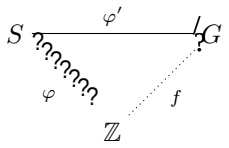
Tema 4.- Grupos libres. Presentaciones.

4.1 Grupos libres.

En el grupo $\mathbb{Z}$ de los enteros vimos una propiedad (cf. ejemplo 2.2.3, 5) que lo caracteriza como grupo libre. Lo enunciamos al modo de una Propiedad Universal en la siguiente proposición.

Sea $S = \{a\}$ un conjunto con un único elemento, y $\varphi : S \to \mathbb{Z}$ la aplicación (necesariamente inyectiva) dada por $\varphi(a) = 1$.

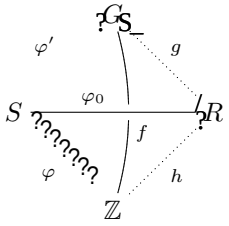
PROPOSICIÓN 4.1.1.– Para cada grupo G y para cada aplicación $\varphi' : S \to G$, se tiene que φ' se factoriza a través de φ, es decir, existe un único homomorfismo $f : \mathbb{Z} \to G$ tal que el siguiente diagrama



conmuta, es decir, $f\varphi = \varphi'$.

Esta propiedad universal caracteriza al grupo $\mathbb{Z}$:

COROLARIO 4.1.2.– Sea R un grupo, $\varphi_0 : S = \{a\} \to R$ una aplicación, verificando la propiedad universal de $\mathbb{Z}$, es decir, para cada grupo G y para cada aplicación $\varphi' : S \to G$, se tiene que φ' se factoriza, de modo único, a través de φ_0, i.e $\varphi' = g\varphi_0$. Entonces existe un isomorfismo $h : \mathbb{Z} \to R$ tal que los siguientes diagramas



conmutan, es decir, $h\varphi = \varphi_0$ y $f = gh$.

PRUEBA: Primero se aplica la proposición a φ_0 y R, obteniéndose un homomorfismo $h : \mathbb{Z} \to R$. Ahora se aplica la hipótesis a φ y $\mathbb{Z}$, obteniéndose un homomorfismo $h' : R \to \mathbb{Z}$. Se aplica de nuevo la proposición a φ y $\mathbb{Z}$, viendo que $h'h$ y la identidad en $\mathbb{Z}$ hacen el correspondiente diagrama conmutativo, y por la unicidad, son iguales. Análogamente, usando la hipótesis, se prueba que hh' es la identidad en R. Por tanto h es un isomorfismo. □

Vamos a generalizar los resultados anteriores para un conjunto cualquiera S.

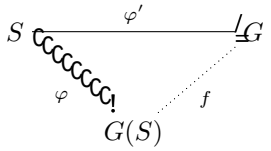
DEFINICIÓN 4.1.3.– Diremos que un subconjunto S de un grupo H es una *base* si la inclusión $\varphi : S \to H$ verifica la propiedad universal anterior. Un grupo H que posea una base se dirá que es un *grupo libre*.

EJEMPLO 4.1.4.–

1. Los subconjuntos $\{1\}$, $\{-1\}$ son las únicas bases del grupo $\mathbb{Z}$.

2. Ningún grupo cíclico finito es libre.

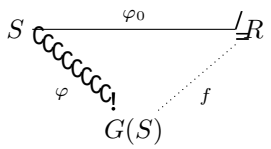
TEOREMA 4.1.5.– Sea S un conjunto cualquiera. Existe un grupo $G(S)$ y una aplicación $\varphi : S \to G(S)$ inyectiva tal que: para cada grupo G y para cada aplicación $\varphi' : S \to G$, se tiene que φ' se factoriza a través de φ, es decir, existe un único homomorfismo $f : G(S) \to G$ tal que el siguiente diagrama



conmuta, es decir, $f\varphi = \varphi'$.

