Lección nº 5 Junio, 2021

Capítulo 5

Grupos libres

Definición. Sea X un subconjunto de un grupo G. Diremos que X es un *sistema libre de generadores de* G (o base de G) si todo $g \in G \setminus \{1\}$, g se escribe de forma única como producto

$$g = x_1^{n_1} \dots x_k^{n_k},$$

donde $x_1, \dots, x_n \in X$ y $n_1, \dots,_k \in \mathbb{Z}$ y para $1 \leq i \leq k$ se cumple que: $n_i \neq 0$ y $x_i \neq x_{i+1}$.

Con forma única nos referimos a que si g es de la forma $g = y_1^{m_1} \dots y_l^{m_l}$, con $y_1, \dots, y_l \in X$, $m_1, \dots, m_l \in \mathbb{Z}$ y donde $y_i \neq y_{i+1}$ y $m_i \neq 0$ para todo $1 \leq i \leq l$, entonces $k = l$ y $y_i = x_i$ para todo $1 \leq i \leq k$.

Definición. Un grupo G es libre si admite un sistema libre de generadores.

Ejemplo 5.1. G un grupo con un generador $g \in G$,

$$G = \langle g \rangle = \{1, g^{\pm 1}, g^{\pm 2}, \dots, g^{\pm n}, \dots\},$$

tal que si $g^n \neq g^m$ entonces $m \neq n$ (es decir que G es un grupo cíclico infinito), entonces G es libre.

Ejemplo 5.2. Sea G libre con sistema de generadores $\{x, y\}$. Los elementos de G son de la forma

$$x^{n_1} y^{n_1} x^{n_2} y^{n_2} \dots x^{n_k} y^{mk}.$$

Teorema 5.3. *Sea $X \neq \emptyset$ un conjunto. Entonces X es un sistema libre de generadores de un grupo G. En particular existen grupos libres con bases arbitrarias.*

Construcción de G: Una *palabra* del "*alfabeto*"X es una expresión formal

$$x_1^{m_1} x_2^{m_2} \dots x_n^{x_n},$$

con $x_1, x_2, \dots, x_n \in X$, $m_1, \dots, m_n \in \mathbb{Z}$. Diremos que esta palabra es *reducida* si $x_i \neq x_{i+1}$ y $m_i \neq 0$ para todo $1 \leq i \leq n$. Por ejemplo $x_1 x_2 x_1$ es reducida si $x_1 \neq x_2$, y $x_1^2 x_2^3 x_2^5$ no es reducida. La palabra $x_1^2 x_2^3 x_2^5$ se puede reducir usando la operación $x^a x^b = x^{a+b}$ y x^0 se "borra". Luego

$$x_1^2 x_2^3 x_2^5 \xrightarrow{\text{red}} x_1^2 x_2^8,$$

que es reducida.

Ejemplo 5.4. Tomemos $X = \{x, y, z\}$ y $p = x^{-3}x^2y^5y^{-6}y^6x^7z^2z^3x^{-1}xzy^2x^{-1}$, entonces

$$p \xrightarrow{\text{red}} x^{-1}y^5x^7z^6y^2x^{-1}.$$

Proceso de reducción: Si en una palabra aparecen bases repetidas consecutivas, se reemplazan por la base elevada a la suma de los exponentes, x^0 se elimina ($x^0 \to 1$).

Proposición 5.5. *(1) El proceso de reducción de una palabra no es único.*

(2) Toda palabra se puede, por este proceso de reducción, conducir a una palabra reducida, la cual no depende del proceso de reducción.

Hay varias maneras de presentar un grupo finito.

(1) Subgrupo de permutaciones $G \to \mathrm{Sym}(G)$.

(2) Subgrupo de $\mathrm{GL}(n, \mathbb{K})$:

$$\begin{array}{rl} G \to S(G) & \to \mathrm{GL}(n, \mathbb{R}) \\ \sigma & \mapsto I_\sigma. \end{array}$$

(3) Descripción por generadores y relaciones. Ejemplos:

- Grupo cíclico: $C(n) = \langle g \mid g^n = 1 \rangle$.
- $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, xyx = x^{-1} \rangle$. No es el único grupo que satisfacen estas relaciones pues $C(2) = \langle a, b \mid a^2 = 1, b^2 = 1, ab = ba \rangle$.
- $Q_n = \langle a, b \mid a^{2^{n-1}}, b^2 = a^{2^{n-2}}, bab^{-1} = a^{-1} \rangle$. Para $n = 3$ tenemos el grupo de cuaterniones Q_6.

Definición (Grupos abelianos libres)**.** A es un grupo abeliano libre si y sólo si $X \subseteq A$ tal que para toda aplicación $f\colon X \to G$, con G un grupo abeliano, existe una única extensión de f a A tal que el diagrama

$$\begin{tikzcd} A \arrow[dr, dashed, "\tilde{f}"] & \\ X \arrow[u, "i"] \arrow[r, "f"'] & G \end{tikzcd}$$

es tal que $f = \tilde{f} \circ i$. X se dice base de A.

Definición (Grupo libre)**.** Sea F un grupo y $X \hookrightarrow F$ un subconjunto. F es un *grupo libre* con base X si para cualquier aplicación $f\colon X \to G$, con G un grupo, existe un único homomorfismo $\tilde{f}\colon F \to G$ tal que el diagrama

$$\begin{tikzcd} F \arrow[dr, dashed, "\tilde{f}"] & \\ X \arrow[u, "i"] \arrow[r, "f"'] & G \end{tikzcd}$$

es tal que $f = \tilde{f} \circ i$.

Supongamos que para todo conjunto X existe un grupo libre con base X. Definamos al grupo libre $F = F(\{x,y\})$, $X = (\{x,y\})$. Denotemos por N al subgrupo normal de F generado por los elementos

$$X = \{x^{2^{n-1}}, y^{-2}x^{2^{n-2}}, yxyx^{-1}\},$$

es decir $N = \bigcap\limits_{\substack{K \trianglelefteq F \\ X \subset K}} K$. Formemos el cociente F/N. Demostraremos que se tiene un epimorfismo

$$\begin{aligned} \tilde{f} \colon F/N &\twoheadrightarrow Q_n \\ \overline{x} &\mapsto a \\ \overline{y} &\mapsto b. \end{aligned}$$

Así se comprueba que $|Q_n| \leq |F(N)| = 2^n$, de donde $|Q_n| = 2^n$.

Sea X un conjunto arbitrario y sea X^{-1} un conjunto no vació, disjunti de X tal que

$$\begin{aligned} \phi \colon X &\to X^{-1} \\ x &\mapsto \phi(x) := x^{-1}, \end{aligned}$$

es una biyección. Al conjunto $X \cup X^{-1}$ lo llamamos un alfabeto. Los elementos de $X \cup X^{-1}$ se llaman letras. Definimos una *palabra* en este alfabeto a una función

$$w \colon \{1, 2, \ldots, n\} \to X \cup X^{-1}$$

para algún $n \in \mathbb{N}_0$ (cuando $n = 0$, X tiene la palabra vacía, que denotaremos por 1). Denotaremos

$$w(i) = x_i^{e_i}, \quad e_i \pm 1 \qquad \forall 1 \leq i \leq m,$$

y $|w| = n$ se llama el largo de la palabra w. También denotamos

$$w = x_1^{e_1} x_2^{e_1} \ldots x_n^{e_n} \quad \text{y} \quad 1 = (\ ).$$

Ejemplo 5.6. $|xx^{-1}|$=$|x^{-1}x| = 2$ y $|1| = 0$, $\left|x_1 x_2^{-1} x_1 x_3\right| = 4$.

