Grupos libres

Sésar

1. Definición

Definition 1. Sea A un conjunto. Decimos que F_A es un **grupo libre** (con **base** A) si existe una aplicación $\imath : A \to F_A$ tal que se cumple la siguiente propiedad universal:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\imath"'] & G \\ F_A \arrow[ur, dashed, "\Phi"'] & \end{tikzcd}$$

Para toda aplicación $\varphi : A \to G$, existe un único homomorfismo $\Phi : F_A \to G$ tal que $\varphi = \Phi \circ \imath$.

Remark 1. La aplicación $\imath : A \to F_A$ es una inyección. Sea $x, y \in A$ tal que $\imath(x) = \imath(y)$. Sea $G = C_2$ y la aplicación $\varphi : A \to C_2$ definida como $\varphi(x) = e$ y $\varphi(z) = a$ para todo $z \neq x$. En este caso, por la definición de grupo libre, $\varphi(x) = \Phi(\imath(x)) = \Phi(\imath(y)) = \varphi(y)$. Como $\varphi(y) = \varphi(x) = e$, entonces por definición de φ, $x = y$.

Theorem 1 (Unicidad)**.** Sean A, B conjuntos. $F_A \cong F_B$ si y solo si $|A| = |B|$.

Demostración. En primer lugar, supongamos que $|A| = |B|$. Luego existe una biyección $f : A \to B$. tomando $G = F_B$ y $\varphi = \jmath \circ f : A \to F_B$, tenemos que por definición existe un homomorfismo $\Phi : F_A \to F_B$ tal que $\jmath \circ f = \Phi \circ \imath$. Por otro lado, tomando $G = F_B$, y $\psi = \imath \circ f^{-1} : B \to F_A$, entonces existe un homomorfismo $\Psi : F_B \to F_A$ tal que $\imath \circ f^{-1} = \Psi \circ \jmath$. Combinando las dos ecuaciones, llegamos a que $\Psi \circ \Phi \circ \imath = \Psi \circ \jmath \circ f = \imath \circ f^{-1} \circ f = \imath$. De este modo, como $\imath$ es inyectiva —un monomorfismo—, entonces $\Psi \circ \Phi = \mathrm{id}_{F_A}$. De la misma manera, llegamos a la conclusión de que $\Phi \circ \Psi = \mathrm{id}_{F_B}$, obteniendo entonces que Φ es un isomorfismo con $\Phi^{-1} = \Psi$.

Supongamos ahora que existe un isomorfismo $\Theta : F_A \to F_B$. Denotemos $V_A = \mathrm{Hom}(F_A, \mathbb{F}_2)$ y $V_B = \mathrm{Hom}(F_B, \mathbb{F}_2)$ los espacios vectoriales sobre el cuerpo $\mathbb{F}_2$ formado por dos elementos. En primer lugar, $V_B \cong V_A$ como espacios vectoriales mediante el isomorfismo $f \mapsto f \circ \Theta$. Por tanto, sus bases tienen la misma cardinalidad. Una base de V_A puede ser definida como el conjunto de funciones $f_a : F_A \to \mathbb{F}_2$ tal que $f_a(a) = 1$ y $f_a(x) = 0$ para todo $x \neq a \in A$. De este modo, $\dim(V_A) = |A|$ y de la misma manera, $\dim(V_B) = |B|$. Por la isomorfía de los espacios vectoriales, las dimensiones coinciden por lo que $|A| = |B|$. $\square$

Definition 2. El **rango** de grupo libre F_A es

$$\mathrm{rank}(F_A) = |A|.$$

Decimos que F_A está **finitamente generado** si $\mathrm{rank}(F_A) < \infty$.

Remark 2. Por tanto, todos los grupos libres del mismo rango son isomorfos, por lo que podemos denotar el grupo libre como F_n, donde n es el rango del grupo libre.

Theorem 2 (Nielsen-Schreier)**.** Todo subgrupo de un grupo libre es libre.

Theorem 3. Todo grupo es cociente de un grupo libre. En particular,

$$F_X / \ker \Phi \cong G$$

donde $X \subseteq G$ es un generador de X.

