Universidad Nacional Autónoma de México

Facultad de Ciencias

Grupos y Módulos Libres

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICA

PRESENTA:
XÓCHITL JUDITH VÁZQUEZ ESTRADA

DIRECTORA DE TESIS:
DANIELA MARIYET TERÁN GUERRERO

2014

1.Datos del alumno

Apellido paterno	Vázquez
Apellido materno	Estrada
Nombre(s)	Xóchitl Judith
Teléfono	62724963
Universidad	Universidad Nacional Autónoma de México
Facultad o escuela	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	408065528

2. Datos del tutor

Grado	Mat.
Nombre(s)	Daniela Mariyet
Apellido paterno	Terán
Apellido materno	Guerrero

3. Datos del sinodal 1

Grado	Dra.
Nombre(s)	Bertha María
Apellido paterno	Tomé
Apellido materno	Arreola

4. Datos del sinodal 2

Grado	Dra.
Nombre(s)	Diana
Apellido paterno	Avella
Apellido materno	Alaminos

5. Datos del sinodal 3

Grado	Dr.
Nombre(s)	Alejandro
Apellido paterno	Alvarado
Apellido materno	García

6. Datos del sinodal 4

Grado	M. en C.
Nombre(s)	José Cruz
Apellido paterno	García
Apellido materno	Zagal

7.Datos del trabajo escrito.

Título	Grupos y Módulos Libres
Número de páginas	99 p.
Año	2014

A mi madre, abuela y hermanos...

Aprovecho este espacio para agradecer a Dios por darme la oportunidad de estar aquí. A mi madre Estela quien siempre está pendiente de mi, ella que siempre me impulsa para seguir avanzando. A mi abuelita Gloria quien me consiente y me apoya. A mi hermano Omar que es quien guía mi camino desde que somos niños. A mi hermano Alejandro quien me enseña a luchar por lo que quiero en cada momento de mi vida. A mis amigos Eric, Alejandra, Edmundo por estar a mi lado en la Facultad durante largo tiempo. Agradezco a Daniela mi tutora quien tuvo paciencia durante todo este período y también a todos mis sinodales que se preocuparón de este trabajo. Y a todos aquellos que me brindaron de su ayuda, amistad y tiempo. Tío Chuy te fuiste, pero igual gracias.

Índice general

Introducción

En este trabajo se presentarán 3 objetos categóricos en dos categorías de interés, la de grupos y la de R-módulos. Esto se hará por medio de tres capítulos, el primero donde se introducen las categorías y se explican lo que son y cómo funcionan de manera general los objetos que queremos mostrar: **productos, coproductos y objetos libres**.

Una vez que se dan las nociones de estos tres objetos, se presentan en dos capítulos más la obtención y manejo de los objetos descritos en la categoría **GRP** de los grupos y en la categoría ${}_R\mathbf{MOD}$ de los R-módulos.

En el capítulo 2, destinado a los grupos se omiten las nociones básicas y el trabajo se concentra en la construcción de los objetos libres y su coproducto.

El capítulo 3 relativo a R-módulos presenta conceptos básicos así como la construcción de productos y coproductos entre dos R-módulos para poder generalizarlos a familias arbitrarias. Se presentan los módulos libres como una generalización de los grupos libres pero con una estructura mayor (se le dota de una operación más).

En los tres capítulos se dan ejemplos trabajados de manera minuciosa para que el lector se familiarice con estos conceptos.

Capítulo 1

Categorías

En este capítulo trataremos de dar una breve introducción a la teoría de categorías o al menos, lo que se usará en el resto del documento. Es decir, daremos definiciones, el principio de dualización, la noción de objeto, producto y coproducto en categorías y algunos resultados relacionados con estos últimos en la categoría de los grupos (**GRP**) y la categoría de los módulos (**MOD**).

1.1. Conceptos básicos

Las categorías nos proveen de un lenguaje y un contexto general que relaciona o que comparten numerosos problemas de distintas áreas de las matemáticas. La idea intuitiva que subyace a la definición de categoría es que la mayoría de los objetos matemáticos que ya conocemos como conjuntos, grupos, anillos (junto con un conjunto de *flechas* que serán funciones entre conjuntos, homomorfismos de grupos, homomorfismos de anillos, respectivamente) tienen numerosas propiedades comunes.

Definición 1.1.1. Una **categoría** es una cuarteta $\mathcal{C} = (\mathcal{OB}, hom, id, \circ)$ que consiste de:

1. Una clase de objetos, cuyos miembros son llamados $\mathcal{C}$-objetos y son denotados por $\mathcal{OB}_{\mathcal{C}}$.

2. Para cada par (A, B) de $\mathcal{C}$-objetos, un conjunto $Hom(A, B)$, cuyos elementos son llamados $\mathcal{C}$-morfismos de A en B que son también conocidos

como el conjunto de flechas de A en B. (Notación: Cada $\mathcal{C}$-morfismo de A en B se denotará por $f : A \longrightarrow B$ ó $A \xrightarrow{f} B$)

3. Para cada $\mathcal{C}$-objeto A , un morfismo $A \xrightarrow{id_A} A$, llamado A-identidad en $\mathcal{C}$.

4. Una composición denotada por $\circ$ que asocia a cada par de $\mathcal{C}$-morfismos $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ un $\mathcal{C}$-morfismo $A \xrightarrow{g \circ f} C$, llamado la *composición* de f y g, que cumple con:

   a) La $\circ$ es asociativa es decir, dados los morfismos $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ y $C \xrightarrow{h} D$ se cumple $h \circ (g \circ f) = (h \circ g) \circ f$,

   b) $\mathcal{C}$-identidad actúa como identidad con respecto a la composición; es decir, para $\mathcal{C}$-morfismos $A \xrightarrow{f} B$, se tiene que $id_B \circ f = f$ y $f \circ id_A = f$,

   c) Los conjuntos $Hom(A, B)$ son ajenos dos a dos.

Es conveniente, antes de seguir, mostrar ejemplos de categorías debido a su importancia y uso.

Ejemplo 1.1.2.

1. La categoría de conjuntos denotada por **SET** se compone de:

   a. La clase de objetos $\mathcal{OB}_{\mathbf{SET}}$ son los conjuntos.

   b. Si $A, B \in \mathcal{OB}_{\mathbf{SET}}$ es decir si A y B son conjuntos, entonces $Hom(A, B) = \{f : A \to B | f \text{ es función}\}$.

   c. Si $A \in \mathcal{OB}_{\mathbf{SET}}$ entonces la función identidad es el morfismo A-identidad en **SET**

   d. La composición de **SET**-morfismos es la composición de funciones.

2. La categoría de espacios vectoriales sobre un campo F denotada por **VEC** se compone de:

   a. La clase de objetos $\mathcal{OB}_{\mathbf{VEC}}$ son los F-espacios vectoriales.

   b. Si $V, W \in \mathcal{OB}_{\mathbf{VEC}}$ es decir si V y W son F-espacios vectoriales, entonces $Hom(V, W) = \{T : V \to W | T \text{ es transformación lineal}\}$.

c. Si $V \in \mathcal{OB}_{\mathbf{VEC}}$ entonces la transformación lineal identidad es el morfismo V-identidad en **VEC**

d. La composición de **VEC**-morfismos es la composición de transformaciones lineales.

3. La categoría de grupos denotada por **GRP** se compone de:

a. La clase de objetos $\mathcal{OB}_{\mathbf{GRP}}$ son los grupos.

b. Si $G, H \in \mathcal{OB}_{\mathbf{GRP}}$ es decir si G y H son grupos, entonces $Hom(G, H) = \{f : G \to H | f$ es homomorfismo de grupos$\}$.

c. Si $G \in \mathcal{OB}_{\mathbf{GRP}}$ entonces el homomorfismo identidad es el morfismo G-identidad en **GRP**

d. La composición de **GRP**-morfismos es la composición de homomorfismos de grupos.