Definición. Dos palabras u, v, $u = x_1^{e_1} \ldots x_n^{e_n}$, $v = y_1^{d_1} \ldots y_n^{d_m}$, son iguales $(u = v)$ si y sólo si $m = n$ y para todo $1 \leq i \leq n$: $x_i = y_i$ y $e_i = d_i$.

Definición. Sea $w = x_1^{e_1} \ldots x_n^{e_n}$ una palabra. Una subpalabra de w es 1 ó $v = x_r^{e_r} \ldots x_s^{e_s}$ con $1 \leq r \leq s \leq n$.

Ejemplo 5.7.
- $x_1^{e_1}$ es una subpalabra de $w = x_1^{e_1} \ldots x_n^{e_n}$.
- xy es subpalabra de $xyx^{-1}xy$, o xyx^{-1} y también lo es.

Si $u = x_1^{e_1} \ldots x_n^{e_n}$ es palabra, entonces

$$u^{-1} = x_n^{-e_n} \ldots x_1^{-e_1}$$

es la *palabra nueva* de u.

Sea $W(X)$ el conjunto de todas las palabras en X $(W(\emptyset) = \{1\})$. Una palabra w se dice *reducida* si no tiene subpalabras de la forma xx^{-1} o $x^{-1}x$ con $x \in X$.

Ejemplo 5.8.

- $xyx^{-1}xyxx$ no es reducida.
- $xyyxx$ sí es reducida.

Multiplicación: a $W(X)$. Por yuxtaposición: Si $u, v \in W(X)$, $u, v \mapsto uv$. Así obtenemos una función
$$\cdot\colon W(X) \times W(X) \to W(X).$$

(1) $\cdot$ es asociativa:
$$u \cdot (v \cdot w) = u \cdot vw = uvw$$
$$(u \cdot v) \cdot w = uv \cdot w = uvw.$$

Así $(u \cdot v) \cdot w = u \cdot (v \cdot w)$.

(2) $1 \in W(X)$,
$$1 \cdot u = u \cdot 1 = u.$$

$W(X)$ es un *monoide.*

Observación. En $W(X)$, $xx^{-1} \neq 1$, $x^{-1}x \neq 1$.

Definición (Operaciones elementales)**.** Sea $A, B \in W(X)$ (posiblemente vacíos), y sea $w = AB$.

i. *Inserción* $AB \to Aaa^{-1}B$, con $a \in X$.

ii. *Eliminación* Si $w = Aaa^{-1}B$ ó $Ab^{-1}bB$, entonces
$$w \to AB.$$

Definición. Sean w y w' dos palabras. Escribiremos $w \to w'$ si w' se obtiene de w por una operación elemental.

Definición. Dos palabras $u, v \in W(X)$ se dicen equivalentes si existe una cadena de operaciones equivalentes
$$u = w_1 \to W_2 \to \cdots \to w_n = v.$$
Denotamos
$$u \sim v.$$

Ejercicio 5.9. Probar que $\sim$ es una relación de equivalencia en $W(X)$.

En particular, el ejercicio anterior muestra que toda operación elemental es invertible. Notamos por $[u]$ a la clase de equivalencia de una palabra u.

Ejemplo 5.10. $xx^{-1} \sim 1$, pues $xx^{-1} \to 1$ por eliminación, para todo $x \in X$.

Proposición 5.11. *Sean X un conjunto y $W(X)$ el monoide de palabras sobre X. Se tiene que*

(1) Si $u \sim u'$ y $v \sim v'$ entonces $uv \sim u'v'$.

(2) Si G es un grupo y $f\colon X \to G$ es una aplicación, entonces existe un homomorfismo (de

monoides) $\tilde{f}\colon W(X) \to G$ *tal que* $f = \tilde{f} \circ i$, *donde* $i\colon X \to W(X)$ *y*

$$\begin{tikzcd} W(X) \arrow[dr, "\tilde{f}"] & \\ X \arrow[u, "i"] \arrow[r, "f"'] & G \end{tikzcd}$$

con la propiedad: si $u \sim v$ *entonces* $(u) = \tilde{f}(v)$.

Demostración. (1) Supongamos que $u \sim u'$ y $v \sim v'$, así

$$u = w_1 \to w_2 \to \cdots \to w_n = u'$$
$$v = z_1 \to z_2 \to \cdots \to z_n = v'.$$

Luego

$$uv \to w_2 v \to \cdots \to u'v \to u'z_2 \to u'v',$$

es decir que $uv \sim u'v'$.

(2) Sean $f\colon X \to G$ una aplicación y $w \in W(X)$, w se escribe de manera única

$$w = x_1^{e_1} \dots x_n^{e_n}.$$

Entonces podemos definir

$$\tilde{f}(w) = f(x_1)^{e_1} \dots f(x_n)^{e_n}.$$

Si $x \in X$, $\tilde{f}(x) = f(x)$ y f es un homomorfismo pues

$$\tilde{f}(xy^{-1}) = f(x)f(y)^{-1} = \tilde{f}(x)\tilde{f}(y)^{-1},$$

para todo $x, y \in X$.

$\square$

Notación. $\tilde{f}([u]) := \tilde{f}(u)$.

Observación. $x_1^{e_1} \dots x_n^{e_n} x_n^{-e_n} \dots x_1^{-e_1} \sim 1$, así $[uu^{-1}] \sim [1]$ para todo $x_1, \dots, x_n, u \in X$.

De la propiedad 1 de la proposición anterior se sigue que si $u \sim u'$ y $v \sim v'$, entonces $uv \sim u'v'$ y así

$$\tilde{f}(uv) = \tilde{u'v'}.$$

Teorema 5.12. *Para toda palabra* $w \in W(X)$ *existe una única palabra reducida* w' *tal que* $w \sim w'$. *En particular, si* $[w]$ *es la clase de equivalencia de* w, *entonces* $[w] = [w']$ *y* w' *es la única representante de* $[w]$ *que es reducida.*

Demostración. Si $X = \emptyset$ entonces $W(X) = \{1\}$ y no hay nada que demostrar. Así, suponemos que $X \neq \emptyset$. Procedemos por inducción respecto al largo de las palabras. Suponemos que para todo w tal que $|w| = x$ existe w' reducida tal que $w' \sim w$. Sea $w \in W(X)$ tal que $|w| = n + 1$, demostraremos que existe $w' \in W(X)$ reducida tal que $w' \sim w$. Si w ya es reducida tomamos $w' = w$, si no, existe subpalabra aa^{-1} (o $a^{-1}a$) de w. Sea xx^{-1} la primera palabra de esta forma que aparece en w, así $w \to w_1$, donde w_1 se obtiene de w por eliminación de xx^{-1}. Luego, tenemos que $|w_1| < |w| = n + 1$

y por hipótesis de inducción existe w' reducida tal que $w' \sim w$, pero como $w \sim w_1$, se concluye que $w' \sim w$.

