitud positiva tal que $[u] \in \mathsf{Z}(\mathsf{L}(X))$.

Como $|X| > 1$, existe $y \in X \setminus \{x_1\}$. Luego la palabra yu es reducida. Como $[yu] = [uy]$ y $|yu| = |uy|$, uy debe ser reducida también. Vemos así que

$$yx_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y$$

De esta igualdad deducimos que debe ser $y = x_1$, lo que es absurdo. □

3.21. Proposición. *Sea* $u \in \mathsf{M}(X^{\pm})$ *una palabra reducida no vacía y sea* $k \in \mathbb{N}$. *Entonces* $\mathsf{red}(u^k)$ *y* u *tienen un prefijo común no trivial y un sufijo común no trival.*

Demostración. Existen $v, w \in \mathsf{M}(X^{\pm})$ tales que $u = vwv^{-1}$ con v de longitud máxima con respecto a esta propiedad. Es claro que entonces w es cíclicamente reducida. Además, $w \neq 1$ porque sino u no sería reducida. Notemos que $u^k = (vwv^{-1})^k \sim vw^kv^{-1}$.

Como w es cíclicamente reducida, w^k es reducida. Como vwv^{-1} es reducida, entonces, vw^kv^{-1} es reducida. Luego, de hecho, $\mathsf{red}(u^k) = vw^kv^{-1}$ y vw es un prefijo común entre u y $\mathsf{red}(u^k)$. □

3.22. Mostramos en **2.14** que si $x \in X$, $[x]$ tiene orden infinito en $\mathsf{L}(X)$. Podemos hacerlo más directamente ahora. En efecto, cualquiera sea $n \in \mathbb{N}$, la palabra x^n es reducida, así que $[x]^n \neq [1]$. Más generalmente, tenemos la siguiente proposición:

Proposición. *Todo elemento de* $\mathsf{L}(X) \setminus 1$ *tiene orden infinito.*

Demostración. Sea $u \in \mathsf{M}(X^{\pm})$ tal que $[u] \neq [1]$. Para ver que $[u]$ tiene orden infinito en $\mathsf{L}(X)$, basta mostrar que algún conjugado de $[u]$ tiene orden infinito. Podemos suponer entonces que u es cíclicamente reducida. Pero esto implica que u^k es reducida para cada $k \in \mathbb{N}$, así que por supuesto $[u^k] \neq [1]$. □

3.23. Decimos que un elemento $u \in \mathsf{L}(X)$ es *primitivo* si siempre que $v \in \mathsf{L}(X)$ y $k \in \mathbb{N}$ son tales que $u = v^k$, es $k = 1$.

Proposición. *Sea* $u \in \mathsf{M}(X^{\pm})$. *Entonces* $[u]$ *es primitivo en* $\mathsf{L}(X)$ *sii la palabra reducida* $\mathsf{red}(u)$ *correspondiente es primitiva en* $\mathsf{M}(X^{\pm})$.

Demostración. Sea $u \in \mathsf{M}(X^{\pm})$ reducida y supongamos que existen $v \in \mathsf{M}(X^{\pm})$ y $k \in \mathbb{N}$ tales que $u = v^k$ y $k \geq 2$. Entonces por supuesto $[u] = [v]^k$ así que $[u]$ no es primitivo. Esto muestra que la condición es necesaria.

Para ver la suficiencia, supongamos que $u \in \mathsf{M}(X^{\pm})$ es tal que $[u]$ no es primitivo. Sin pérdida de generalidad, podemos suponer que u es cíclicamente reducida; en efecto, conjugando a por un elemento apropiado podemos reducirnos a este caso. Por hipótesis, existe una palabra reducida $v \in \mathsf{M}(X^{\pm})$ y

$k \in \mathbb{N}$ tales que $k \geq 2$ y $u \sim v^k$. Entonces $\mathsf{red}(v^k) = u$ y usando **3.21** vemos que u y v comparten un prefijo no trivial y un sufijo no trivial. Esto implica que v es cíclicamente reducida y, en particular, que v^k es reducida. Luego $u = v^k$ y u no es primitiva en $\mathsf{M}(X)$. □

3.24. La siguiente proposición es el análogo para $\mathsf{L}(X)$ de **1.15**. La demostración es esencialmente la misma, salvo que complicada por el hecho de que pasamos al cociente.

Proposición. *Sea $w \in \mathsf{L}(X)$. Entonces existe $w_0 \in \mathsf{L}(X)$ y $k \in \mathbb{N}$ tal que w_0 es primitivo en $\mathsf{L}(X)$ y $w = w_0^k$. Tanto, w_0 y k están unívocamente determinados por w. Además, si $v \in \mathsf{L}(X)$ y $l \in \mathbb{N}$ son tales que $w = v^l$, entonces $l \mid k$ y $v = w_0^{k/l}$.*

Demostración. Sea $u \in \mathsf{M}(X^{\pm})$ reducida tal que $w = [u]$. Sin pérdida de generalidad, podemos suponer de hecho que u es cíclicamente reducida.

Usando **1.15** vemos que existe $u_0 \in \mathsf{M}(X^{\pm})$ y $k \in \mathbb{N}$ tal que u_0 es primitiva en $\mathsf{M}(X^{\pm})$ y $u = u_0^k$. Como u es cíclicamente reducida, u_0 es cíclicamente reducida; por otro lado, **3.23** implica que $w_0 = [u_0]$ es primitivo en $\mathsf{L}(X)$. Notemos que $w = w_0^k$.