4. La categoría de los conjuntos parcialmente ordenados **POS** se compone de:

a. La clase de objetos $\mathcal{OB}_{\mathbf{POS}}$ son los conjuntos parcialmente ordenados.

b. Si $A, B \in \mathcal{OB}_{\mathbf{POS}}$ es decir si A y B son conjuntos parcialmente ordenados, entonces $Hom(A, B) = \{f : A \to B | f$ es función monótona$\}$.

c. Si $A \in \mathcal{OB}_{\mathbf{POS}}$ entonces la función identidad es el morfismo A-identidad en **POS**

d. La composición de **POS**-morfismos es la composición de funciones monótonas.

Así como generalizamos muchas de las nociones que tenemos de ciertas estructuras y ciertas propiedades matemáticas, es importante dar una interpretación adecuada del concepto *isomorfismo* en el lenguaje categórico.

Definición 1.1.3. Un morfismo $f : A \longrightarrow B$ en una categoría $\mathcal{C}$ es una **equivalencia** (o **isomorfismo**) si existe un morfismo $g : B \longrightarrow A$ en $\mathcal{C}$ tal que

$$g \circ f = id_A \text{ y } f \circ g = id_B.$$

Este morfismo g es llamado **inverso** de f.

Sobre esta definición es fácil dar como ejemplo los morfismos identidad en cualquier categoría $\mathcal{C}$. De los ejemplos 1.1.2, en la categoría **SET** las equivalencias resultan ser las *funciones biyectivas* que son precisamente las únicas con inverso (el concepto de inverso se usa como inverso bilateral, de otra manera se detallará si es inverso izquierdo o inverso derecho); en el caso de que la categoría de la que se habla sea **VEC** entonces las equivalencias resultan ser las transformaciones lineales biyectivas que también son conocidas como *isomorfismos lineales*; si la categoría que estamos viendo es **GRP** entonces las equivalencias resultan ser los *isomorfismos de grupos* y por último en el caso en el que la categoría estudiada sea **POS** entonces las equivalencias resultan ser las *funciones biyectivas monótonas*.

Definición 1.1.4. Dada una categoría $\mathcal{C}$, podemos construir una nueva categoría llamada la **categoría opuesta** $\mathcal{C}^{\mathrm{OP}}$ (con " OP" por opuesta) que tiene los mismos objetos que $\mathcal{C}$ pero tal que:

$$Hom_{\mathcal{C}^{\mathrm{OP}}}(B, A) = Hom_{\mathcal{C}}(A, B),$$

y cuya ley de composición se deriva naturalmente de la $\mathcal{C}$. Se dice frecuentemente que $\mathcal{C}^{\mathrm{OP}}$ se ha obtenido a partir de $\mathcal{C}$ "poniendo las flechas al revés "; en efecto:

$$B \xrightarrow{f} A \text{ en } \mathcal{C}^{\mathrm{OP}} \text{ si y sólo si } B \xleftarrow{f} A \text{ en } \mathcal{C}.$$

1.2. El principio de dualidad

La importancia de la noción de la categoría dual u opuesta, es la posibilidad de "duplicar", en cierto sentido, cada concepto y cada teorema acerca de las categorías. Sin mucha dificultad podemos observar que para cada categoría $\mathcal{C}$ se tiene que $(\mathcal{C}^{\mathrm{OP}})^{\mathrm{OP}} = \mathcal{C}$. Entonces cada construcción que se tenga en $\mathcal{C}$ puede considerarse como una construcción en $\mathcal{D}^{\mathrm{OP}}$, donde $\mathcal{D} = \mathcal{C}^{\mathrm{OP}}$. Esto cambia la dirección de las flechas o la dirección de los morfismos sin cambiar las matemáticas.

Desde el principio de nuestros estudios, en las matemáticas es común ser testigos de definiciones que parecen complementarias en algún sentido. Para ello es necesario dar una noción sobre lo opuesto.

i. Para un concepto P, relativo a una categoría general $\mathcal{C}$, el *concepto dual* se obtiene al aplicar este concepto en la categoría dual $\mathcal{C}^{\mathrm{OP}}$.

ii. Para cada teorema válido en categorías el *teorema dual*, que se obtiene al cambiar todos los conceptos en el teorema original por sus duales, es también válido.

Aunque el *Principio de Dualidad* es un tanto informal y vago, sus aplicaciones son claras y muy amplias. Algunos conceptos duales de la matemática:

1. En conjuntos el cuantificador universal $\forall$ su concepto dual es el cuantificador $\exists$.

2. En **TOP** (la categoría de los espacios topológicos), el concepto dual de un abierto es el de cerrado.

Demos un método para dualizar una propiedad relativa a objetos en una categoría arbitraria.

Ejemplo 1.2.1. Sea $\mathscr{P}$ una propiedad de objetos en $\mathcal{C}$, donde $\mathcal{C}$ es una categoría arbitraria.

1. Sea $X \in \mathcal{OB}_{\mathcal{C}}$, defínase la siguiente propiedad $\mathscr{P}_{\mathcal{C}}(X)$ como:

$$\mathscr{P}_{\mathcal{C}}(X) \equiv \forall A \in \mathcal{OB}_{\mathcal{C}}\ \exists! f \in Hom(A, X)$$

Es decir existe un único morfismo $A \xrightarrow{f} X$

i. Como primer paso hay que sustituir $\mathcal{OB}_{\mathcal{C}}$ por ${\mathcal{OB}_{\mathcal{C}}}^{OP}$ y $Hom_{\mathcal{C}}(A, B)$ por $Hom_{\mathcal{C}}(A, B)^{OP}$, con lo que obtenemos:

$$\mathscr{P}^{OP}_{\mathcal{C}}(X) \equiv \forall A \in \mathcal{OB}_{\mathcal{C}^{\mathrm{OP}}}\ \exists! f \in (Hom(A, X))^{OP}$$

ii. Sabemos que:

$${\mathcal{OB}_{\mathcal{C}}}^{OP} \equiv \mathcal{OB}_{\mathcal{C}^{\mathrm{OP}}} \equiv \mathcal{OB}_{\mathcal{C}}$$

Y que:

$$Hom_{\mathcal{C}}(A, B)^{OP} \equiv Hom_{\mathcal{C}^{\mathrm{OP}}}(A, B) \equiv Hom_{\mathcal{C}}(B, A).$$

De esta manera hay que dar el enunciado lógicamente equivalente:

$$\mathscr{P}_{\mathcal{C}^{\mathrm{OP}}}(X) \equiv \forall A \in \mathcal{OB}_{\mathcal{C}}\ \exists! f \in Hom(X, A)$$

En caso de que existan los objetos que cumplan las propiedades anteriores, éstos son conocidos en teoría de categorías como *objeto inicial* (el objeto X que cumple $\mathscr{P}_{\mathcal{C}}(X)$) y *objeto terminal* (el objeto X que cumple ${\mathscr{P}^{\mathrm{OP}}}_{\mathcal{C}}(X)$) respectivamente.

Si pensamos en una categoría específica como **SET** la propiedad anterior y su dual pueden ser muy ilustrativas, así pues consideremos $X \in \mathcal{OB}_{\mathbf{SET}}$ es decir, sea X un conjunto.

$\mathscr{P}_{\mathbf{SET}}(X) \equiv \forall A \in \mathcal{OB}_{\mathbf{SET}}\ \exists!\ f \in Hom(A, X)$.

Esto significa que dado un conjunto X existe una única función f de él a cualquier conjunto A.