Demostración. Notemos que G siempre tiene un conjunto generador porque podemos tomar a lo sumo $X = G$. La aplicación $\varphi : X \to G$ es la inyección y por la definición del grupo libre en X, existe un homomorfismo $\Phi : F_X \to G$ tal que $\varphi = \Phi \circ \imath$. En primer lugar, notemos que Φ es sobreyectiva, puesto que todo elemento de G está expresada como producto de sus generadores. Finalmente, por le primer teorema de isomorfía, se tiene que $F_X / \ker \Phi \cong G$. □

2. Construcción de grupos libres

Definition 3. Sea X un conjunto. Una **palabra** en X es una secuencia finita de $x_i \in X$:

$$w = x_1 \dots x_n,$$

donde $x_i \in X$. Definimos la **longitud** de la palabra como $|w| := n$.

Denotamos como $W(X)$ al conjunto de palabras en X. Por otro lado, decimos que dos palabras son iguales si la palabras están formadas por la misma concatenación de elementos en el mismo orden —es decir, son iguales componente a componente—.

Remark 3. Una secuencia ε que no tenga ningún elemento puede considerarse como una palabra llamada **vacía** y es la única palabra con longitud $|\varepsilon| = 0$.

Para cada X, tomemos un conjunto X^{-1} biyectivo y disjunto a X de tal manera que $x \mapsto x^{-1}$ es una biyección. En particular, podemos considerar el conjunto $\overline{X} := X \sqcup X^{-1} \sqcup \{\varepsilon\}$ y definir palabras en este conjunto. De manera general, podemos definir una función «inversa» en $\overline{X}$ como sigue: si $y \in \overline{X}$, entonces

$$y^{-1} := \begin{cases} x^{-1} & \text{si } y = x \in X \\ x & \text{si } y = x^{-1} \in X^{-1} \end{cases}$$

En particular, tenemos que $(x^{-1})^{-1} = x$ para todo $x^{-1} \in X^{-1}$.

Definition 4. Una **reducción** de una palabra $w \in W(\overline{X})$ consiste en la eliminación de una subpalabra de la forma yy^{-1}.

Remark 4. Denotamos las reducciones como $wyy^{-1}w' \to ww'$.

Si una palabra w contiene una subpalabra yy^{-1}, entonces podemos aplicar una reducción $w \to w_1$. Por otro lado, si w_1 también tiene una subpalabra con tales características, podemos aplicar una segunda reducción $w \to w_1 \to w_2$.

Definition 5. Una palabra $w \in W(\overline{X})$ es **reducida** si $w \to w' \Rightarrow w = w'$.

Esta definición implica que no puede aplicarse ninguna reducción en la palabra w, luego equivalentemente no posee ninguna subpalabra con la forma yy^{-1}.

Lemma 1. Sea $w \in W(\overline{X})$. Si $w \to w_1$ y $w \to w_2$, entonces existe un $w' \in W(\overline{X})$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} w \arrow[r] \arrow[d] & w_1 \arrow[d, dashed] \\ w_2 \arrow[r, dashed] & w' \end{tikzcd}$$

Demostración. Supongamos primero que puedo expresar w como $w = u_1yy^{-1}u_2xx^{-1}u_3$, donde $w_1 = u_1u_2xx^{-1}u_3$ y $w_2 = u_1yy^{-1}u_2u_3$. De este modo, $w' = u_1u_2u_3$ y podemos definir de manera natural las reducciones $w_1 \to w'$ y $w_2 \to w'$ de tal manera que es fácil comprobable la conmutatividad del diagrama.

Por otro lado, si $w = u_1yy^{-1}yu_2$, entonces las reducciones resultantes son para w_1 la eliminación de yy^{-1} y para w_2 la eliminación de $y^{-1}y$. Ambas reducciones nos dan como resultado que $w_1 = w_2$. Luego basta tomar $w' = w_1 = w_2$. $\square$

Definition 6. Sean $w, u \in W(\overline{X})$. Decimos que w es **confluente** con u si existe una cadena de reducciones finita:

$$w = w_0 \to w_1 \to \ldots \to w_n = u.$$

Denotamos la confluencia como $w \overset{*}{\to} u$.

Theorem 4. Toda palabra tiene una palabra reducida confluente.