Supongamos ahora que $v \in \mathsf{M}(X^{\pm})$ es una palabra reducida y $l \in \mathbb{N}$ son tales que $w_0^k = [v]^l$, de manera que $u_0^k \sim v^l$. Como $u_0^k = u$ es reducida, esto nos dice que $\mathsf{red}(v^l) = u_0^k$. La proposición **3.21** asegura ahora que v y u_0 comparten un prefijo no trivial y un sufijo no trivial; en particular, v es cíclicamente reducida. Pero entonces v^l es reducida y debe ser $v^l = u_0^k$. Usando **1.15** otra vez, concluimos que $l \mid k$ y que $v = u_0^{k/l}$.

Si $[v]$ es primitiva, entonces **3.23** implica que v es primitiva. Es claro que debe ser en ese caso $k = l$ y $v = u_0$. □

4. Presentaciones

4.1. Si X es un conjunto y $R \subset \mathsf{L}(X)$, escribimos $\mathsf{L}(X : R) = \mathsf{L}(X)/\langle\langle X \rangle\rangle$. Todo grupo es isomorfo a un grupo de esta forma. Más precisamente, tenemos:

Proposición. *Sea G un grupo. Sea X un conjunto y $f : X \to G$ una función tal que $G = \langle \mathsf{im}\, f \rangle$. Entonces el morfismo $\bar{f} : \mathsf{L}(X) \to G$ de* **2.9** *es sobreyectivo y, en particular, $G \cong \mathsf{L}(X)/\ker \bar{f}$.*

Si $R \subset \mathsf{L}(X)$ es tal que $\ker \bar{f} = \langle\langle R \rangle\rangle$, entonces $G \cong \mathsf{L}(X : R)$.

Demostración. Esto sigue inmediatamente de **2.10**. □

4.2. Sea G un grupo. Una *presentación* de G es una terna (X, R, ι) en la que X es un conjunto, $R \subset \mathsf{L}(X)$ es un subconjunto arbitrario y $\iota : X \to G$ es una aplicación tal que si $\bar{\iota} : \mathsf{L}(X) \to G$ es el homomorfismo que extiende a ι, entonces $\bar{\iota}$ es una sobreyección con núcleo $\ker \bar{\iota} = \langle\langle R \rangle\rangle$.

4.3. Si X es un conjunto, $R \subset \mathsf{L}(X)$ y $\iota : X \to \mathsf{L}(X : R)$ es la composición de la inclusión $X \hookrightarrow \mathsf{L}(X)$ con la proyección canónica $\mathsf{L}(X) \to \mathsf{L}(X : R)$, entonces es claro que (X, R, ι) es una presentación de $\mathsf{L}(X : R)$.

4.4. La proposición **4.1** implica que todo grupo admite alguna presentación. De hecho, todo grupo tiene en general muchas y todas se obtienen como en **4.1**.

4.5. *Ejemplo.* Sea $G = \mathbb{Z}_2$. Sea $X = \{x\}$ y sea $f : X \to \mathbb{Z}_2$ tal que $f(x) = \bar{1}$. Sabemos que todo elemento de $\mathsf{L}(X)$ es de la forma x^n con $n \in \mathbb{Z}$ y, de hecho, $x^n \in \mathsf{L}(X) \mapsto n\mathbb{Z}$ es un isomorfismo. Claramente, $\bar{f} : x^n \in \mathsf{L}(X) \mapsto \bar{n} \in \mathbb{Z}_2$. En particular, $\ker \bar{f} = \{x^n : n \in 2\mathbb{Z}\}$. Luego el isomorfismo $\mathbb{Z}_2 \cong \mathsf{L}(X)/\ker \bar{f}$ es precisamente el isomorfismo $G \cong \mathbb{Z}/2\mathbb{Z}$ usual. Notemos que $\ker \bar{f} = \langle x^2 \rangle$.

4.6. *Ejemplo.* Tomemos otra vez $G = \mathbb{Z}_2$, pero ahora sea $X = \{x, y\}$ con $x \neq y$ y sea $f : X \to \mathbb{Z}_2$ tal que $f(x) = f(y) = \bar{1}$. En este caso el morfismo $\bar{f} : \mathsf{L}(X) \to \mathbb{Z}_2$ es tal que $f([u]) = \overline{|u|}$. Luego

$$\ker \bar{f} = \{[u] \in \mathsf{L}(X) : |u| \equiv 0 \mod 2\}.$$

Es fácil ver que $\ker \bar{f} = \langle x^2, y^2, xy^{-1} \rangle$.

4.7. *Ejemplo.* Sea $G = \mathbb{Z}_2$ y $X = \{x, y\}$ con $x \neq y$ como antes y sea $f : X \to \mathbb{Z}_2$ tal que $f(x) = \bar{0}$ y $f(y) = \bar{1}$. En este caso el morfismo $\bar{f} : \mathsf{L}(X) \to \mathbb{Z}_2$ es tal que si $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, entonces

$$f([u]) = \overline{\mathsf{card}\left\{i \in \{1, \ldots, n\} : x_i = y\right\}}.$$

Esta vez, entonces,

$$\ker \bar{f} = \left\{[x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}] \in \mathsf{L}(X) : \mathsf{card}\left\{i \in \{1, \ldots, n\} : x_i = y\right\} \equiv 0 \mod 2\right\}.$$

En este caso es $\ker \bar{f} = \langle x,\, y^2,\, yxy^{-1} \rangle$.

4.8. *Ejemplo.* Sea $n \geq 2$ y $\alpha = 2\pi/n$. Consideremos los siguientes dos elementos de $\mathsf{GL}_2(\mathbb{R})$:

$$\rho = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

El *n-ésimo grupo diedral* es, por definición, $D_n = \langle \rho, \sigma \rangle$.