Si este conjunto X existiera, y tuviese al menos un elemento entonces la función a cualquier conjunto, con al menos un elemento más que él, no sería única. Así que si tal conjunto X existe debe ser vacío, es decir $X = \emptyset$.

La interpretación del concepto dual en **SET**:

$\mathscr{P}_{\mathbf{SET}^{OP}}(X) \equiv \forall A \in \mathcal{OB}_{\mathbf{SET}}\ \exists!\ f \in Hom(X, A)$.

Es decir, dado un conjunto X existe una única función f de cualquier conjunto A a él.

Ahora bien, si este conjunto X existiese, por la definición de función y debido a que el conjunto A puede ser no vacío entonces X debe ser necesariamente distinto del conjunto vacío. Si el conjunto X tuviera más de un elemento, podrían definirse más de una función (si tiene al menos dos elementos pueden definirse al menos dos funciones constantes distintas). Por esta razón el conjunto X está forzado a ser unitario $X = \{a\}$.

Entonces hemos encontrado que en la categoría **SET** existe objeto inicial y objeto final, a saber $\emptyset$ y $\{a\}$ respectivamente. Hay que notar que el objeto inicial parece ser único y se verá adelante mientras que el final parece que no. Más adelante veremos con detalle estas definiciones.

Veamos ahora un par de ejemplos de dualización de una propiedad de flechas de una categoría.

2. Sean $\mathcal{C}$ una categoría arbitraria, $A, B \in \mathcal{OB}_{\mathcal{C}}$ y $f \in Hom_{\mathcal{C}}(A, B)$, definamos la siguiente propiedad de f:

$$\mathscr{P}_{\mathcal{C}}(f) \equiv \exists g \in Hom_{\mathcal{C}}(B, A) \text{ tal que } g \circ f = id_A.$$

Sigamos el método para dualizar usado en el inciso anterior:

i. $\mathscr{P}_{\mathcal{C}}(f)^{OP} \equiv \exists g \in Hom_{\mathcal{C}}(B, A)^{OP}$ tal que $g \circ_{OP} f = id_A^{OP}$.

ii. Demos el enunciado lógicamente equivalente usando las propiedades descritas en la Definición 1.1.4

$$\mathscr{P}_{\mathcal{C}^{\mathrm{OP}}}(f) \equiv \exists g \in Hom_{\mathcal{C}}(A, B) \text{ tal que } f \circ g = id_B.$$

Analicemos su significado en la categoría de los conjuntos **SET**:

⋆ Consideremos pues $A, B \in \mathbf{SET}$ y sea $f : A \to B$ una función, entonces

$$\mathscr{P}_{\mathbf{SET}}(f) \equiv \exists g \in Hom(B, A) \text{ tal que } g \circ f = id_A.$$

Es decir esta propiedad es la definición de la función *inversa izquierda* de f.

⋆ Y claramente el significado de la propiedad opuesta en la categoría de los conjuntos es la definición de función *inversa derecha* de f.

3. Sea $\mathcal{C}$ una categoría, un $\mathcal{C}$-morfismo $f : A \longrightarrow B$ es una *retracción* si existe un morfismo $g : B \longrightarrow A$ tal que

$$f \circ g = Id_B.$$

Es decir la propiedad queda como sigue:

$$\mathscr{P}_{\mathcal{C}}(f) \equiv \exists g \in Hom_{\mathcal{C}}(B, A) \text{ tal que } f \circ g = id_B.$$

Sigamos el método usado en los incisos anteriores para dualizar:

i. $\mathscr{P}_{\mathcal{C}}(f)^{OP} \equiv \exists g \in Hom_{\mathcal{C}}(B, A)^{OP}$ tal que $f \circ_{OP} g = id_B^{OP}$.

ii. Demos el enunciado lógicamente equivalente usando las propiedades descritas en la Definición 1.1.4

$$\mathscr{P}_{\mathcal{C}^{\mathrm{OP}}}(f) \equiv \exists g \in Hom_{\mathcal{C}}(A, B) \text{ tal que } g \circ f = id_A.$$

Este concepto es conocido como *corretracción*.

Así como en los incisos anteriores, presentaremos una definición explícita para una mejor comprensión del concepto antes dado.

Tanto la *retracción* como la *corretracción* son conceptos "abstractos": se definen únicamente por medio de propiedades algebraicas de la composición. Ahora estamos interesados en su significado concreto, es decir, necesitamos saber cuáles morfismos son retracciones y corretracciones cuando hablamos de una categoría específica.

a. Consideremos la categoría $\mathcal{C} = \mathbf{SET}$, tal como lo muestra el punto 2 de este ejemplo, las retracciones son precisamente las funciones suprayectivas y las corretracciones son las funciones inyectivas.

b. En la categoría de los espacios topológicos **TOP** donde los objetos son parejas (X, α) con X un conjunto y α su topología, los morfismos de un espacio (X, α) en el espacio (Y, β) (ambos $\mathcal{OB}_{\mathbf{TOP}}$) son todas las funciones continuas, es decir, las funciones $f : X \to Y$ tales que la preimagen de un conjunto abierto es un conjunto abierto

$$M \in \beta \text{ implica que } f^{-1}(M) \in \alpha.$$

La composición es la composición de funciones continuas.

El término retracción proviene de la topolgía general. Un subespacio (Y, β) de un espacio topológico (X, α) es llamado *retracción* de (X, α) si existe una función continua $f : (X, \alpha) \to (Y, \beta)$ con $f(x) = x$ para toda $y \in Y$. Aquí f es retracción, y el morfismo inclusión $i : (Y, \beta) \to (X, \alpha)$ es corretracción.

1.3. Diagramas

Uno de los aspectos más agradables de pensar y trabajar con categorías es que esto nos permite hacer analogías que antes no podíamos o no sabíamos

reconocer. Además, pensar categóricamente nos da la oportunidad de ver a los objetos como puntos y a los morfismos entre ellos como flechas. De esta manera, debemos dar la formalización del concepto de multigráfica y diagrama.

Definición 1.3.1. Una **multigráfica dirigida** G consiste de un conjunto V llamado el conjunto de vértices y, para cada pareja ordenada $(u, v) \in V \times V$ un conjunto (posiblemente vacío) A llamado conjunto de flechas de u a v.

Definición 1.3.2. Un **diagrama** en una categoría $\mathcal{C}$ es una multigráfica dirigida cuyos vértices son $\mathcal{C}$-objetos y cuyas flechas son $\mathcal{C}$-morfismos.

Por ejemplo,

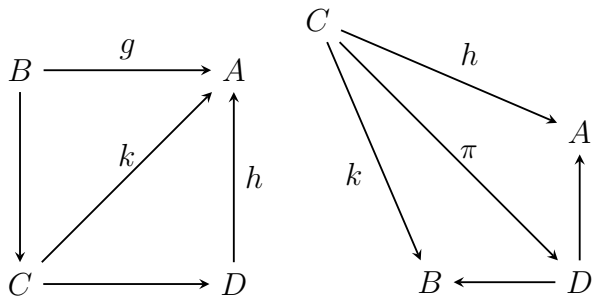


Figura 1.1: Ejemplos de diagramas

Si pensamos en una flecha como en una calle con una sola dirección, entonces un *camino* en un diagrama es una "caminata" de un vértice a otro cuidándose de no equivocarse de sentido. Un camino en un diagrama se ve como la composición de morfismos.

Definición 1.3.3. Un diagrama *conmuta* si, para cada par de vértices A y B cualesquiera dos caminos de A a B son iguales; esto significa que las composiciones deben ser el mismo morfismo.

Tenemos el diagrama de la Figura 1.2 de la retracción definida en el Ejemplo 1.2.1 inciso 3, donde se tiene que $f \circ g = Id_B$.