Antes de demostrar el teorema, veremos que la propiedad enunciada caracteriza al grupo $G(S)$, al que llamaremos *grupo libre* engendrado por S, sobrentendiéndose la 'inclusión' $\varphi : S \to G(S)$. A este teorema se le califica normalmente como la Propiedad Universal de los Grupos Libres. Nótese que esta propiedad tiene una formulación análoga a la propiedad (universal) siguiente de los espacios vectoriales : para dar un homomorfismo f de espacios vectoriales que parta de V, basta dar la imagen por f de un sistema S de generadores de V.

COROLARIO 4.1.6.– Sea R un grupo, $\varphi_0 : S \to R$ inyectiva, verificando la propiedad universal de $G(S)$. Entonces existe un isomorfismo $f : G(S) \to R$ tal que el siguiente diagrama



conmuta, es decir, $f\varphi = \varphi_0$.

La demostración del corolario es análoga a la del corolario anterior.

PRUEBA: (DEL TEOREMA) Construiremos $G(S)$ en dos pasos.

1) Sea S' un nuevo conjunto equipotente con S, es decir, para cada elemento $a \in S$ hay asociado un elemento $a' \in S'$. Con el *alfabeto* formado por los elementos o *letras* de $S \cup S'$, formamos el conjunto $P(S)$ de todas las *palabras* (finitas) construidas adjuntando letras del alfabeto. En el conjunto $P(S)$ hay

una operación binaria $*$ consistente en adjuntar palabras. La palabra *vacía* sería elemento neutro de la operación $*$, que es obviamente asociativa. Pero $P(S)$ todavía no es grupo, por la ausencia de elementos simétricos. Para lograrlo, definimos una transformación *reducción* $\rho : P(S) \to P(S)$, consistente en hacer recurrentemente, mientras sea posible, la siguiente sustitución: dada una palabra p, en la primera ocurrencia de una pareja aa' o $a'a$ en p, para $a \in S$, $a' \in S'$, se elimina en p cualquiera de estas parejas.

2) Construimos $G(S) = \mathrm{Im}(\rho)$, que llamamos conjunto de palabras *reducidas*. Definimos una operación binaria en $G(S)$, de la siguiente manera: si $p, q \in G(S)$, $p \cdot q = \rho(p * q)$. Se tiene fácilmente que el vacío es también el elemento neutro de esta operación. Los elementos inversos de los de S son los de S', y recíprocamente. En general, el elemento inverso de una palabra reducida se construye cambiando cada letra de S (resp. S') por la correspondiente en S' (resp. S), y después cambiando el orden de la palabra. No es nada fácil probar la propiedad asociativa, por lo que no entraremos en los detalles (cf. 'Introducción al Álgebra' de Xambó-Delgado-Fuertes, por ejemplo). Por tanto $G(S)$ es un grupo con la operación $\cdot$ dada.

Queda ver que $G(S)$ con la inclusión de S verifica las condiciones del teorema. Como $\langle S \rangle = \{x_1 \cdots x_r \mid x_i \in S \cup S^{-1}\}$ y $S^{-1} = S'$, se tiene que $G(S) = \langle S \rangle$. Por tanto, para definir un homomorfismo $f : G(S) \to G$, basta dar la imagen de los elementos del sistema generador S. Para que el diagrama enunciado conmute, debe ser $f(a) = \varphi'(a)$ para cada $a \in S$; de ahí la unicidad de f. □

Un resultado no trivial es que todo subgrupo de un grupo libre es libre. Es decir, si H es un subgrupo de $G(S)$, entonces H es isomorfo a un grupo libre $G(T)$, para un cierto conjunto T.

4.2 Relaciones.

Una consecuencia directa de la propiedad universal de los grupos libres es la siguiente

PROPOSICIÓN 4.2.1.– Todo grupo es cociente de uno libre. PRUEBA: Dado un grupo G, sea S un sistema de generadores de G. Aplicando el teorema a la inclusión de S en G, se tiene un epimorfismo $f : G(S) \to G$. Se aplica ahora el primer teorema de isomorfía y se obtiene lo deseado. □

A los elementos de $\ker(f)$ se les llama *relaciones* de S en G. Muchas veces una relación $u \in \ker(f)$ la escribiremos $u = e$, por abuso de lenguaje.