Es claro que $\rho^n = \sigma^2 = 1$. Por otro lado, un cálculo elemental muestra que $\rho\sigma = \sigma\rho^{-1}$. Esto implica que

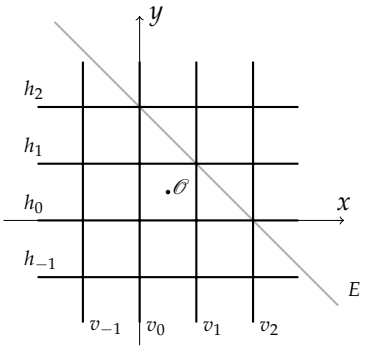
$$D_n = \{\sigma^i \rho^j : 0 \leq i < 2,\ 0 \leq j < n\}.$$

Más aún, calculando explícitamente los $2n$ elementos listados a la izquierda se puede ver que son todos distintos. Así, $|D_n| = 2n$.

Sea ahora $X = \{r, s\}$ con $r \neq s$ y sea $f : X \to D_n$ tal que $f(r) = \rho$ y $f(s) = \sigma$. Queremos describir el núcleo del morfismo $\bar{f} : \mathsf{L}(X) \to D_n$.

Un candidato es el subgrupo $H = \langle r^n, s^2, rsrs^{-1} \rangle$. Veamos, sin embargo, que $\ker \bar{f} \neq H$. De hecho, H no es normal ni tiene índice finito. Veámoslo, por ejemplo, cuando $n = 4$.

Para cada $i \in \mathbb{Z}$ consideremos las rectas $h_i = \{(x, i) \in \mathbb{R}^2 : x \in \mathbb{R}\}$ y $v_i = \{(i, y) \in \mathbb{R}^2 : y \in \mathbb{R}\}$ y pongamos $\mathscr{L} = \{h_i : i \in \mathbb{Z}\} \cup \{v_i : i \in \mathbb{Z}\}$; evidentemente, en esta enumeración de los elementos de $\mathscr{L}$ no hay repeticiones.



Sea $\mathscr{O} = (\frac{1}{2}, \frac{1}{2})$. Sea $R : \mathbb{R}^2 \to \mathbb{R}^2$ la rotación en 90° en el sentido contrario al de las agujas del reloj con centro en $\mathscr{O}$ y sea $S : \mathbb{R}^2 \to \mathbb{R}^2$ la simetría con respecto a la recta E de ecuación

$$x + y = 2.$$

Explícitamente, es

$$R : (x, y) \in \mathbb{R}^2 \mapsto (1 - y, x) \in \mathbb{R}^2$$

y

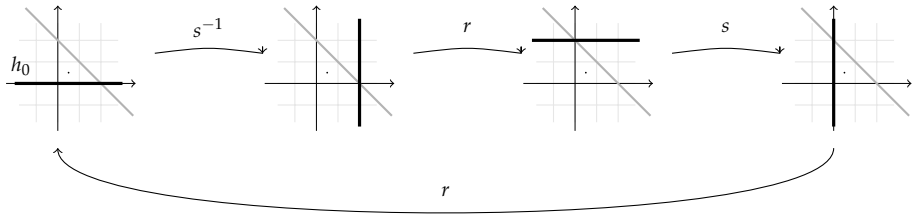
$$S : (x, y) \in \mathbb{R}^2 \mapsto (2 - y, 2 - x) \in \mathbb{R}^2.$$

Ahora bien, es claro que R y S permutan las rectas de $\mathscr{L}$; esto es, podemos considerar $R, S \in \mathsf{S}(X)$. Existe entonces un morfismo de grupos $\phi : \mathsf{L}(r, s) \to \mathsf{S}(\mathscr{L})$ tal que $\phi(r) = R$ y $\phi(s) = S$. Obtenemos así una acción de $\mathsf{L}(r, s)$ sobre $\mathscr{L}$. Calculando, podemos ver que, si $i \in \mathbb{Z}$,

$$r \cdot h_i = v_{1-i}, \qquad s \cdot h_i = v_{2-i},$$
$$r \cdot v_i = h_i, \qquad s \cdot v_i = h_{2-i}.$$

Usando estas relaciones vemos que $sr \cdot h_i = h_{i+1}$, así que, por inducción, es $h_i = (sr)^{i-1} \cdot h_0$ y $v_i = r^{-1}(sr)^{i-1} \cdot h_0$ para cada $i \in \mathbb{Z}$. Concluímos así que la acción de $\mathsf{L}(r,s)$ sobre $\mathscr{L}$ es transitiva.

Sea, como arriba, $H = \langle r^4, s^2, rsrs^{-1} \rangle$. Es evidente que $r^4 \cdot h_0 = s^2 \cdot h_0 = h_0$ y un cálculo trivial muestra que también $rsrs^{-1} \cdot h_0 = h_0$.



Así que concluímos que $H \subset \mathsf{stab}(h_0)$ y, en particular, que

$$[\mathsf{L}(r,s) : H] \geq [\mathsf{L}(r,s) : \mathsf{stab}(h_0)] = |\mathscr{L}| = \infty.$$

Como $\ker \bar{f}$ tiene índice finito en $\mathsf{L}(r,s)$ vemos que, por supuesto, $\ker \bar{f} \neq H$.

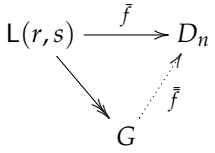
Más aún, vemos que H no es ni siquiera normal. En caso contrario tendríamos que

$$H = \bigcap_{g \in \mathsf{L}(r,s)} gHg^{-1} \subset \bigcap_{g \in \mathsf{L}(r,s)} g\, \mathsf{stab}(h_0)\, g^{-1} = \bigcap_{g \in \mathsf{L}(r,s)} \mathsf{stab}(g \cdot h_0)$$

y H debería actuar trivialmente sobre todos los elementos de $\mathscr{L}$. Pero es $rsrs^{-1} \cdot v_0 = v_{-2}$, así que esto es imposible.

Volvamos al caso en que $n \in \mathbb{N}$ es cualquiera. Afirmamos que $\ker \bar{f} = \langle\langle r^n, s^2, rsrs^{-1} \rangle\rangle$, el menor subgrupo normal de $\mathsf{L}(r,s)$ que contiene a r^n, s^2 y $rsrs^{-1}$.