En el diagrama de la derecha de la misma Figura 1.2 tenemos el *producto fibrado* de dos $\mathcal{C}$-morfismos $f : B \to A$ y $g : C \to A$ (este concepto se verá posteriormente con detalle).

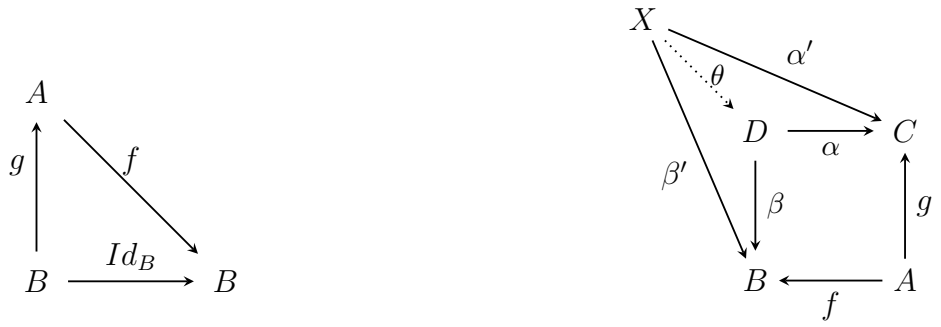


Figura 1.2: Ejemplos de diagramas conmutativos

1.4. Producto y coproducto

Al igual que en los primeros estudios de cualquier entidad nueva en las matemáticas, es conveniente definir operaciones entre los objetos introducidos, de esta manera podemos dar lo siguiente:

Definición 1.4.1. Sean I un conjunto de índices, $\mathcal{C}$ una categoría arbitraria y $\{A_i | i \in I\}$ una familia de $\mathcal{C}$-objetos indexada por el conjunto I. El **producto** de la familia $\{A_i | i \in I\}$ es un $\mathcal{C}$-objeto P junto con una familia de $\mathcal{C}$-morfismos llamados *proyecciones*, $\{\pi_i : P \to A_i | i \in I\}$ tal que para cada $\mathcal{C}$-objeto B y cualquier familia de $\mathcal{C}$-morfismos $\{\varphi_i : B \to A_i | i \in I\}$ existe un único $\mathcal{C}$-morfismo $\varphi : B \to P$ tal que $\pi_i \circ \varphi = \varphi_i$ para toda $i \in I$.

El *producto* P de la familia $\{A_i | i \in I\}$, normalmente se denota como $\prod_{\mathbf{i \in I}} \mathbf{A_i}$.

Usemos lo que hemos aprendido de diagramas conmutativos para describir la definición de forma esquemática. En el caso particular donde el conjunto de índices $I = \{1, 2\}$, el producto de $\{A_1, A_2\}$ es el $\mathcal{C}$-objeto P junto con una familia de $\mathcal{C}$-morfismos $\{\pi_i : P \to A_i | i \in \{1, 2\}\} = \{\pi_1, \pi_2\}$. Si ponemos esta frase con flechas, obtenemos:

El producto de $\{A_1, A_2\}$ es el $\mathcal{C}$-objeto P junto con los $\mathcal{C}$-morfismos

$$A_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} A_2,$$

tales que para cualquier otro diagrama de la forma

$$A_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2} A_2,$$

existe un único morfismo $\varphi : B \to P$ tal que el siguiente diagrama conmuta:

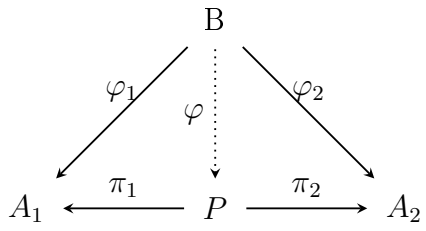


Figura 1.3: Diagrama del producto de dos $\mathcal{C}$-objetos

Si ponemos un conjunto de índices arbitrario obtenemos que el siguiente diagrama conmuta para cada i:

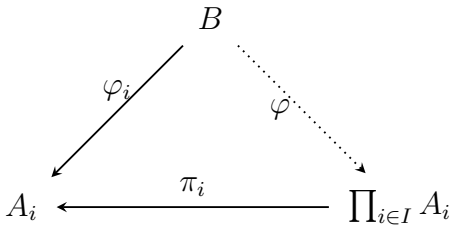


Figura 1.4: Diagrama del producto de una familia de $\mathcal{C}$-objetos

En ocasiones no existe el producto de una familia, pero hay muchas categorías en las que siempre existe. En la categoría **SET** el producto sí existe y de hecho es el producto cartesiano de conjuntos.

Observación 1.4.2. Si $\{A_i | i \in I\}$ es una familia de conjuntos, entonces su producto cartesiano $\prod_{i\in I} A_i$ es el producto en la categoría **SET**.

Demostración. El enunciado de la observación obvia los $\mathcal{C}$-morfismos que se requieren para que se pueda dar la condición de producto. Para cada $j \in I$

definamos $\pi_j : \prod_{i\in I} A_i \to A_j$ como $\pi_j(a_i)_{i\in I} = a_j$, con $a_j \in A_j$. Sea B un conjunto y, para cada $i \in I$ consideremos a la familia de funciones $\{\varphi_i | \varphi_i : B \to A_i \text{ es función}\}$. Definamos $\varphi : B \to \prod_{i\in I} A_i$ como $\varphi(x) = (\varphi_i(x))_{i\in I}$ para toda $x \in B$. Verifiquemos dos cosas, la primera es que efectivamente el diagrama conmuta y la segunda es que φ es única.

1. Sea $x \in B$ entonces $(\pi_i \circ \varphi)(x) = \pi_i(\varphi(x)) = \pi_i\left((\varphi_j(x))_j\right) = \varphi_i(x)$, por tanto $\pi_i \circ \varphi = \varphi_i$ para toda $i \in I$. En términos de diagrama eso significa que el diagrama conmuta.

2. Finalmente demostremos que φ es única. Supongamos que

$$\psi : B \to \prod_{i\in I} A_i$$

es una función que hace que el diagrama también conmute, esto significa que $(\pi_i \circ \psi)(x) = \varphi_i(x)$ para toda $i \in I$. Es decir para cada i, la i-ésima coordenada de $\psi(x)$ es $\varphi_i(x)$ que es también la i-ésima coordenada de $\varphi(x)$. Por lo tanto $\psi(x) = \varphi(x)$ para toda $x \in B$, y de esta manera obtenemos que $\psi = \varphi$.

■

Tal como ya se ha expuesto, cada enunciado que se tiene en una categoría viene acompañado por su dual. Demos el dual de la Definición 1.4.1.

Definición 1.4.3. El **coproducto**, también conocido como **suma**, de una familia $\{A_i | i \in I\}$ de $\mathcal{C}$-objetos, es un $\mathcal{C}$-objeto S, junto con una familia de $\mathcal{C}$-morfismos $\{\iota_i : A_i \to S | i \in I\}$ llamados *inyecciones* tales que para cualquier $\mathcal{C}$-objeto B y cualquier familia de $\mathcal{C}$-morfismos $\{\psi_i : A_i \to B | i \in I\}$ existe un único $\mathcal{C}$-morfismo $\psi : S \to B$ tal que $\psi \circ \iota_i = \psi_i$ para toda $i \in I$.

La notación para coproducto $S = \coprod_{i\in I} A_i$. Al igual que el producto, el coproducto puede o no existir dependiendo de la categoría.