DEFINICIÓN 4.2.2.– Sea $R \subset G$ un subconjunto de un grupo. Notamos $N(R)$ a la intersección de todos los subgrupos normales de G que contienen a R, que es el menor subgrupo normal de G que contiene a R.

EJEMPLO 4.2.3.– Si G es un grupo cíclico, $G = \langle a \rangle$, de orden infinito, entonces G es isomorfo al grupo libre $\mathbb{Z}$, mediante el isomorfismo $f : \mathbb{Z} \to G$ dado por $f(n) = a^n$ (cf. ejemplo 2.2.3, 5. Si G es de orden finito n, entonces el

epimorfismo anterior tiene como núcleo $\ker(f) = \mathbb{Z}n$, y por el primer teorema de isomorfía $G \cong \mathbb{Z}/\mathbb{Z}n$.

EJEMPLO 4.2.4.– Sea $G = C_2 \times C_2 = \{(1,1),(1,-1),(-1,1),(-1,-1)\}$; si notamos a sus elementos por $1, \alpha, \beta, \gamma$ respectivamente, se tiene $\alpha^2 = \beta^2 = \gamma^2 = 1$, $\alpha\beta = \beta\alpha = \gamma$, $\alpha\gamma = \gamma\alpha = \beta$, $\beta\gamma = \gamma\beta = \alpha$. Como $G = \langle \alpha, \beta \rangle$, sean $S = \{a, b\}$ y $S' = \{a', b'\}$, entonces $G(S)$ es el conjunto de palabras reducidas en el alfabeto $\{a, b, a', b'\}$, y el epimorfismo $f : G(S) \to G$ está definido por $f(a) = \alpha$, $f(b) = \beta$. Está claro que $H = N(a^2, b^2, (ab)^2) \subset \ker(f)$. Por el lema previo al primer teorema de isomorfía, se tiene que f induce un epimorfismo $f' : G(S)/H \to G$. Por otra parte $a^2H = H$, luego $aH = a^{-1}H$. De $ababH = H$ se deduce que $abH = baH$. Por tanto, un elemento genérico de $G(S)/H$, será $a^{m_1}b^{n_1} \cdots a^{m_r}b^{n_r}H = a^{m_1+\cdots+m_r}b^{n_1+\cdots+n_r}H$. Queda así que $G(S)/H \subset \{H, aH, bH, abH\}$. Contando elementos, se deduce que $G(S)/H = \{H, aH, bH, abH\} \cong G$, y por tanto $H = \ker(f)$.

EJEMPLO 4.2.5.– Sea $G = S_3$. Un argumento análogo al anterior prueba que $G \cong G(S)/H$ con $S = \{a, b\}$ y $H = \langle a^3, b^2, (ab)^2 \rangle$.

EJEMPLO 4.2.6.– Sea G el grupo de simetría del cuadrado. Análogamente se tiene que $G \cong G(S)/H$ con $S = \{a, b\}$ y $H = \langle a^4, b^2, (ab)^2 \rangle$.

EJEMPLO 4.2.7.– Sea G el grupo aditivo y abeliano $\mathbb{Z}^2$, generado por $\sigma = (1, 0)$ y $\tau = (0, 1)$. Se prueba fácilmente que $G(S)/H \cong G$ con $S = \{s, t\}$ y $H = \langle sts^{-1}t^{-1} \rangle$, mediante el isomorfismo f', dado por $f'(s^m t^n H) = (m, n)$. Nótese quef' se puede construir con la propiedad universal de G(S).

En los ejemplos anteriores hemos visto que, dado un grupo G, podemos encontrar un conjunto S y un subgrupo normal N tales que $G \cong G(S)/N$; pero podemos trabajar también a la inversa.