En todo caso, como r^n, s^2 y $rsrs^{-1} \in \ker \bar{f}$, es claro que $\langle\langle r^n, s^2, rsrs^{-1} \rangle\rangle \subset \ker \bar{f}$. Sea $G = \mathsf{L}(r,s)/\langle\langle r^n, s^2, rsrs^{-1} \rangle\rangle$. La propiedad universal del cociente nos dice que existe un morfismo $\bar{\bar{f}} : G \to D_n$ que hace conmutar el siguiente diagrama:



Como $\bar{f}$ es sobreyectiva, la conmutatividad implica que $\bar{\bar{f}}$ es sobreyectiva. Si mostramos que G tiene a lo sumo $2n$ elementos, claramente podremos concluir que tiene de hecho exáctamente $2n$, que $\bar{\bar{f}}$ es un isomorfismo y, en particular, que

$$\ker \bar{f} = \langle\langle r^n, s^2, rsrs^{-1} \rangle\rangle,$$

como afirmamos arriba.

Llamemos $\hat{r}$ y $\hat{s}$ a las clases de r y s, respectivamente, en G. Es evidente que $G = \langle \hat{r}, \hat{s} \rangle$; más aún, $\hat{r}^n = \hat{s}^2 = 1$ y $\hat{r}\hat{s} = \hat{s}\hat{r}^{-1}$. Luego exactamente el mismo razonamiento que hicimos con D_n muestra que

$$G = \{\hat{s}^i \hat{r}^j : 0 \leq i < 2,\ 0 \leq j < n\}.$$

Esto implica que $|G| \leq 2n$, como queríamos.

En definitiva, vemos que

$$D_n \cong \mathsf{L}(r, s) / \langle\langle r^n, s^2, rsrs^{-1} \rangle\rangle.$$

5. Enumeración de coclases

Grafos de Cayley

5.1. Sea G un grupo, $X \subset G$ un subconjunto y sea E un conjunto sobre el cual G actúa a izquierda. El *grafo de Cayley de G sobre E con respecto a X* es el grafo orientado $\mathscr{C}(G, E, X)$ con arcos etiquetados por elementos de X siguiente: el conjunto de vértices de $\mathscr{C}(G, E, X)$ es E y, dados $e, e' \in E$ y $x \in X$, hay un arco $e \xrightarrow{x} e'$ en $\mathscr{C}(G, E, X)$ sii $x \cdot e = e'$.

Grafos de Cayley

5.2. Cuando $E = G$ dotado de su acción a izquierda regular, escribimos simplemente $\mathscr{C}(G, X)$ en vez de $\mathscr{C}(G, G, X)$.

5.3. *Ejemplo.* Consideremos $G = S_3$, $x = (1\,2), y = (2\,3) \in G$ y $X = \{x, y\}$. Sea $E = \{1, 2, 3\}$ sobre el que G actúa tautológicamente. El grafo $\mathscr{C}(G, E, X)$ está ilustrado en la figura 5.2.

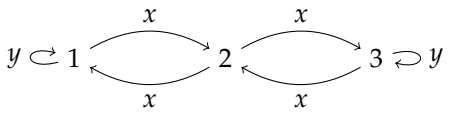


Figura 1: Ejemplo **5.3**.

5.4. *Ejemplo.* Consideremos $G = S_3$, sean $x = (1\,2), y = (1\,2\,3) \in G$ y $X = \{x, y\}$. Sea $E = \{(1\,2), (2\,3), (1\,3)\}$ el conjunto de transposiciones de G, sobre el que G actúa por conjugación. Entonces el grafo de Cayley $\mathscr{C}(G, E, X)$ es el que aparece en la figura 5.2.

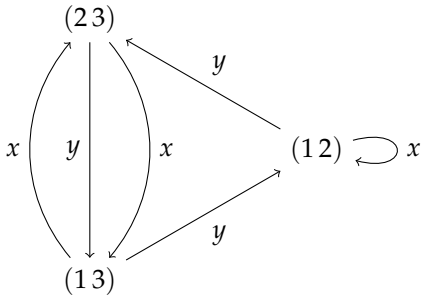


Figura 2: Ejemplo **5.4**.

5.5. *Ejemplo.* Sea $G = \mathbb{Z}_7$ y $X = \{\bar{1}, \bar{3}\}$. Entonces $\mathscr{C}(G, X)$ es el grafo de la figura 5.2.

5.6. Es claro que $\mathscr{C}(G, E, X)$ coincide con $\mathscr{C}(\langle X \rangle, E, X)$. Luego casi siempre asumiremos que X genera a G.

5.7. La siguiente proposición establece las propiedades básicas de $\mathscr{C}(G, E, X)$:

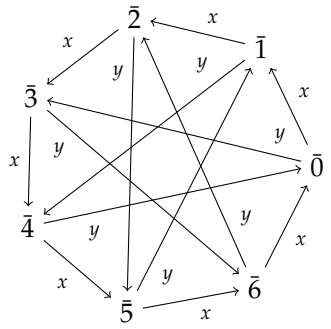


Figura 3: Ejemplo **5.5**.