Pongamos la definición anterior con un diagrama, primero para el coproducto de $\{A_1, A_2\}$ y después para una familia $\{A_i | i \in I\}$ de $\mathcal{C}$-objetos, con I un conjunto de índices:

Demos la observación dual de la Observación 1.4.2 pero antes hagamos una construcción que nos dará pauta para dar la observación dual:

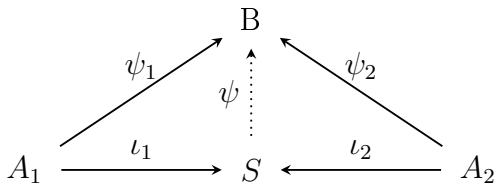


Figura 1.5: Diagrama del coproducto de dos $\mathcal{C}$-objetos

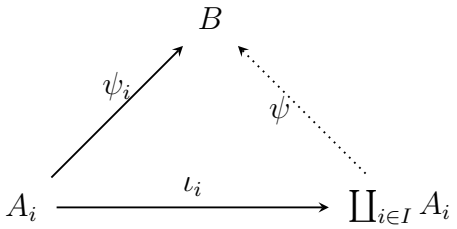


Figura 1.6: Diagrama del coproducto de una familia de $\mathcal{C}$-objetos

Consideremos a A_1 y a A_2 dos subconjuntos de un conjunto cualquiera X, entonces sabemos la forma de definir su intersección como

$$A_1 \cap A_2 = \{s \in X | s \in A_1 \text{ y } s \in A_2\}.$$

Podemos definir la unión ajena de dos subconjuntos A_1 y A_2 que no son ajenos, realizando un proceso de ajenización. Consideremos el producto cartesiano $(A_1 \cup A_2) \times \{1, 2\}$, y consideremos los subconjuntos $A_1' = A_1 \times \{1\}$ y $A_2' = A_2 \times \{2\}$. Es claro que $A_1' \cap A_2' = \emptyset$. Se suele llamar a $A_1' \cup A_2'$ la *unión ajena* de A_1 y A_2. Pongamos atención a las siguientes dos funciones $\iota_1 : A_1 \to A_1'$ y $\iota_2 : A_2 \to A_2'$ dadas por $\iota_1(s) = (s, 1)$ y $\iota_2(s) = (s, 2)$. Denotamos la unión ajena $A_1' \cup A_2'$ por $A_1 \coprod A_2$. Es fácil generalizar la ajenización a una familia $\{A_i | i \in I\}$ de conjuntos. De esta manera podemos dar la dualización de la Observación 1.4.2.

Observación 1.4.4. Si $\{A_i | i \in I\}$ es una familia de conjuntos, entonces su unión ajena definida en el párrafo anterior $\coprod_{i\in I} A_i = \bigcup_{i\in I} A_i'$ es el coproducto en la categoría **SET**.

Demostración. Sean B un conjunto arbitrario y $\psi_i : A_i \to B$ una familia de funciones dadas, entonces existe una función $\psi : \coprod_{i\in I} A_i \to B$ que extiende

a cada ψ_i. Sea $c \in \coprod_{i\in I} A_i$, entonces $c = (a_i, i) \in A'_i$ para alguna $i \in I$. Definamos $\psi((a_i, i)) = \psi_i(a_i)$, entonces $(\psi \circ \iota_i)(a_i) = \psi((a_i, i)) = \psi_i(a_i)$ para toda $a_i \in A_i$. Por lo tanto $\psi \circ \iota_i = \psi_i$, es decir el Diagrama 1.6 conmuta en la categoría **SET**. Falta verificar la unicidad de la función encontrada:

Supongamos que $\theta : \coprod_{i\in I} A_i \to B$ es una función que satisface $\theta \circ \iota_i = \psi_i$ para toda $i \in I$, entonces

$$\theta((a_i, i)) = \theta(\iota_i(a_i)) = (\theta \circ \iota_i)(a_i) = \psi_i(a_i, i) = \psi((a_i, i)).$$

Por tanto, θ coincide con ψ en $\coprod_{i\in I} A_i = \bigcup_{i\in I} A'_i$ de ahí que $\theta = \psi$ y en conclusión la función ψ es única. ■

Es necesario aclarar que si tenemos dos $\mathcal{C}$-objetos que son productos o coproductos de una familia en la categoría, entonces dichos objetos tienen que ser equivalentes. Es decir hay unicidad en el producto y el coproducto. Solamente se demostrará una equivalencia debido a que la otra es análoga y se puede encontrar en la bibliografía [7] p. 448. Además es sencillo generalizar el resultado para una familia arbitraria pero para fines de claridad se da el resultado para el coproducto de dos $\mathcal{C}$-objetos.

Teorema 1.4.5. *Sea $\mathcal{C}$ una categoría y sea $\{A_i | i \in \{1, 2\}\}$ $\mathcal{C}$-objetos, entonces cualesquiera dos productos (coproductos) de la familia $\{A_i | i \in I\}$, en caso de existir, son equivalentes.*

Demostración. Supongamos que P y P' son los productos de los $\mathcal{C}$-objetos A_1 y A_2. Es decir, el producto de A_1 y A_2 cumple:

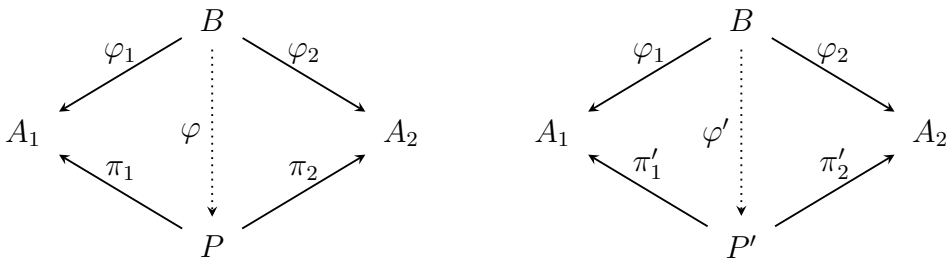


Figura 1.7: Diagrama donde P y P' son los productos de los $\mathcal{C}$-objetos A_1 y A_2.

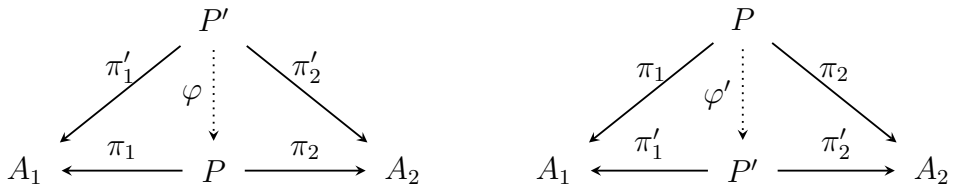


Figura 1.8: Diagrama considerando a B como P' y a B como P del Diagrama 1.7

Considerando a B como P' y también considerando a B como P en el Diagrama 1.7 obtenemos el Diagrama 1.8

Consideremos ahora el diagrama que resulta de fusionar la información de los Diagramas 1.8.

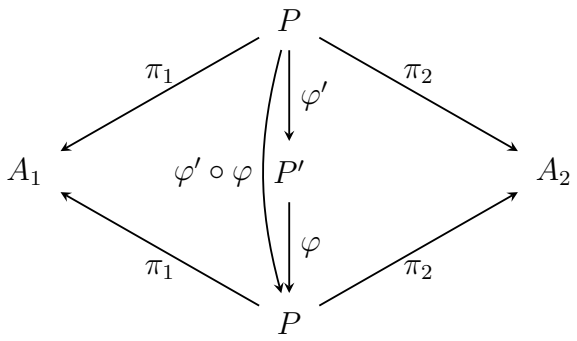


Figura 1.9: Diagrama que resulta de fusionar la información de los diagramas 1.8

El Diagrama 1.9 conmuta debido a que:

$$\pi_1 \circ (\varphi \circ \varphi') = (\pi_1 \circ \varphi) \circ \varphi' = \pi_1' \circ \varphi' = \pi_1,$$

y también

$$\pi_2 \circ (\varphi \circ \varphi') = (\pi_2 \circ \varphi) \circ \varphi' = \pi_2' \circ \varphi' = \pi_2.$$

Pero claramente, el morfismo identidad $Id_P : P \to P$ también hace que el diagrama conmute. Pero por la unicidad de la flecha punteada en el diagrama

de la definición de producto (Definición 1.4.1), $\varphi' \circ \varphi = Id_P$. El mismo argumento se aplica para demostrar que $\varphi \circ \varphi' = Id_{P'}$. Por tanto φ es una equivalencia. ■

1.5. Funtores

En teoría de categorías los morfismos, más que los objetos, son los que tienen un papel fundamental. De hecho, es posible definir "categoría" sin hacer uso de la noción de objeto. Es posible dar también una visión más general y considerar a las categorías mismas como objetos estructurados. Los "morfismos" entre ellas que preservan su estructura son llamados *funtores*.