Unicidad: Basta demostrar que si u y v son dos palabras reducidas tales que $u \sim v$, entonces $u = v$. Supongamos que $u \sim v$, así, existe al menos una cadena de operaciones elementales

$$u = w_1 \to w_2 \to \cdots \to w_m = v.$$

De todas las cadenas elejimos la que posea rango minimal $n \in N$. Como u y v son reducidas, entones la primera operación elemental es una inserción y la última debe ser una eliminación. Existe un índice i tal que

$$w_{i-1} \xrightarrow[\substack{\text{inserción}\\ aa^{-1}}]{} w_i \xrightarrow[\substack{\text{eliminación}\\ bb^{-1}}]{} w_{i+1}.$$

Consideramos varios casos.

(1) Si las palabras aa^{-1} y bb^{-1} coinciden, entonces

$$u \to w_{i-1} \to w_{i+1} \to \cdots \to v,$$

obteniendo una cadena de largo menor que n, lo cual es una contradicción.

(2) Si las palabras aa^{-1} y bb^{-1} se intersectan, esto puede pasar de dos maneras

i) Si

$$w_{i-1} \to w_i = Aaa^{-1}b^{-1}B \to w_{i+1},$$

entonces $b = a^{-1}$ o $(a = b^{-1})$, de donde $w_i = Aaa^{-1}aB$, $w_{i-1} = AaB$ y $w_{i+1} = AaB$, entonces se obtiene nuevamente una cadena de largo menor.

ii) Si

$$w_{i-1} \to w_i = Abb^{-1}b^{-1}B \to w_{i+1},$$

entonces $a^{-1} = b$ y se sigue lo mismo que en i).

(3) Las palabras aa^{-1} y bb^{-1} no se intersecan, entonces

$$\begin{aligned} w_i &= A'aa^{-1}A''bb^{-1}B \\ w_{i+1} &= A'aa^{-1}A''B = A'aa^{-1}C \\ w_{i-1} &= A'A''bb^{-1}B. \end{aligned}$$

En este caso, existen $j < i-1$ y $k > i+1$ tales que

$$w_{j-1} \to w_j$$

es inserción de bb^{-1} y

$$w_k \to w_{k+1}$$

es eliminación de aa^{-1}, y entonces obtenemos una cadena de largo menor eliminando estas dos operaciones, con las modificaciones apropiadas (los detalles se dejan como ejercicio para el lector). $\square$

Definición. $F(X) = F = W(X)/\sim$

Si $u \in W(X)$, entonces $[u] = \{v \in W(X) \colon u \sim v\}$. Hemos visto que para toda clase de equivalencia $[u] \in F$, existe una única palabra reducida u' tal que $[u] = [u']$. Además, si w y w' son reducidas, si $[w] = [w']$ entonces $w = w'$. Esto permite identificar $[u] = u$ cuando u es una palabra reducida. Entonces, si $[u] \in F$, escribimos $[u] = [u'] = u'$, con u' reducida. En resumen, F se identifica con todas las palabras reducidas.

Definición. Definimos el producto en $F(X) = F = W(X)/\sim$, para $u, v \in W(X)$ y u', v' palabras reducidas tales que $[u] = u'$, $[v] = v'$:

$$u' \cdot v' = [u] \cdot [v] := [uv] = (uv)'$$

el cual es asociativo, $1 = [1]$, $1 \cdot [u] = [u] \cdot 1 = [u]$ y $[u][u^{-1}] = [uu^{-1}] = [1] = 1 = [u^{-1}][u]$.

Teorema 5.13. *Sea X un conjunto, entonces $F = F(X)$ es un grupo libre con base X.*

Demostración. Si $X = \emptyset$, entonces $F = \{1\}$ es un grupo libre. Supongamos que $X \neq \emptyset$. Vimos que $\sim$ es compatible con la operación de yuxtaposición. La operación producto

$$u' \cdot v' = [u] \cdot [v] := [uv] = (uv)'$$

está bien definida. Demostraremos la asociatividad mediante la asociatividad de la yuxtaposición.

$$[u] \cdot ([v] \cdot [w]) = [u] \cdot [vw] = [u(vw)] = [(uv)w] = [uv][w] = ([u] \cdot [v])[w].$$

El elemento neutro es $1 = [1]$. El elemento inverso: Sea $u = x_1^{e_1} \dots x_n^{e_n}$ y tomamos $u^{-1} x_n^{-e_n} \dots x_1^{-e_1}$, entonces

$$[u] \cdot [u^{-1}] = [uu^{-1}] = [x_1^{e_1} \dots x_n^{e_n} x_n^{-e_n} \dots x_1^{-e_1}] = [1] = 1.$$

Así, $[u]^{-1} = [u^{-1}]$. Hemos probado que $F(X)$ es un grupo.

Se puede ver con facilidad que X es un sistema de generadores de $F(X)$. Sea $[w] = w \in F$ reducida. Así $w = x_1^{e_1} \dots x_n^{e_n}$, con $x_1, \dots, x_n \in X$.

La unicidad de la representación de la palabra reducida implica que si

$$w = x_1^{e_1} \dots x_n^{e_n} = y_1^{d_1} \dots y_n^{d_n},$$

entonces $n = m$, $e_i = d_i$ y $x_i = y_i$ para todo $1 \leq i \leq n$.

Probemos que $F(X)$ posee la propiedad universal de un grupo libre. Tenemos que $X \overset{i}{\hookrightarrow} F(X)$ y sean G un grupo, $f \colon X \to G$ una aplicación. Tenemos el diagrama

$$\begin{tikzcd} F(X) \arrow[dr, dashed, "\tilde{f}"] & \\ X \arrow[u, "i"] \arrow[r, "f"'] & G. \end{tikzcd}$$

Para todo $w \in F(X)$ reducida, w se escribe de manera única $w = x_1^{e_1} \dots x_n^{e_n}$, definimos

$$F(w) = f(x_1)^{e_1} \dots f(x_m)^{e_m}.$$

Obtenemos una aplicación

$$\begin{aligned} \tilde{f} \colon F(X) &\to G \\ x &\mapsto \tilde{f}(x), \end{aligned}$$

donde la igualdad $\tilde{f} \circ i = f$ es inmediata. Finalmente, para ver que $\tilde{f}$ es un homomorfismo: Si $v = x_1^{e_1} \dots x_n^{e_n}$ y $w = y_1^{d_1} \dots y_m^{d_n}$, se tiene que

$$f(vw^{-1}) = f(x_1)^{e_1} \dots f(x_n)^{e_n} f(y_1)^{-d_1} \dots f(y_m)^{-d_m} = f(v)f(w).$$

$\square$

Ejercicio 5.14. Sean X_1 y X_2 dos conjuntos. Si $X_1 \to X_2$ es una biyección, esta biyección se extiende a un isomorfismo $F(X_1) \xrightarrow{\sim} F(X_2)$.