Proposición. *Sea G un grupo y sea $X \subset G$ tal que $G = \langle X \rangle$ y E un conjunto sobre el que G actúa. Sea $\mathscr{C} = \mathscr{C}(G, E, X)$ el grado de Cayley de G sobre E con respecto a X.*

(a) *Para cada $e \in E$ y cada $x \in X$ hay exactamente un arco etiquetado con x que sale de e y un arco etiquetado con x que llega a e en $\mathscr{C}$.*
(b) *El grafo $\mathscr{C}$ es conexo sii la acción de $\langle X \rangle$ sobre E es transitiva.*
(c) *Sea $\iota : \mathsf{L}(X) \to G$ es el morfismo que existen la inclusión $X \hookrightarrow G$. Entonces $\mathscr{C}$ es un árbol sii ι es un isomorfismo y la acción de G sobre E es libre.*

6. Subgrupos: el teorema de Nielsen-Schreier

6.1. El resultado principal de esta sección afirma que todo subgrupo de un grupo libre es libre. Para probarlo, necesitaremos el siguiente criterio para reconocer grupos libres:

Proposición. (J. Tits, [5]) *Sea G un grupo y sea S un conjunto sobre el cual G actúa a derecha. Sea $Z \subset G$ tal que $G = \langle Z \rangle$. Sean además $(S(g))_{g \in Z \cup Z^{-1}}$ una familia de subconjuntos de S y $p \in S \setminus \bigcup_{g \in Z \cup Z^{-1}} S(g)$. Suponemos que:*

- *si $g \in Z \cup Z^{-1}$, es $p \cdot g \in S(g)$; y*
- *si $h \in (Z \cup Z^{-1}) \setminus \{g^{-1}\}$, entonces $S(h) \cdot g \subset S(g)$.*

Sea $\iota : Z \to G$ la inclusión y sea $\bar{\iota} : \mathsf{L}(Z) \to G$ el homomorfismo que extiende a ι. Entonces $\bar{\iota}$ es un isomorfismo.

Demostración. Como $G = \langle Z \rangle$, es claro que $\bar{\iota}$ es sobreyectivo, así que solo tenemos que mostrar que es inyectivo. Para hacerlo, consideremos una palabra reducida $u = z_1^{\varepsilon_1} \cdots z_n^{\varepsilon_n} \in \mathsf{L}(Z)$, con $z_1, \ldots, z_n \in Z$ y $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$, y mostremos que $\bar{\iota}(u) \neq 1$. Notemos que para lograrlo alcanza mostrar que $p \cdot \bar{\iota}(u) \in S(z_n^{\varepsilon_n})$; en efecto, como $p \notin S(z_n^{\varepsilon_n})$, esto implica que $p \cdot \bar{\iota}(u) \neq p$ y, en particular, que $\bar{\iota}(u) \neq 1$.

Si $n = 1$, es $p \cdot \bar{\iota}(u) = p \cdot z_1^{\varepsilon_1} \in S(z_1^{\varepsilon_1})$ por hipótesis. Supongamos entonces que $n > 1$. En ese caso la hipótesis inductiva implica que $p \cdot \bar{\iota}(z_1^{\varepsilon_1} \cdots z_{n-1}^{\varepsilon_{n-1}}) \in S(z_{n-1}^{\varepsilon_{n-1}})$. Ahora bien,

$$p \cdot \bar{\iota}(z_1^{\varepsilon_1} \cdots z_n^{\varepsilon_n}) = p \cdot \bar{\iota}(z_1^{\varepsilon_1} \cdots z_{n-1}^{\varepsilon_{n-1}}) \bar{\iota}(z_n^{\varepsilon_n}) \in S(z_{n-1}^{\varepsilon_{n-1}}) \cdot \bar{\iota}(z_n^{\varepsilon_n})$$

y, como $z_{n-1}^{\varepsilon_{n-1}} \neq z_n^{-\varepsilon_n}$ porque la palabra $z_1^{\varepsilon_1} \cdots z_n^{\varepsilon_n}$ es reducida, la segunda condición del enunciado nos dice que $p \cdot \bar{\iota}(u) \in S(z_{n-1}^{\varepsilon_{n-1}}) \cdot \bar{\iota}(z_n^{\varepsilon_n}) \subset S(z_n^{\varepsilon_n})$. □

6.2. Fijemos un conjunto X y un subgrupo $H \leq \mathsf{L}(X)$.

6.3. Una *sección* para H en $\mathsf{L}(X)$ es un subconjunto $\Sigma \subset \mathsf{L}(X)$ tal que para todo $c \in \mathsf{L}(X)/H$ existe un único $s \in \Sigma$ tal que $c = sH$.

6.4. Es claro que H admite una sección. En efecto, para cada $c \in G/H$ es $c \neq \emptyset$, así que existe $u_c \in c$. El conjunto $\{u_c : c \in G/H\}$ es una sección para H.

6.5. Si Σ es una sección para H, ponemos $\Delta'(\Sigma) = X \times \{\pm 1\} \times \Sigma$.

Sea $\delta = (x, \varepsilon, s) \in \Delta'(\Sigma)$. Como Σ es una sección, existe exactamente un elemento $s_\delta \in \Sigma$ tal que $x^\varepsilon s H = s_\delta H$. Ponemos

$$h_\delta = s_\delta^{-1} x^\varepsilon s.$$

6.6. Observemos que si $x^\varepsilon s \in \Sigma$, entonces $s_\delta = x^\varepsilon s$ y, en consecuencia, $h_\delta = 1$.

6.7. Por otro lado, si $\delta \in \Delta'(\Sigma)$, entonces existe $\kappa \in \Delta'(\Sigma)$ tal que $h_\kappa = h_\delta^{-1}$. De hecho, si $\delta = (x, \varepsilon, s)$, basta tomar $\kappa = (x, -\varepsilon, s_\delta)$.

6.8. Proposición. *Sea X un conjunto, $H \leq \mathsf{L}(X)$ un subgrupo y $\Sigma \subset \mathsf{L}(X)$ una sección para H en $\mathsf{L}(X)$. Sea $\Delta(\Sigma) = \{(x, \varepsilon, s) \in X \times \{\pm 1\} \times \Sigma : x^\varepsilon s \notin \Sigma\}$. Entonces $H = \langle \{h_\delta : \delta \in \Delta(\Sigma)\} \rangle$.*

Demostración. Claramente, en vista de **6.6**, basta mostrar que $\{h_\delta : \delta \in \Delta'(\Sigma)\}$ genera a H.