DEFINICIÓN 4.2.8.– Sea S un conjunto y $R \subset G(S)$ un subconjunto. Diremos que $G(S, R) = G(S)/N(R)$ es el grupo definido por el conjunto de *generadores* S y las *relaciones* R. Más generalmente, si G es un grupo y existe un isomorfismo f de $G(S, R)$ sobre G, diremos que (S, R, f) es una *presentación* de G.

EJEMPLO 4.2.9.– Un grupo dado por un único generador s y la única relación s^n, con $n \in \mathbb{Z}_+$, es cíclico de orden n. En efecto, $G(S) = \langle s \rangle = \{s^m, m \in \mathbb{Z}\}$ que es abeliano, $N(R) = \langle s^n \rangle$. Entonces $G(S, R) \cong \mathbb{Z}/\mathbb{Z}n$.

EJEMPLO 4.2.10.– Sea $S = \{x, y\}$, $R = \{y^2x = y, yx^2y = x\}$. Por tanto $\{yx, yx^2yx^{-1}\} \in N(R)$, de donde $xyx^{-1} = (yx)^{-1}(yx^2yx^{-1}) \in N(R)$, y de aquí $y \in N(R)$. Por tanto $x = y^{-1}(yx) \in N(R)$, por lo que $N(R) = G(S)$ y $G(S, R)$ es trivial.

El problema de decidir si dos palabras de $G(S, R)$ son iguales es trivial si $R = \emptyset$, y está resuelto si R se reduce a un único elemento. Sin embargo, se puede demostrar que no puede existir ningún algoritmo para decidirlo, en forma universal. Este problema se conoce con el nombre de *problema de la palabra*.

Del mismo modo, dados dos grupos $G(S, R)$ y $G(S', R')$, no es posible encontrar un algoritmo general que decida si son o no isomorfos, ni siquiera cuando $G(S, R)$ es trivial y $G(S', R')$ es finitamente generado.

4.3 Grupo derivado.

Sea G un grupo.

DEFINICIÓN 4.3.1.– Si $x, y \in G$, pondremos $[x, y]$ para denotar el *conmutador* de x e y, es decir $[x, y] = xyx^{-1}y^{-1}$. Al subgrupo generado por el conjunto de conmutadores de G será denotado por G' o por $[G, G]$ y se llamará *grupo derivado* de G.

PROPOSICIÓN 4.3.2.– Sea G un grupo y G' su grupo derivado.

1. $G' \lhd G$.
2. G es abeliano si y sólo si $G' = \{1\}$.

La demostración es inmediata.

PROPOSICIÓN 4.3.3.– Sea $f : G_1 \to G_2$ un homomorfismo (resp. epimorfismo).

1. $f(G_1') \subset G_2'$ (resp. $f(G_1') = G_2'$).
2. Si f es epimorfismo, entonces G_2 es abeliano si y sólo si $G_1' \subset \ker(f)$.

COROLARIO 4.3.4.– Si $N \lhd G$, entonces G/N es abeliano si y sólo si $G' \subset N$.

DEFINICIÓN 4.3.5.– Dado un grupo G, al grupo cociente G/G' lo llamaremos *abelianizado* de G y lo notaremos G^{ab}. Dicho grupo siempre viene acompañado de la proyección canónica $\pi : G \to G^{ab}$.

PROPOSICIÓN 4.3.6.– *(Propiedad universal del abelianizado)* Para cada grupo G y cada homomorfismo de grupos $f : G \to H$ donde H es un grupo abeliano, existe un único homomorfismo de grupos $g : G^{ab} \to H$ tal que $f = g \circ \pi$.

EJEMPLO 4.3.7.–

1. Si D_4 es el grupo de simetría del cuadrado, $D_4' = \{1, g^2\}$, donde g es el giro de 90^0.
2. Si S_n es el grupo de permutaciones de n elementos, $S_n' = A_n$. Para ello se debe comprobar que, para i, j, k distintos, $[(ij), (ik)] = (ijk)$. Además se debe comprobar que A_n está generado por $\{(123), \ldots, (12n)\}$