Consideremos el caso particular $X\{x_1, \dots, x_n\}$, sea $F_n = F(x_1, \dots, x_n)\colon = (\{x_1, \dots, x_n\})$.

Proposición 5.15. *Sea $F_n'\colon = [F_n, F_n]$ el subgrupo de conmutadores de F_n. Entonces F_n/F_n' es abeliano libre en donde $X' = \{x_1F_n', \dots, x_nF_n'\}$. Así $F_n/F_n' \equiv \bigoplus_{i=1}^n x_iF_n'\mathbb{Z}$.*

Demostración. $X = \{x_1, \dots, x_n\}$ genera a F_n. Consideremos

$$\begin{array}{rcl} F_n & \longrightarrow & F_n/F_n' \\ g & \longmapsto & \bar{g} = gF_n'. \end{array}$$

Así, si $\bar{u} \in F_n/F_n'$ y $u = x_1^{e_1} \cdots x_n^{e_n}$, entonces obtenemos que

$$\bar{u} = \bar{x_1}^{e_1} \cdots \bar{x_n}^{e_n},$$

es decir $\{x_1F_1', \dots, x_nF_n'\}$ es un sistema de generadores de F_n/F_n'.

Probemos que la aplicación natural

$$\begin{array}{rcl} \{x_1, \dots, x_n\} & \hookrightarrow & F_n/F_n' \\ x_i & \longmapsto & \bar{x_i}, \end{array}$$

es inyectiva. Supongamos que $\bar{x_1} = \bar{x_2}$, entonces $\overline{x_1x_2^{-1}} = 1$, y así $x_1x_2^{-1} \in F_n'$. Por tanto

$$x_1x_2^{-1} = \prod_k x_i^{e_1} x_k^{e_k} x_i^{-e_1} x_k^{-e_n}. \tag{5.1}$$

Si $x_1 = x_2$, entonces esto se escribe como

$$1 = \prod_{\substack{k \\ x_1 = x_2 = x}} x_i^{e_1} x_k^{e_k} x_i^{-e_1} x_k^{-e_k},$$

con $F_{n-1} = F(x_1, x_2, \dots, x_n)$; de donde, (5.1) no es posible pues F_{n-1} es libre.

Queda probar que F_n/F_n' es abeliano libre con base $\{\bar{x_1}, \dots, \bar{x_n}\}$. Sea $j\colon \{\bar{x_1}, \dots, \bar{x_n}\} \to F_n/F_n'$, y sea

$$\begin{array}{rcl} \pi\colon \{x_1, \dots, x_n\} & \longrightarrow & \{\bar{x_1}, \dots, \bar{x_n}\} = \bar{X} \\ x_i & \longmapsto & \bar{x_i}. \end{array}$$

Sea, además, $p\colon X \hookrightarrow F_n$, con lo que tenemos el siguiente diagrama

$$\begin{tikzcd}
F_n \arrow[rr, "\pi"] \arrow[dr, dotted, "g"] & & F_n/F_n' \arrow[dl, dotted] \\
& G & \\
X \arrow[uu, "p"] \arrow[ur, "r\pi"] \arrow[rr, "\pi/X=\Pi"] & & \bar{X}. \arrow[ul, "r"'] \arrow[uu, "j"']
\end{tikzcd}$$

Sea G un grupo abeliano y $r\colon \bar{X} \to G$ una aplicación cualquiera. Sea la composición

$$X \xrightarrow{\ \pi\ } \bar{X} \xrightarrow{\ r\ } G$$

$$X \xrightarrow{\ r\pi\ } G.$$

Como G es libre sobre X existe un homomorfismo $g\colon F \to G$ tal que $g|_X = r\pi$ y $g \circ p = r \circ \pi = r\pi$. Como G es abeliano, $F_n' \subseteq \ker(g)$. Así, el homomorfismo $F_n \xrightarrow{\pi} F_n/F_n'$ se factora a través de un único homomorfismo

$$g'\colon F_n/F_n' \longrightarrow G,$$

dado por $g'(wF_n') = g(w)$, y así $g' \circ j = r$ (pues $g' \circ \pi = g$ y entonces $g'j\pi = g'\pi p = gp = r\pi$.)

Como π es epiyectiva, $g'j = r$. Así, F_n/F_n' verifica la propiedad universal del grupo abeliano libre, con base $\bar{X}$. □

5.1. Presentaciones de Grupos

Definición. Sea G un grupo. Una *presentación* de G es un par ordenado $G = (X|R)$, donde X es un conjunto y $R \subseteq W(X)$ tal que

$$G \cong F(X)/N,$$

donde $F = F(X)$ es el grupo libre con base X y N es el subgrupo normal de $F(X)$ generado por R, es decir,

$$N = \langle \{grg^{-1} \mid g \in F, r \in R\} \rangle$$

Los elementos de R se llaman *relaciones*.

Definición. Un grupo G con la presentación $(X|R)$ se llama *finitamente presentado* si X y R son finitos.

Observación. Existen grupos finitamente generados que no son finitamente presentados (Neumann)

Ejemplos 5.16.

(1) Consideremos $G = C(6) = (x|x^6)$, donde $x^6 = xxxxxxx$. Pero G admite otra presentación

$$G = (x, y|x^2, y^2, xyx^{-1}x^{-1}).$$

Así, $G = \langle a \mid a^6 = 1\rangle$, $G = \langle a, b \mid a^3 = b^3 = 1, ab = ba\rangle$.

(2) Tomemos $G = D_{2n}$, en este caso $G = (x, y|x^n, y^2, xyx^{-1}y^{-1})$.

(3) $F(X) = (X|\emptyset)$.

Notación: Sea r una palabra en $x_1, \ldots, x_n$, entonces $r = r(x_1, x_2, \ldots, x_n)$. Si G es un grupo y $g_1, \ldots, g_n \in G$, podemos reemplazar x_i por g_i y obtenemos un elemento de G, $r(g_1, \ldots, g_n) \in G$. En el caso $G = (X|R)$ y $G \cong F(X)/N$, entonces todas las $r \in R$ se transforman en $r(\bar{x_1}, \ldots, \bar{x_n}) = 1$, donde $\bar{x}$ representa la clase de x en G.

Teorema 5.17 (de von Dyck). *Sea G un grupo con una presentación $G = (x_1, \ldots, x_n|r_j,\ j = 1, \ldots, J)$ tal que $G = F(X)/N$, con $N \trianglelefteq F(X)$ generado por $r_1, \ldots, r_J$. Sea H un grupo* *generado por $h_1, \dots, h_n$, es decir $H = \langle h_1, \dots, h_n \rangle$ tal que*

$$r_j(h_1, \dots, h_n) = 1 \quad \forall\, j \in \{1, \dots, J\}.$$

Entonces, existe un epimorfismo $G \twoheadrightarrow H$ tal que $x_i N \mapsto h_i$ para todo $i \in \{1, \dots, n\}$.