Sea $h \in H$. Supongamos que es $h = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ con $x_1, \ldots, x_n \in X$ y $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$.

Para cada $i \in \{1, \ldots, n\}$, existe $s_i \in \Sigma$ tal que $x_{i+1}^{\varepsilon_{i+1}} \cdots x_n^{\varepsilon_n} H = s_i H$. En particular, $s_n = 1$. Pongamos $\delta_i = (x_i, \varepsilon_i, s_i)$. Por definición, s_{δ_i} es el único elemento de Σ tal que $x_i^{\varepsilon_i} s_i H = s_{\delta_i} H$. Esto dice que $s_{\delta_1} = 1$ y que si $i > 1$, es

$$s_{i-1} H = x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}} \cdots x_n^{\varepsilon_n} H = x_i^{\varepsilon_i} s_i H = s_{\delta_i} H.$$

Como Σ es una sección, vemos que $s_{i-1} = s_{\delta_i}$ cuando $i > 1$.

Usando todo esto, concluímos que

$$h_{\delta_1} \cdots h_{\delta_n} = s_{\delta_1}^{-1} x_1^{\varepsilon_1} s_1 \cdot s_{\delta_2}^{-1} x_2^{\varepsilon_2} s_2 \cdot \cdots \cdot s_{\delta_n}^{-1} x_n^{\varepsilon_n} s_n = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = h$$

y entonces que $h \in \langle \{h_\delta : \delta \in \Delta'(\Sigma)\} \rangle$, como queríamos. □

6.9. Si Σ es una sección para H, decimos que Σ es una *sección de Schreier* si siempre que $s \in \Sigma$ y s' es un sufijo de s, entonces $s' \in \Sigma$.

6.10. Proposición. *Sea X un conjunto y $H \leq \mathsf{L}(X)$ un subgrupo de $\mathsf{L}(X)$. Entonces H admite una sección de Schreier.*

Demostración. Si $c \in G/H$, escribimos $\lambda(c) = \mathsf{mín}\{|u| : u \in c\}$.

Mostremos que existe una sucesión $(\Sigma_n)_{n \in \mathbb{N}_0}$ de subconjuntos de $\mathsf{L}(X)$ tal que:

- si $s \in \Sigma_n$, entonces $|s| = n$;
- si $c \in G/H$, entonces existe un único $s \in \Sigma_{\lambda(c)}$ tal que $c = sH$; y
- si $s \in \Sigma_n$ y s' es un sufijo de s, entonces $s' \in \Sigma_{|s'|}$.

Construimos la sucesión inductivamente, empezando por $\Sigma_0 = \{1\}$.

Sea $n \in \mathbb{N}_0$ y supongamos ya contruida una secuencia $(\Sigma_i)_{i=0}^n$ que satisface las condiciones deseadas. Consideremos $c \in \mathsf{L}(X)/H$ tal que $\lambda(c) = n + 1$. Entonces existen $x \in X$, $\varepsilon \in \{\pm 1\}$ y $u \in \mathsf{L}(X)$ tal que $x^\varepsilon u \in c$ y $|u| = n$. Entonces $\lambda(uH) = n$ y la hipótesis inductiva implica que existe un único $s' \in \Sigma_n$ tal que $uH = s'H$. Sea $s_c = x^\varepsilon s'$. Claramente $c = s_c H$ y si s' es un sufijo de s_c, es $s' \in \Sigma_{|s'|}$. Ponemos $\Sigma_{n+1} = \{s_c : c \in \mathsf{L}(X)/H,\ \lambda(c) = n + 1\}$.

Ahora pongamos $\Sigma = \bigcup_{n \in \mathbb{N}_0} \Sigma_n$. Es inmediato verificar que Σ es una sección de Schreier para H en $\mathsf{L}(X)$. □

6.11. Se sigue inmediatamente de la definición que toda sección de Schreier contiene a 1.

6.12. La razón por la cual la propiedad de Schreier nos interesa es que es precisamente la hipótesis que hace cierta la siguiente proposición:

Proposición. *Si Σ es una sección de Schreier para H y $\delta = (x, \varepsilon, s) \in \Delta(\Sigma)$, entonces tanto $x^\varepsilon s$ como $h_\delta = s_\delta^{-1} x^\varepsilon s$ son palabras reducidas.*

Por otro lado, si $\kappa \in \Delta(\Sigma)$ es tal que $h_\kappa = h_\delta$, entonces $\kappa = \delta$.

Demostración. Si $x^\varepsilon s$ es reducible, entonces claramente $\mathsf{red}(x^\varepsilon s)$ es un sufijo de s. Como Σ es una sección de Schreier, esto implica que $x^\varepsilon s \in \Sigma$, lo que es imposible porque $\delta \in \Delta(\Sigma)$.

Veamos que h_δ es reducida. Si no lo es, entonces $x^{-\varepsilon}s_\delta$ debe ser reducible, así que su reducción es un prefijo de s_δ. Como Σ es de Schreier, vemos que entonces $x^{-\varepsilon}s_\delta \in \Sigma$. Ahora bien, como $sH = x^{-\varepsilon}s_\delta H$ y Σ es una sección, podemos concluir que $s = x^{-\varepsilon}s_\delta$. Pero entonces $x^\varepsilon s = s_\delta \in \Sigma$, contradiciendo nuestra hipótesis de que $\delta \in \Delta(\Sigma)$. Esta contradicción nos dice que h_δ debe ser reducida.

Sea ahora $\kappa = (y, \eta, t) \in \Delta(\Sigma)$ tal que $h_\kappa = h_\delta$. Como $h_\delta = s_\delta^{-1}x^\varepsilon s$ y $h_\kappa = s_\kappa^{-1}y^\eta t$ son palabras reducidas, vemos que la igualdad $s_\delta^{-1}x^\varepsilon s = s_\kappa^{-1}y^\eta t$ tiene lugar en $\mathsf{M}(X^\pm)$.