Definición 1.5.1. Sean $\mathcal{C}$ y $\mathcal{D}$ categorías, entonces un **funtor** $\mathbf{F}$ de $\mathcal{C}$ a $\mathcal{D}$ es una función que asigna a cada $\mathcal{C}$-objeto A un $\mathcal{D}$-objeto $\mathbf{F}(A)$, y a cada $\mathcal{C}$-morfismo $A \xrightarrow{f} A'$ un $\mathcal{D}$-morfismo $\mathbf{F}(A) \xrightarrow{\mathbf{F}(f)} \mathbf{F}(A')$, tal que

1. $\mathbf{F}$ preserva la composición; es decir,

$$\mathbf{F}(f \circ g) = \mathbf{F}(f) \circ \mathbf{F}(g)$$

   siempre que $f \circ g$ esté definida, y

2. $\mathbf{F}$ preserva morfismos identidad; es decir,

$$\mathbf{F}(Id_A) = id_{\mathbf{F}(A)}$$

   para cada $\mathcal{C}$-objeto A.

Normalmente los funtores $\mathbf{F}$ de $\mathcal{C}$ a $\mathcal{D}$ se denotan por $\mathbf{F} : \mathcal{C} \to \mathcal{D}$ ó también pueden denotarse como $\mathcal{C} \xrightarrow{\mathbf{F}} \mathcal{D}$. Suele escribirse una notación simplificada $\mathbf{F}\mathcal{C}$ y $\mathbf{F}f$ en lugar de $\mathbf{F}(\mathcal{C})$ y $\mathbf{F}(f)$. De hecho es común denotar la acción del funtor $\mathbf{F}$ al mismo tiempo en objetos y morfismos como:

$$\mathbf{F}\left(A \xrightarrow{f} B\right) = \mathbf{F}A \xrightarrow{\mathbf{F}f} \mathbf{F}B.$$

Hay que hacer notar que un funtor $\mathbf{F} : \mathcal{C} \to \mathcal{D}$ es técnicamente una familia de funciones; de $\mathcal{OB}(\mathcal{C})$ en $\mathcal{OB}(\mathcal{D})$, y para cada pareja (A, B) de $\mathcal{C}$-objetos, una familia de $hom(A, B)$ en $hom(\mathbf{F}A, \mathbf{F}B)$. Debido a que los funtores preservan los morfismos identidad y debido también a que existe una

correspondencia biyectiva entre la clase de objetos y la clase de los morfismos identidad en una categoría, la parte del objeto de un funtor está determinada por morfismos. De hecho un funtor entre categorías puede simplificarse como una función entre las clases de morfismos que preservan identidades y composición. Antes de continuar demos ejemplos para entender mejor lo que es un funtor:

Ejemplo 1.5.2. Sean $\mathcal{C}$ y $\mathcal{D}$ categorías:

1. El *funtor identidad*, denotado por $id_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ definido por
$$id_{\mathcal{C}} \left(A \xrightarrow{f} B \right) = \left(A \xrightarrow{f} B \right).$$

2. Dado cualquier $\mathcal{D}$-objeto A' se define el *funtor constante* $C_{A'} : \mathcal{C} \to \mathcal{D}$ con valor A', definido como
$$C_{A'} \left(A \xrightarrow{f} B \right) = A' \xrightarrow{id_{A'}} A'.$$

3. Para cualquiera de los ejemplos 1.1.2, hay un *funtor olvidadizo* (también conocido como *funtor subyacente*) $U : \mathcal{C} \to \mathbf{SET}$, donde en cada caso $U(c)$ es el conjunto subyacente de $c \in \mathcal{C}$, y $U(f) = f$ es la función subyacente del morfismo f.

4. Para cualquier $\mathcal{C}$-objeto C, existe el *funtor hom covariante* denotado por $hom(C, \_) : \mathcal{C} \to \mathbf{SET}$ definido por
$$hom(C, \_) \left(A \xrightarrow{f} B \right) = \left(hom(C, A) \xrightarrow{hom(C,f)} hom(C, B) \right)$$
donde $hom(C, f)(g) = f \circ g$.

5. Para cualquier $\mathcal{C}$-objeto C, existe el *funtor hom contravariante* denotado por $hom(\_, C) : \mathcal{C}^{OP} \to \mathbf{SET}$ definido en cualquier $\mathcal{C}^{OP}$-morfismo $A \xrightarrow{f} B$ como:
$$hom(\_, C) \left(A \xrightarrow{f} B \right) = \left(hom_{\mathcal{C}}(A, C) \xrightarrow{hom(f,C)} hom_{\mathcal{C}}(B, C) \right)$$
donde $hom(f, C)(g) = g \circ f$, donde la composición es la misma que en $\mathcal{C}$.

6. El *funtor covariante conjunto potencia* denotado como $\mathcal{P} : \mathbf{SET} \to \mathbf{SET}$ se define por

$$\mathcal{P}\left(A \xrightarrow{f} B\right) = \mathcal{P}A \xrightarrow{\mathcal{P}f} \mathcal{P}B$$

donde $\mathcal{P}A$ es el conjunto potencia de A, es decir, el conjunto de todos los subconjuntos de A; y para cada $C \subseteq A$, $\mathcal{P}f(C)$ es la imagen $f[C]$ de C bajo f.

7. El *funtor contravariante conjunto potencia* denotado como $\mathcal{Q} : \mathbf{SET}^{OP} \to \mathbf{SET}$ se define por

$$\mathcal{Q}\left(A \xrightarrow{f} B\right) = \mathcal{Q}A \xrightarrow{\mathcal{Q}f} \mathcal{Q}B$$

donde $\mathcal{Q}A$ es el conjunto potencia de A y para cada $C \subseteq A$, $\mathcal{Q}f(C)$ es la imagen inversa $f^{-1}[C]$ de C bajo la función $f : B \to A$.

8. Para cualquier entero positivo n, el *funtor n-ésima potencia* $S^n : \mathbf{SET} \to \mathbf{SET}$ está dado por

$$S^n\left(A \xrightarrow{f} B\right) = A^n \xrightarrow{f^n} B^n$$

donde $f^n(x_1, \ldots, x_n) = (f(x_1), \ldots, f(x_n))$.

9. El *funtor dual para espacios vectoriales sobre los reales* denotado por $(\widehat{\ }) : \mathbf{VEC}^{OP} \to \mathbf{VEC}$ el cual asocia a cualquier espacio vectorial V su espacio dual $\widehat{V}$ (es decir, el espacio vectorial $hom(V, \mathbb{R})$ con las operaciones definidas puntualmente) y con cualquier $\mathbf{VEC}^{OP}$-morfismo $V \xrightarrow{f} W$, es decir cualquier función lineal $W \xrightarrow{f} V$, el morfismo $\widehat{f} : \widehat{V} \to \widehat{W}$, definido por $\widehat{f}(g) = g \circ f$.