Demostración. Sea $F = F(x_1, \dots, x_n)$ grupo libre y sea

$$\begin{array}{rcl} \{x_1, \dots, x_n\} & \xrightarrow{f} & H \\ x_i & \longmapsto & h_i. \end{array}$$

Por la propiedad universal del grupo libre existe un único homomorfismo $\varphi\colon F \to H$ tal que $\varphi(x_i) = h_i$ para todo $i \in \{1, \dots, n\}$, de hecho, φ es un epimorfismo. Como $r_j(h_1, \dots, h_n) = 1$ para todo j, vemos que $r_j(x_1, \dots, x_n) = r_j \in \ker(\varphi)$ para todo $j \in \{1, \dots, J\}$; y por ende N, el subgrupo normal generado por los r_j's, verifica

$$N \trianglelefteq \ker(\varphi).$$

Por tanto, φ induce un epimorfismo $\bar{\varphi}\colon F/N \twoheadrightarrow H$ tal que $\bar{\varphi}(x_i N) = h_i$ para todo $i \in \{1, \dots n\}$. □

Ejemplo 5.18. Consideremos $\mathbb{Q}_n$ el "grupo"de cuaternioes generalizados, es decir

$$\mathbb{Q}_n = \langle a, b \,|\, a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}} = -1, bab^{-1} = a^{-1} \rangle,$$

con $|\mathbb{Q}_n| = 2^n$.

Ahora, vamos a generalizar estas relaciones. Sea $w = 2^{n-1}$ raíz primitiva de 1 en $\mathbb{C}$„ es decir

$$w = e^{\frac{2\pi}{2^{n-1}} i} i$$

Así, $w^{2^{n-1}} = 1$, y $|w| = 2^{n-1}$.

Definamos

$$A = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

y sea $H_n = \langle A, B \rangle \leq \mathbb{C}^*$. Entonces

$$A^{2^j} = \begin{pmatrix} w^{2^j} & 0 \\ 0 & w^{-2^j} \end{pmatrix},$$

y por ende $A^{2^{n-1}} = I$. Además, también se tiene que

$$A^{2^{n-2}} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = B^2 = -I,$$

y

$$BAB^{-1} = \begin{pmatrix} w^{-1} & 0 \\ 0 & w \end{pmatrix} = A^{-1}.$$

En consecuencia

$$H_n = \langle A, B \,|\, A^{2^{n-1}} = I, B^2 = A^{2^{n-2}} = -I, BAB^{-1} = A^{-1} \rangle.$$

Vemos que $AB \neq BA$, por lo que H_n no es conmutativo. También $B \notin \langle A \rangle$, pero $B^2 \in \langle A \rangle$. Así

$$H_n \supseteq \langle A \rangle \cup^{\circ} B \langle A \rangle,$$

por ende $|H_n| \geq 2^{n-1} + 2^{n-1} = 2^n$.

Demostremos que H_n realiza a $\mathbb{Q}_n$. Consideremos el grupo con 6 permutaciones

$$G_n = (x, y | x^{2^{n-1}} = 1, y^2 = a^{2^{n-2}}, yxy^{-1} = x^{-1}).$$

Existe un epimorfismo $G_n \twoheadrightarrow H_n$ tal que

$$x \longmapsto A, \quad y \longmapsto B.$$

Luego, $|G_n| \geq |H_n| \geq 2^n$. Notemos que $\langle x \rangle \trianglelefteq G_n$ y $G_n/\langle x \rangle = \langle \bar{y} \rangle$. Y como $y' \in \langle x \rangle$, entonces $\bar{y}^2 = \bar{1}$, así

$$G_n/\langle x \rangle = \langle \bar{y} \rangle = \{\bar{1}, \bar{y}\},$$

de donde $|G_n/\langle x \rangle| \leq 2$. Por lo tanto

$$|G_n| \leq |G_n/\langle x \rangle||\langle x \rangle| \leq 2 \cdot 2^{n-1} \cdot 2^n,$$

de donde $2^n \geq |G_n| \geq |H_n| \geq 2^n$, y así $|G_n| = |H_n| = 2^n$. Por tanto, $H_n = \mathbb{Q}_n$.

Ejercicio 5.19. $D_{2n} = \langle a, b \,|\, a^n = 1, b^2 = 1, bab = a^{-1} \rangle$. Demostrar que $|D_{2n}| = 2n$.

Ejercicio 5.20. Sea F grupo libre con base X, y sea $Y \subseteq X$. Sea $N \trianglelefteq F$ el subgrupo normal generado por Y. Probar que F/N es libre.

Teorema 5.21 (Nielsen - Schreier)**.** *Sea F un grupo libre y $S \leq F$. Entonces S es libre.*

Definición. Sea G un grupo y $S \leq G$. Se define

$$S \backslash G = \{Sb \,|\, b \in G\}.$$

Un *transversal de S en G* (sistema de representantes de las clases laterales) consiste en exactamente un elemento

$$l(Sb) \in Sb,$$

para toda clase lateral $Sb \in S\backslash G$ tal que $l(S) = 1$.

Sea F un grupo libre y $S \leq F$. Sea l un transversal de S en F, y sea X base de F. Observemos que para todo $x \in X$ y para todo $Sb \in S\backslash F$, consideramos la clase lateral Sbx

$$l(Sb)x \in Sbx, \quad l(Sbx) \in Sbx,$$

así $t_{Sb,x} = l(Sb)xl(Sbx)^{-1} \in S$.

La idea es demostrar que eligiento una transversal l adecuada (transversal de Schreier), los elementos $1 \neq t_{Sb,x}$ y $Sb \in S\backslash F$, para cada $x \in X$, forman una base de S.

Notación: Para todo $Sb \in S\backslash F$, $x \in X$, sea $y_{Sb,x}$ un símbolo. Así

$$\{y_{Sb,x}\} \longrightarrow \{t_{Sb,x}\}.$$

Sea Y el grupo libre con base $\{y_{Sb,x} \,|\, Sb \in S\backslash F,\, x \in X\}$, y tenemos una aplicación

$$\begin{aligned} \varphi \colon \{y_{Sb,x}\} &\longrightarrow S \\ y_{Sb,x} &\longmapsto t_{Sb,x}. \end{aligned}$$

φ se prolonga con un homomorfismo, también denotado por φ,

$$\varphi\colon Y \longrightarrow S$$

tal que $\varphi(y_{Sb,x}) = t_{Sb,x}$, es decir

$$\varphi(y_{Sb,x}) = l(Sb)xl(Sbx)^{-1}.$$

Para toda clase lateral Sb, definamos una aplicación

$$\begin{aligned}
(\ )^{Sb}\colon F &\longrightarrow Y \\
u &\longmapsto u^{Sb},
\end{aligned}$$

donde u^{Sb} se define por inducción respecto al largo de la palabra $(|\cdot|)$.