Si $|s| < |t|$, $x^\varepsilon s$ resulta ser un sufijo de t y la propiedad de Schreier implica que $x^\varepsilon s \in \Sigma$, lo que es absurdo. Por simetría, no puede ser tampoco que $|s| > |t|$. Luego $s = t$, y vemos que $x = y$, $\varepsilon = \eta$ y, en definitiva, $\kappa = \delta$, como queríamos probar. □

6.13. Estamos ya en condiciones de demostrar el resultado central de esta sección. Este teorema fue obtenido, para subgrupos finitamente generados, por Jacob Nielsen en 1921; en 1926, Otto Schreier mostró en su tesis de habilitación que la hipotesis de finita generación no era necesaria.

Proposición. (J.Nielsen–O. Schreier) *Sea X un conjunto y sea $H \leq \mathsf{L}(X)$. Entonces H es libre.*

Demostración. Sea Σ una sección de Schreier para H en $\mathsf{L}(X)$ y pongamos $Y = \{h_\delta : \delta \in \Delta(S)\}$. Sabemos de **6.8** que $H = \langle Y \rangle$.

Usando **6.7** y el hecho de que no hay en $\mathsf{L}(X)$ elementos de orden 2, vemos que existe $Z \subset Y$ tal que $Y = Z \sqcup Z^{-1}$. Por supuesto, es $H = \langle Z \rangle$.

Si $y \in Y$, existe exactamente un $\delta = (x, \varepsilon, s) \in \Delta(\Sigma)$ tal que $y = h_\delta$. Ponemos entonces $S_y = \{u \in \mathsf{L}(X) : u \text{ tiene a } x^\varepsilon s \text{ como sufijo}\}$. Queremos ver que podemos aplicar **6.1** a la acción regular a derecha de H sobre $\mathsf{L}(X)$, el conjunto generador Z, la familia $(S_y)_{y \in Z \sqcup Z^{-1}}$ y $p = 1 \in \mathsf{L}(X)$.

Antes que nada, es claro que $p \notin \bigcup_{y \in Z \sqcup Z^{-1}} S_y$.

Por otro lado, si $y \in Z \sqcup Z^{-1}$ y $\delta = (x, \varepsilon, s) \in \Delta(\Sigma)$ es tal que $y = h_\delta$, entonces $p \cdot y = s_\delta^{-1}x^\varepsilon s$ tiene a $x^\varepsilon s$ como sufijo, como probamos en **6.12**, así que $p \cdot y \in S_y$. Vemos que la primera condición de **6.1** se satisface.

Para ver que también la segunda condición se cumple, tenemos que mostrar que si $\delta = (x, \varepsilon, s)$, $\kappa = (y, \eta, t) \in \Delta(\Sigma)$ son tales que $h_\delta \neq h_\kappa^{-1}$ y $w \in S(h_\kappa)$, de manera que $y^\eta t$ es un sufijo de w, entonces wh_δ tiene a $x^\varepsilon s$ como sufijo.

Ahora bien , existe λ tal que $w = \lambda y^\eta t$ y el lado derecho de esta igualdad es reducido. Entonces $w \cdot h_\delta = \lambda y^\eta t s_\delta^{-1} x^\varepsilon s$. Supongamos, para llegar a un absurdo, que $x^\varepsilon s$ no es un sufijo del miembro derecho de esta igualdad.

Es claro que debe existir entonces λ' tal que $\lambda y^\eta t = \lambda' x^{-\varepsilon} s_\delta$ y el lado derecho de esta igualdad es reducido.

Si $|t| < |s_\delta|$, vemos que $y^\eta t$ es un sufijo de s_δ, lo que no es posible. Si, en cambio, $|t| > |s_\delta|$, $x^{-\varepsilon}s_\delta$ es un sufijo de t, así que $x^{-\varepsilon}s_\delta \in \Sigma$; pero entonces, como $sH = x^{-\varepsilon}s_\delta H$, es $s = x^{-\varepsilon}s_\delta$ y $x^\varepsilon s = s_\delta \in \Sigma$: otra vez esto es imposible.

Concluimos que $|t| = |s_\delta|$. Esto implica inmediatamente que $t = s_\delta$, $y = x$ y $\eta = -\varepsilon$. Pero entonces $h_\kappa = h_\delta^{-1}$, contradiciendo nuestra hipótesis. Esto prueba que wh_δ tiene a $x^\varepsilon s$ como sufijo.

La proposición sigue entonces de **6.1**. □

6.14. Observemos que en el curso de la prueba de la proposición construimos, a partir de una sección de Schreier, una base para H.

Ejemplos

6.15. Tomemos $X = \{x, y\}$ con $x \neq y$, $n \in \mathbb{N}$ y $H = \langle\langle x^2, y^n, yxyx^{-1}\rangle\rangle$, de manera que $\mathsf{L}(X)/H \cong D_n$.