En muchas categorías como las mencionadas en el Ejemplo 1.1.2, todo objeto en la categoría es de hecho un conjunto y todo morfismo $f : A \to B$ en la categoría es una función en los conjuntos subyacentes (que además suelen tener otras propiedades). Formalicemos esta noción:

Definición 1.5.3. Sea $\mathscr{X}$ una categoría. Una **categoría concreta** sobre $\mathscr{X}$ es una pareja $(\mathcal{C}, U)$ donde $\mathcal{C}$ es una categoría y $U : \mathcal{C} \to \mathscr{X}$ es el funtor olvidadizo. Algunas veces U es llamado el *funtor olvidadizo* (o también puede ser llamado *subyacente*) de la categoría concreta y $\mathscr{X}$ es llamada la *categoría base* de $(\mathcal{C}, U)$.

Una categoría concreta sobre **SET** es llamada **construcción**.

Ejemplo 1.5.4. Tal como ya habíamos mencionado tenemos que:

1. Toda categoría $\mathcal{C}$ puede ser vista como una categoría concreta por medio del funtor identidad $(\mathcal{C}, id_{\mathcal{C}})$ sobre sí misma.

2. La categoría de grupos **GRP** es una construcción.

3. $(\mathcal{C}, U)$ es una construcción, por un abuso de notación se denota sólo con $\mathcal{C}$. Por ejemplo, la categoría abstracta de los espacios vectoriales y la construcción de los espacios vectoriales ambas se denotan por **VEC**. Siempre será claro en el contexto a cuál se está haciendo referencia.

1.6. Objeto libre

Las construcciones son muy usadas ya que se pueden trabajar no sólo sus propiedades categóricas, sino que también se tienen propiedades de conjuntos, subconjuntos, etc.

Definición 1.6.1. Sean F un objeto en una construcción $\mathcal{C}$, X un conjunto no vacío e $i : X \to F$ una función (de conjuntos). F es **libre en el conjunto** X siempre que para cualquier $\mathcal{C}$-objeto A y cualquier función (de conjuntos) $f : X \to A$ existe un único morfismo en $\mathcal{C}$, $\bar{f} : F \to A$ tal que $\bar{f} \circ i = f$ (como función de conjuntos $X \to A$).

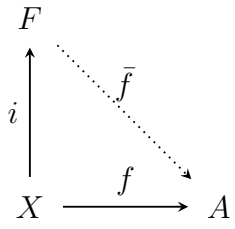


Figura 1.10: Diagrama donde F es libre en el conjunto X

Si observamos cuidadosamente la definición anterior podremos darnos cuenta que ya hemos visto esto en estructuras conocidas, como los espacios vectoriales.

Ejemplo 1.6.2. Esta definición categórica tiene una gran variedad de teoremas en ramas de las matemáticas, nos restringiremos a construcciones:

- En **VEC** tenemos el teorema que nos dice la manera de construir transformaciones lineales entre espacios vectoriales sobre el mismo campo. El teorema nos dice que si $v_1, \ldots, v_n$ es una base del espacio vectorial V sobre un campo F, W es también un F-espacio vectorial y $\{w_1, \ldots, w_n\} \subseteq W$ entonces existe una única transformación lineal $T : V \to W$ con $T(v_i) = w_i$. Esto nos dice que las bases son objetos libres en **VEC**.

- En **GRP** veamos que $\mathbb{Z}$ (el grupo de los números enteros) es objeto libre: Consideremos a G un grupo arbitrario y a $f : \mathbb{Z} \to G$ una función de conjuntos. Fijémonos en el valor de f en 1, supongamos que $f(1) = g$ para alguna $g \in G$. Definamos $\bar{f} : \mathbb{Z} \to G$ como $\bar{f}(n) = g^n$. Claramente $\bar{f}$ es un morfismo único, ya que por un lado $\langle 1 \rangle = \mathbb{Z}$ y bajo $\bar{f}$ se tiene que $1 \mapsto g$ entonces si hubiese otra función $k : \mathbb{Z} \to G$ tal que $k(1) = g = \bar{f}(1)$ entonces $k(n) = g^n$ por lo cual $\bar{f} = k$. De esta manera consideremos $X = \{1\}$ e $i : X \to \mathbb{Z}$ la función inclusión, entonces

  $$\left(\bar{f} \circ i\right)(1) = \bar{f}(i(1)) = \bar{f}(1) = g = f(1).$$

  Por tanto $\mathbb{Z}$ cumple ser un objeto libre en **GRP**.

- Veamos que en **GRP**, el grupo aditivo $\mathbb{Q}$ no cumple ser un objeto libre: Consideremos $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \in \mathcal{OB}_{\mathbf{GRP}}$ y notemos que en **GRP** no existe un homomorfismo no trivial de grupos

  $$f : \mathbb{Q} \to S_3$$

  ya que de haberlo tendríamos:

  1. $\mathrm{Nuc} f \lneqq \mathbb{Q}$.
  2. Si $\mathrm{Nuc} f = \{0\}$ entonces por el primer teorema de isomorfismo de grupos

     $$\mathbb{Q}/\mathrm{Nuc} f = \mathbb{Q}/\{0\} \cong \mathbb{Q} \cong \mathrm{Im} f, \text{ con } \mathrm{Im} f \leq S_3.$$

     Claramente por razones de cardinalidad esto es imposible y por tanto el núcleo es un subgrupo propio no trivial de $\mathbb{Q}$.

3. Por el primer teorema de isomorfismo de grupos sabemos que

$$\mathbb{Q}/\mathrm{Nuc}f \cong \mathrm{Im}f, \text{ con } \mathrm{Im}f \leq S_3.$$

Y con los incisos anteriores tenemos que

$$\{0\} \neq \mathrm{Im}f \lneqq S_3.$$

4. Sabemos que los únicos subgrupos propios no triviales de S_3 son $\langle(1\ 2)\rangle \cong \langle(1\ 3)\rangle \cong \langle(2\ 3)\rangle \cong \mathbb{Z}_2$ y $\langle(1\ 2\ 3)\rangle \cong \mathbb{Z}_3$. Por tanto

$$\mathrm{Im}f \cong \mathbb{Z}_2 \text{ o } \mathrm{Im}f \cong \mathbb{Z}_3.$$

5. Por teoría de grupos sabemos que si G es un grupo y $H \trianglelefteq G$ con $[G : H] = p$ entonces para cualquier $g \in G$ se tiene que $g^p \in H$. (Hay que notar la importancia de la hipótesis de normalidad porque de otra manera el resultado citado sería falso). Por los incisos anteriores tenemos que $[\mathbb{Q} : \mathrm{Nuc}f] = 2$ o $[\mathbb{Q} : \mathrm{Nuc}f] = 3$.

   Si $[\mathbb{Q} : \mathrm{Nuc}f] = 2$ entonces consideremos $t \in \mathbb{Q} - \mathrm{Nuc}f$, es claro que $\frac{t}{2} \in \mathbb{Q}$. Aplicando el resultado inicial de este inciso tenemos que $2 \cdot \frac{t}{2} \in \mathrm{Nuc}f$. Esto implica que $t \in \mathrm{Nuc}f$ lo cual es una contradicción. Por tanto $[\mathbb{Q} : \mathrm{Nuc}f] \neq 2$

   De manera análoga se demuestra que $[\mathbb{Q} : \mathrm{Nuc}f] \neq 3$. Y con ello se concluye que no puede haber un homomorfismo no trivial

$$f : \mathbb{Q} \to S_3.$$

Entonces para cualquier conjunto X, cualquier función $i : X \to \mathbb{Q}$ y cualquier función $f : X \to S_3$ con $f(x) \neq (1)$ para alguna $x \in X$ no existe un homomorfismo $\bar{f} : \mathbb{Q} \to S_3$ tal que $\bar{f} \circ i = f$. Con esto hemos demostrado que $\mathbb{Q}$ no es un objeto libre en **GRP**.