- $|u| = 0$ si y solo si $u = 1$. En este caso $1^{Sb} = 1$.
- Sea $|u| \geq 1$.
  - Si $|u| = 1$, $u = x^e$ con $e = \pm 1$, $x \in X$. Definamos

    $$x^{Sb} = y_{Sb,x}, \quad (x^{-1})^{Sb} \cdot (x^{Sbx^{-1}})^{-1} = (y_{Sbx^{-1},x})^{-1} = y^{-1}_{Sbx^{-1},x}.$$

  - Supongamos $(\ )^{Sb}$ definido para todas las palabras de largo $\leq n$ y todas las clases $Sb \in S\backslash F$. Sea v una palabra reducida de largo nH,

    $$v = x^e u, \quad |u| = n, \quad \text{con } e = \pm 1.$$

    Así, $v^{Sb} = (x^e)^{Sb} u^{Sbx^e}$, y obtenemos la aplicación, para cada $Sb \in S\backslash F$

    $$(\cdot)^{Sb}\colon F \longrightarrow Y.$$

Propiedades de la exponencial $(\cdot)^{Sb}$

Proposición 5.22. *Sea F un grupo libre sobre X, Y un grupo libre sobre $\{y_{Sb,x}\}$, $S \leq F$.*

(1) Para todo $u, b \in F$ se tiene que

$$(uv)^{Sb} = u^{Sb} v^{Sbu}.$$

(2) Para todo $u \in F$

$$(u^{-1})^{Sb} = (u^{Sbu^{-1}})^{-1}.$$

(3) Si $\varphi\colon F \to S$ es el único homomorfismo tal que

$$\varphi(y_{Sb,x}) = t_{Sb,x},$$

entonces para todo $u \in F$ y para todo $Sb \in S\backslash F$,

$$\varphi(u^{Sb}) = l(Sb)ul(Sbu)^{-1}.$$

(4) Especialicemos $Sb \mapsto S$ y definamos

$$\begin{aligned}
\theta\colon S &\longrightarrow Y \\
u &\longmapsto \theta(u) = u^S,
\end{aligned}$$

entonces θ es un homomorfismo y se tiene $\varphi \circ \theta = \mathrm{id}_S$.

$$\begin{tikzcd} F \arrow[r, "(\cdot)^S"] & Y \\ S \arrow[u] \arrow[ur, "\theta"] & \end{tikzcd}$$

Demostración.

(1) La realizaremos por inducción sobre $|u|$. Primero, notemos que $|u| = 0$ si y solo si $u = 1$, entonces
$$(uv)^{Sb} = v^{Sb} = 1^{Sb} v^{Sb\cdot 1}.$$
Si $|u| \geq 1$, digamos $|u| = n$, sea $u = x^e w$, con $|w| < n$, $e = \pm 1$.
$$(uv)^{Sb} = (x^e)^{Sb}(wv)^{Sbx^e} = \left((x^e)^{Sb} w^{Sbx^e}\right) v^{Sbx^e w} = (x^e w)^{Sb} v^{Sbu} = u^{Sb} v^{Sbu}.$$

(2) La demostración de este literal se deja de ejercicio al lector.

(3) Al igual que antes, realizaremos la demostración por inducción sobre $|u|$.

Al igual que antes, $|u| = 0$ si y solo si $u = 1$, entonces
$$\varphi(1^{Sb}) = \varphi(1) = 1 = l(Sb) \cdot 1 \cdot l(Sb1)^{-1}.$$
Si $|u| \geq 1$, escribiremos $u = x^e v$, u una palabra reducida, entonces
$$\begin{aligned} \varphi(u^{Sb}) &= \varphi((x^e)^{Sb} v^{Sbx^e}) \\ &= \varphi\left((x^e)^{Sb}\right) \varphi(v^{Sbx^e}) \\ &= \varphi((x^e)^{Sb}) \\ &= l(Sbx^e) v l(Sbx^e v)^{-1}. \end{aligned}$$
Distinguimos dos casos:

- Si $e = +1$, entonces
$$\begin{aligned} \varphi(u^{Sb}) &= l(Sb)xl(Sbx)^{-1} l(Sbx) v l(Sbxv)^{-1} \\ &= l(Sb)xvl(Sbxv)^{-1} \\ &= l(Sb)ul(Sbu)^{-1}. \end{aligned}$$

- Si $e = -1$, entonces
$$\begin{aligned} \varphi(u^{Sb}) &= \varphi(y^{-1}_{Sbx^{-1},x}) l(Sbx^{-1}) v l(Sbx^{-1}v)^{-1} \\ &= (l(Sbx^{-1})xl(Sbx^{-1}x)^{-1})^{-1} l(Sbx^{-1}) v l(Sbx^{-1}v)^{-1} \\ &= l(Sb)x^{-1} l(Sbx^{-1})^{-1} l(Sbx^{-1}) v l(Sbx^{-1}v)^{-1} \\ &= l(Sb)x^{-1} v l(Sbx^{-1}v)^{-1} \\ &= l(Sb)ul(Sbu). \end{aligned}$$

(4) Sea $u \in S$, $\theta(u) = u^S$, $\theta\colon S \to Y$. Sean $u, v \in S$, entonces, como $Su = S$ pues $u \in S$,

$$\theta(uv) = (uv)^S = u^S v^{Su} = u^S v^S = \theta(u)\theta(v),$$

por ende θ es un homomorfismo.

Ahora,

$$\varphi(\theta(u)) = \varphi(u^S) = l(S \cdot 1)ul(S \cdot u)^{-1} = ul(Su)^{-1} = ul(S)^{-1} = u \cdot 1 = u,$$

así $\varphi \circ \theta = \mathrm{id}_S$.

□

Corolario 5.23. *Si $S \leq F$, con F un grupo libre, y l una transversal de S en F, entonces los elementos $t_{Sb,x} \neq 1$ generan a S.*

Demostración. Tenemos que $\varphi \circ \theta = \mathrm{id}_S$, lo que implica que $\varphi(\theta(u)) = u$. φ está definida sobre Y, que es el grupo libre con base $\{y_{Sb,x} \,|\, Sb \in S\backslash F, x \in X\}$, por ende, como φ es un epimorfismo, tenemos que $\varphi(y_{Sb,x}) = t_{Sb,x}$ genera a S. □

Proposición 5.24. $\ker(\varphi)$ *es le subgrupo normal de Y generado por los elementos $l(Sb)^S$.*

$Sb \in S\backslash F$. Sea N el grupo normal de Y generado por las $l(Sb)^S$, $K = \ker(\varphi)$. Y afirmamos que $K = N$.