Sabemos que $\Sigma = \{x^i y^j : 0 \leq i < 2,\ 0 \leq j < n\}$ es una sección para H. Más aún, es evidente que se trata de una sección de Schreier. Es fácil ver que

$$\begin{aligned}\Delta(\Sigma) = {} & \{(x, +1, xy^j) : 0 \leq j < n\} \cup \{(x, -1, y^j) : 0 \leq j < n\} \\ & \cup \{(y, +1, xy^j) : 0 \leq j < n\} \cup \{(y, +1, y^{n-1})\} \\ & \cup \{(y, -1, xy^j : 0 \leq j < n\} \cup \{(y, -1, 1)\}\end{aligned}$$

Calculando, obtenemos la siguiente tabla:

δ	s_δ	h_δ
$(s, +1, sr^j),\quad 0 \leq j < n$	r^j	$r^{-j}s^2r^jX$
$(s, -1, r^j),\quad 0 \leq j < n$	sr^j	$r^{-j}s^{-2}r^jX$
$(r, +1, sr^j),\quad 0 < j < n$	sr^{j-1}	$r^{-(j-1)}s^{-1}rsr^j$
$(r, +1, s)$	sr^{n-1}	$r^{-(n-1)}s^{-1}rs$
$(r, +1, r^{n-1})$	1	r^n
$(r, -1, sr^j),\quad 0 \leq j < n-1$	sr^{j+1}	$r^{-(j+1)}s^{-1}r^{-1}sr^j$
$(r, -1, sr^{n-1})$	s	$s^{-1}r^{-1}sr^{n-1}$

Eliminando uno de cada par de elementos inversos en la tercera columna de la tabla obtenemos bases para H. Por ejemplo,

$$\begin{aligned}\mathcal{B} = {} & \{r^{-j}s^2r^j : 0 \leq j < n\} \cup \{r^{-(j-1)}s^{-1}rsr^j : 0 < j < n\} \\ & \cup \{r^{-(n-1)}s^{-1}rs, r^n\}\end{aligned}$$

es una de ellas.

6.16. Considerando este ejemplo, la primera parte de la siguiente proposición se hace evidente:

Proposición. *Sea X un conjunto y $H \subset \mathsf{L}(X)$ un subgrupo de índice finito. Entonces H es libre de rango finito. Más precisamente, si $n = |X|$ y $m = [\mathsf{L}(X) : H]$,*

$$\mathsf{rg}\, H = n(j-1) + 1.$$

Demostración. En la hipótesis de la proposición, existe una sección de Schreier Σ finita. La construcción de **6.13** produce entonces una base finita para H. Esto prueba la primera parte.

Veamos la segunda. Claramente, $|\Delta'(\Sigma)| = 2nj$ y entonces

$$\mathsf{rg}\, H = \frac{2nj - |\{(x, \varepsilon, s) \in X \times \{\pm 1\} \times \Sigma : x^\varepsilon \in \Sigma\}|}{2}.$$

Sea $P = \{(x, \varepsilon, s) \in X \times \{\pm 1\} \times \Sigma : x^\varepsilon \in \Sigma\}$. Queremos ver que $|P| = 2(j-1)$.

Ahora bien, si $s \in \Sigma \setminus 1$, existe exactamente un elemento $(x, \varepsilon, s) \in P$ con $x^\varepsilon s$ no reducida y existe exactamente un elemento $(y, \eta, s') \in P$ con $s = y^\eta s'$ reducida. Más aún, todo elemento de P es de uno de estos dos tipos y ninguno es de los dos tipos simultáneamente. Esto muestra que $|P| = 2(j-1)$, como queríamos. □

6.17. Por otro lado, los subgrupos de índice infinito pueden tener tanto rango finito — el subgrupo $\langle x \rangle$ en $\mathsf{L}(x, y)$ es un ejemplo de esto — o infinito:

Proposición. *Sea X un conjunto tal que $|X| = 2$ y sea $H = [\mathsf{L}(X), \mathsf{L}(X)]$ el subgrupo derivado de $\mathsf{L}(X)$. Entonces H tiene rango numerable.*

Demostración. Supongamos que $X = \{x, y\}$. Es claro que $\Sigma = \{x^i y^j : i, j \in \mathbb{Z}\}$ es una sección de Schreier para H. Calculando, vemos que

$$\Delta(\Sigma) = \{(y, +1, x^i y^j) : i, j \in \mathbb{Z},\, i \neq 0\} \sqcup \{(y, -1, x^i y^j) : i, j \in \mathbb{Z},\, i \neq 0\}$$

y obtenemos la siguiente tabla:

δ	s_δ	h_δ
$(y, +1, x^i y^j), \quad i, j \in \mathbb{Z},\, i \neq 0$	$x^i y^{j+1}$	$y^{-j-1} x^{-i} y x^i y^i$
$(y, -1, x^i y^j), \quad i, j \in \mathbb{Z},\, i \neq 0$	$x^i y^{j-1}$	$y^{-j+1} x^{-i} y^{-1} x^i y^i$

Eliminando un elemento de cada par de elementos inversos de la tercera columna, vemos que, por ejemplo,

$$\mathcal{B} = \{y^{-j-1} x^{-i} y x^i y^i : i, j \in \mathbb{Z},\, i \neq 0\}$$

es una base de H. Por supuesto, esto implica que $\operatorname{rg} H = \aleph_0$. □

6.18. Por supuesto, como un grupo libre de rango no numerable es no numerable, si X es finito entonces $\mathsf{L}(X)$ no posee subgrupos de rango no numerable.

Referencias

[1] D. J. Collins, R. I. Grigorchuk, P. F. Kurchanov, and H. Zieschang, *Combinatorial group theory and applications to geometry*, Springer-Verlag, Berlin, 1998. Translated from the 1990 Russian original by P. M. Cohn; Reprint of the original English edition from the series Encyclopaedia of Mathematical Sciences [*Algebra. VII*, Encyclopaedia Math. Sci., 58, Springer, Berlin, 1993].

[2] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[3] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*, 2nd ed., Dover Publications Inc., Mineola, NY, 2004. Presentations of groups in terms of generators and relations.

[4] J. J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[5] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

Estas notas fueron compuestas por el autor usando el sistema TEX, de Donald Knuth, y, entre otros, los paquetes de macros LATEX, AMS-math, XY-pic, TikZ, PGF y algunas macros propias. La fuente del texto es Palatino, de Hermann Zapf, mientras que la fuente usada en las ecuaciones es Pazo Math, de Diego Puga.