Ejercicio 5.25. $K = \ker(\varphi)$ es el subgrupo normal de Y generado por los elementos $y^{-1}\rho(y)$, con $y \in Y$ y $\rho = \theta \circ \varphi$ (que verifica $\rho\rho = \rho$). Ahora, $S \cong Y/K \cong Y/N$, así obtenemos una representación de S

$$S = (y_{Sb,x}, x \in X, Sb \in S\backslash F \,|\, l(Sb)^S, Sb \in S\backslash F)$$

Demostración de la Proposición 5.24. Por la proposición anterior,

$$\begin{aligned} y_{Sb,x}^{-1}\rho(y_{Sb,x}) &= y_{Sb,x}^{-1}(l(Sb)xl(Sbx)^{-1})^S \\ &= y_{Sb,x}^{-1}l(Sb)^S x^{Sb}(l(Sbx)^{-1})^{Sbx} \\ &= (y_{Sb,x}^{-1}l(Sb)^S y_{Sb,x})(l(Sbx)^{-1})^{Sb,x}, \end{aligned}$$

en consecuencia

$$y_{Sb,x}^{-1}\rho(y_{Sb,x}) = (y_{Sb,x}^{-1}l(Sb)^S y_{Sb,x})(l(Sbx)^S)^{-1}. \tag{5.2}$$

Ahora, $y_{Sb,x}^{-1}l(Sb)^S y_{Sb,x} \in N$ y $(l(Sbx)^S)^{-1} \in N$, así

$$y_{Sb,x}^{-1}\rho(y_{Sb,x}) \in N,$$

de donde $K \leq N$.

Para demostrar que $K \geq N$, observemos que de (5.2)

$$l(Sb)^S \in K \iff l(Sbx)^S \in K,$$

y por inducción respecto a $|l(Sb)^S|$ se tiene que $l(Sb)^S \in K$ para todo $Sb \in S\backslash F$, y por ende $N \subseteq K$. □

5.2. Transversales de Schreier

Definición. Sean F un grupo libre con base X y $S \leq F$. Una transversal de Schreier es una transversal de S en F con la propiedad que si

$$l(Sb) = x_1^{e_1} \dots x_n^{e_n}, \qquad e_i = \pm 1, \quad \text{para todo } x_i \in X,$$

es reducida, entonces toda todo segmento inicial de la palabra $x_1^{e_1} \dots x_n^{e_n}$ (es decir, las palabras de la forma $x_1^{e_1} \dots x_k^{e_k}$, $k \leq n$) está en la transversal, es decir que existe $Sb_k \in S \backslash F$ tal que $l(Sb_k) = x_1^{e_1} \dots x_k^{e_k}$.

Proposición 5.26. *Las transversales de Schreier existen.*

Demostración. Para todo $Sb \in S\backslash F$ se define el largo de Sb:

$$|Sb| = \text{mín}\{|sb| \mid s \in S\}.$$

La proposición se demuestra por inducción respecto a $|Sb|$. Demostraremos que para todo $Sb \in S\backslash F$ existe un representante $l(Sb)$ tal que todos los segmentos iniciales son representantes de clases laterales de largo menor que Sb.

Definamos $l(S) = 1$ y supongamos que el resultado es válido para las clases Sb, con $|Sb| \leq n$. Sea Sz, con $z \in F$, una clase lateral con lago $|Sz| = n + 1$, entonces existe $ux^e \in Sz$, con $e = \pm 1$ y $|ux^e| = n + 1$. Observemos que $|u| = n$ y no $|u| < n$, pues si $|u| < n$ entonces $|ux^e| < n + 1$, se sigue que $|Su| = n$. Por hipótesis de inducción existe $b = l(Su)$ tal que todo segmento inicial de b es un representante de una clase lateral de largo menor o igual a n. Definamos

$$l(Sz) = bx^e,$$

los segmentos iniciales de bx^e son segmentos iniciales de b. □

Teorema 5.27 (Nielsen-Schreier)**.** *Todo subgrupo de un grupo libre es libre. Si l es una transversal de Schreier entonces S tiene base de elementos* $1 \neq t_{Sb,x} = l(Sb) \times l(Sbx)^{-1}$.

Demostración. Sean el conjunto de símbolos $\{Y_{Sb,x} \mid Sb \in S\backslash F, x \in X\}$ y Y el grupo libre generado por estos símbolos. Sea

$$\begin{aligned} \{Y_{Sb,x} \mid Sb \in S\backslash F, x \in X\} &\to S \\ Y_{Sb,x} &\mapsto t_{Sb,x}. \end{aligned}$$

Existe un homomorfismo $\varphi \colon Y \to S$ que extiende a esta aplicación y como $\varphi(Y_{Sb,x}) = t_{Sb,x}$, entonces φ es un epimorfismo. Se tiene un homomorfismo

$$\begin{aligned} \theta \colon S &\to Y \\ \theta(u) &= u^s \end{aligned}$$

tal que $\varphi \circ \theta = \text{id}_S$, por ende θ es un epimorfismo. Luego $t_{Sb,x}$ genera a S. Vamos a probar que $\{t_{Sb,x} \neq 1 \mid x \in X, Sb \in S\backslash F\}$ es base de S. Tenemos que

$$S \cong Y \backslash Ker(\varphi).$$

Sea $K = \ker(\varphi)$, queremos probar que K es el subgrupo normal de Y generado por $l(Sb)^s$, para ello, basta demostrar que $K = \ker \varphi$ es igual al subgrupo normal $T \trianglelefteq Y$ generado por los $Y_{Sb,x}$ tales que $\varphi(Y_{Sb,x}) = t_{Sb,x} = 1$, utilizando el siguiente ejercicio.

Ejercicio 5.28. Si F es un grupo libre con base X, $N \trianglelefteq$ es el subgrupo normal generado por $A \leq X$, entonces $F \backslash N$ es libre.

Es evidente que $T \subseteq K = \ker(\varphi)$ pues T está generado por $Y_{Sb,x}$, con $\varphi(Y_{Sb,x}) = 1$. Queda probar que $K \subset T$. La demostración se realiza por inducción respecto al largo $l(Su)$. A los símbolos $Y_{Sb,x}$ tales que $\varphi(Y_{Sb,x})$ los llamaremos *especiales*, de igual manera a las palabras. Demostraremos que $l(Sr)^s$ es especial.

Recordamos que K está generado por $l(Sb)^s$ y T es subgrupo normal de Y generado por las palabras especiales. Esto concluye la demostración. $\square$

Si $|l(Sr)| = 0$, entonces $l(Sr) = l(S) = 1$, y por lo tanto $l(Sr)^s = 1$ es especial. Supongamos que $|l(Sr)| \geq 1$, entonces

$$l(Sr) = ux^e, \qquad x \in X, \qquad e \pm 1$$

y $|u| < |l(Sr)|$. l es transversal de Schreier, u es segmento inicial de $l(Sv)$, y por lo tanto $u = l(Sr)$, por hipótesis de inducción, $u^s = l(Su)^s$ es especial, de donde $u^s \in T$. Queda probar que $(x^e)^{Su}$ es especial.

- Si $e = \pm 1$
$$(x^e)^{Su} = x^{Su} = Y_{Su,x},$$
pero $l(Sux) = ux$ pues $l(Sv) = ux$ y $Sv = Sux$, pues l es transversal. Luego
$$\varphi(Y_{Su,x}) = t_{Su,x} = l(Su) \times l(Sux)^{-1} = ux(ux)^{-1} = 1,$$
de donde $Y_{Su,x} = x^{su}$. Concluimos que $l(Sr)^s$ es especial.

- Si $e = -1$, entonces $l(Sr)^s = (ux^{-1})^s = u^s(x^{-1})^{Su}$, basta probar que $(x^{-1})^{Su}$ es especial. Se tiene que
$$(x^{-1})^{Su} = (x^{Sux^{-1}})^{-1} = (Y_{Sux^{-1},x})^{-1}.$$
Calculemos $\varphi((x^{-1})^{Su})$:
$$\begin{aligned}\varphi((x^{-1})^{Su}) &= \varphi(Y_{Sux^{-1},x})^{-1} = t^{-1}_{Sux^{-1},x} \\ &= (l(Sux^{-1})xl(Sux^{-1}x)^{-1})^{-1} \\ &= [l(Sux^{-1})xl(Su)^{-1}]^{-1}.\end{aligned}$$
Por elección de l (transversal de Schreier), $l(Su) = u$ y $l(Sux^{-1}) = ux^{-1}$. Así
$$\varphi((x^{-1})^{Su}) = [ux^{-1}xu^{-1}]^{-1} = 1,$$
como se deseaba probar.

Aplicación: Sean F es un grupo libre y $u, v \in F$, entonces $uv = vu$ conmutan existe $z \in F$ tal que $uv \in \langle z \rangle$.

Corolario 5.29. *Sea F un grupo libre de rango 2 (es decir $X = \{x, y\}$), entonces el subgrupo $F' = [F \colon F]$ tiene rango infinito.*

5.3. Productos libres

Definición. Sean P un grupo, $\{A_i, i \in I\}$ una familia de grupos y $\{j_i, i \in I\}$ una familia de homomorfismos $j_i\colon A_i \to P$. Diremos que P es un producto libre de los grupos A_i si se verifica la siguiente propiedad universal: Para todo grupo G y toda familia de homomorfismos $\{f_i, i \in I\}$, $f_i\colon A_i \to G$, existe un único homomorfismo $\varphi\colon P \to G$ tal que

$$\varphi \circ j_i = f_i, \qquad \forall i \in I,$$

es decir que

$$\begin{tikzcd} P \arrow[dr, dashed, "\varphi"] & \\ A_i \arrow[u, "j_i"] \arrow[r, "f_i"'] & G \end{tikzcd}$$

es un diagrama conmutativo.

Observación. Si P existe, los j_i son monomorfismos, para todo $i \in I$. Identificando A_i con $j_i(A_i)$, podemos suponer que $A_i \hookrightarrow P$.

En efecto, tomando en particular $G = A_i$, $f_i\colon A_i \to A_i$ como la identidad y $f_k\colon A_k \to A_i$ la función 1 si $h \neq i$. Si existe un homomorfismo $\varphi\colon P \to A_i$ tal que $\varphi \circ j_k = f_k$ para todo $k \in I$, de donde $\varphi \circ j_i = \mathrm{id}_{A_i}$ y por tanto j_i es inyectiva.

Ejemplo 5.30. Sean X un conjunto y F el grupo libre con base X. Para cada $x \in X$ tomamos $Ax = \langle x \rangle \leq F$. Definamos $j_x\colon A_x \to F$ el único homomorfismo inducido por la función

$$\begin{aligned} \{x\} &\to F \\ x &\mapsto x. \end{aligned}$$

Probaremos que F es el producto libre de los grupos A_x. En efecto, sean G un grupo arbitrario y $f_x\colon \langle x \rangle \to G$ un homomorfismo. Tomamos $f\colon X \to G$ una función cualquiera y φ el único homomorfismo que prolonga a f.

$$\begin{tikzcd} F \arrow[dr, dashed, "\varphi"] & \\ X \arrow[u, "j_x"] \arrow[r, "f"'] & G. \end{tikzcd}$$

Se tiene que $\varphi\colon F \to G$ satisface $\varphi \circ j_x = f_x$ para todo $x \in X$. Entonces

$$\begin{tikzcd} F \arrow[dr, dashed, "\varphi"] & \\ \langle x \rangle \arrow[u, "j_x"] \arrow[r, "f_x"'] & G. \end{tikzcd}$$

es un gráfico que conmuta y por tanto F es producto libre de los $\langle x \rangle$.

Sean $\{A_i\colon i \in I\}$ una familia de grupos y sean P, Q productos libres de esta familia, con los homomorfismos

$$j_i\colon A_i \to P, \qquad k_i\colon A_i \to Q.$$

Como P es producto libre, existe $\varphi\colon P \to Q$ tal que $\varphi \circ j_i = k_i$, y recíprocamente, existe $\psi\colon Q \to P$ un homomorfismo, tal que $\psi \circ k_i = j_i$.

Ejercicio 5.31. Probar que $\psi \circ \varphi = \mathrm{id}_Q$ y $\psi \circ \varphi = \mathrm{id}_P$.

Proposición 5.32. *Si el producto directo existe, es único salvo isomorfismo.*

Teorema 5.33. *Sea* $(A_i)_{i\in I}$ *una familia de grupos, entonces existe el producto libre de los* A_i *que se denota por* $\underset{i\in I}{\star} A_i$

Ejemplo 5.34. Si F es un grupo libre en X, $\{\langle x\rangle \mid x\in X\}$, entonces $F(X) = \underset{x\in X}{\star}\langle x\rangle$.

Sea $A_i^* = A_i\backslash\{1\}$ y supongamos que $A_i^*\cap A_j^* = \emptyset$, $i\neq j$. Llamemos al conjunto $(\bigcup\limits_{i\in I} A_i^*)\cup\{1\}$ un alfabeto:

Las palabras en este alfabeto son de la forma

$$w = a_1a_2\ldots a_n,$$

donde $a_i\in A_j^*$, para algún $j\in I$. w es reducido si a_i, a_{i+1} no están en el mismo A_j, $j\in I$, y $w=1$ también es reducida. Sea P el conjunto de todas las palabras reducidas en este alfabeto. Definimos el producto en P por *yuxtaposición*:

Sean $w = a_1\ldots a_n$ y $v = b_1\ldots b_m$ son elementos de P.

(1) Si a_n y b_1 no están en el mismo A_j^*, entonces

$$wv = a_1\ldots a_nb_1\ldots b_m$$

es reducida ($wv\in P$).

(2) Si $a_n, b_1\in A_i^*$, $a_nb_1\neq 1$. Definimos

$$wv = a_1\ldots a_{n-1}(a_nb_1)b_2\ldots b_m$$

y wv es reducida.

(3) Si $a_n, b_1\in A_i^*$, $a_nb_1 = 1$. Definimos

$$wv = a_1\ldots a_{n-1}a_{n-1}b_2\ldots b_m$$

y se repite recurrentemente.

Ejercicio 5.35. $(P,\cdot)$ es un grupo que contiene a los A_i,

$$\begin{aligned} A_i &\to P \\ a &\mapsto a \end{aligned}$$

es reducida.