Es importante saber la relación que pueden llegar a tener los objetos libres en nuestras construcciones, demos entonces el resultado de unicidad. De aquí en adelante y a menos que se especifique lo contrario, consideraremos a la categoría $\mathcal{C}$ como una construcción y la llamaremos simplemente categoría.

Teorema 1.6.3. *Si $\mathcal{C}$ es una categoría (construcción), $F, F' \in \mathcal{OB}_{\mathcal{C}}$ tales que F es libre en el conjunto X, F' es libre en el conjunto X' y $|X| = |X'|$, entonces F es equivalente a F'.*

Demostración. Para demostrar que F es equivalente a F', debemos dar la equivalencia entre estos dos $\mathcal{C}$-objetos. Como $|X| = |X'|$ tenemos entonces la biyección dada por la igualdad de la cardinalidad, nombremos $h : X \to X'$ a tal biyección. Como F y F' son libres en X y X' respectivamente tenemos:

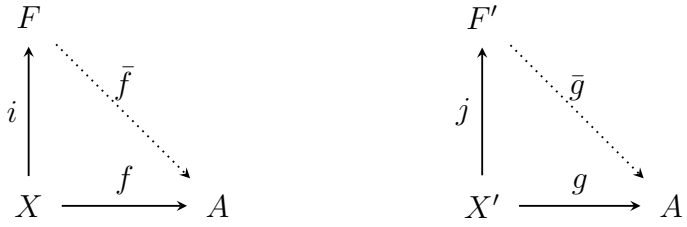


Figura 1.11: Diagramas donde F es libre en X y F' es libre en X'.

Es decir, que dadas las funciones de conjuntos $i : X \to F$ y $j : X' \to F'$ para cualquier $A \in \mathcal{OB}_{\mathcal{C}}$ y cualesquiera funciones de conjuntos $f : X \to A$ y $g : X' \to A$ existen únicos morfismos en $\mathcal{C}$, $\bar{f} : F \to A$ y $\bar{g} : F' \to A$ tales que $\bar{f} \circ i = f$ y $\bar{g} \circ j = g$ (como funciones de conjuntos $X \to A$ y $X' \to A$.)

Fusionemos ambos Diagramas de 1.11 considerando en el de la izquierda a A como F', la biyección $h : X \to X'$, la función $j : X' \to F'$, el único morfismo que existe por ser F' libre en X' $\bar{g} : F' \to A$ y la función $j \circ h : X \to F'$.

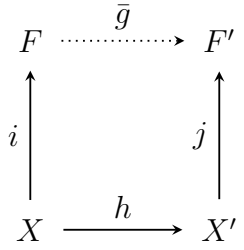


Figura 1.12: Diagrama 1.11 considerando en el de la izquierda a A como F', la biyección $h : X \to X'$, la función $j : X' \to F'$, el único morfismo que existe por ser F' libre en X' $\bar{g} : F' \to A$ y la función $j \circ h : X \to F'$.

Análogamente, como h es una función biyectiva, entonces h tiene inversa $h^{-1} : X' \to X$, usando el otro Diagrama de 1.11 con $A = F$, la biyección

$h^{-1} : X' \to X$, la función $i : X \to F$, el único morfismo que existe por ser F libre en X $\bar{f} : F \to A$ y la función $i \circ h^{-1} : X' \to F$.

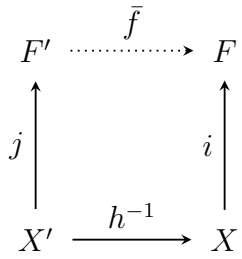


Figura 1.13: Diagrama 1.11 considerando en el de la derecha a A como F, la biyección $h^{-1} : X' \to X$, la función $i : X \to F$, el único morfismo que existe por ser F libre en X' $\bar{f} : F \to A$ y la función $i \circ h^{-}1 : X' \to F$.

Conjuntemos estos dos diagramas obteniendo que,

$$\begin{aligned}\left(\bar{f} \circ \bar{g}\right) \circ i &= \bar{f} \circ (\bar{g} \circ i) \\ &= \bar{f} \circ (j \circ h) = \left(\bar{f} \circ j\right) \circ h \\ &= \left(i \circ h^{-1}\right) \circ h \\ &= i.\end{aligned}$$

También tenemos que $Id_F \circ i = i$ y sabemos que F es libre en X lo que significa que para cualquier $\mathcal{C}$-objeto F y cualquier función digamos $i : X \to F$ existe un único morfismo en $\mathcal{C}$, $\psi : F \to F$ tal que $\psi \circ i = i$. Pero en este caso tenemos tanto a $\bar{f} \circ \bar{g}$ como a Id_F que lo hacen, por la unicidad del morfismo del objeto libre tenemos que $\psi = \bar{f} \circ \bar{g} = Id_F$.

De manera análoga es claro que $\bar{g} \circ \bar{f} = Id_{F'}$ y por lo tanto F es equivalente a F'.

■

Ya hemos observado que tanto en la demostración del Teorema 1.4.5 como en la del Teorema 1.6.3 se ha seguido un procedimiento que es importante mencionar. Un objeto S en una categoría $\mathcal{C}$ es llamado *solución* o *flecha universal* si está definido por un diagrama donde, no importa si variamos

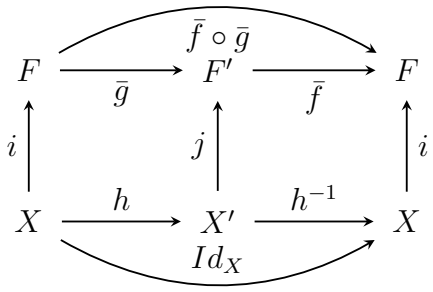
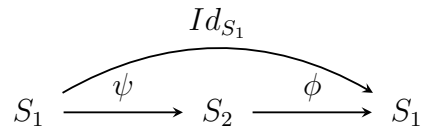


Figura 1.14: Conjuntando los diagramas 1.12 y 1.13.

el objeto X junto con morfismos del diagrama, existe un único morfismo que hace que el diagrama conmute. El "metateorema" son las soluciones, si existen, son únicas con una equivalencia única. En esta tesis únicamente se dará una noción esquemática e informal ya que su formalización requiere de abundante material que sale del objetivo de este trabajo, si se requiere la noción formal y exacta así como todo el material aledaño necesario puede consultarse [5] y [1].

En la demostración del "metateorema" hay dos pasos. El primero, si tenemos dos soluciones $\mathcal{C}$-objetos (en el caso del objeto libre, dos objetos libres) junto con dos $\mathcal{C}$-morfismos ψ y ϕ y tenemos que hay un $\mathcal{C}$-objeto en el diagrama que es arbitrario digamos X, entonces lo que hacemos es sustituir a este $\mathcal{C}$-objeto arbitrario X por la solución de la que no se habla en el diagrama. Es decir si se tienen dos soluciones S_1 y S_2 con sus respectivos $\mathcal{C}$-morfismos y un $\mathcal{C}$-objeto arbitrario X en cada diagrama entonces sustituimos en el diagrama de S_1 a X por S_2 y en el diagrama de S_2 a X por S_1.

El segundo paso es juntar los dos diagramas que se tienen en uno de manera adecuada. Es decir, se considera un solo diagrama con la solución $X = S_1$ en el diagrama de S_1 pero haciendo uso de las flechas $\psi \circ \phi$ y con Id_{S_1}.



Ambos resultan ser $\mathcal{C}$-morfismos que hacen que el diagrama para S_1 conmute pero resulta que el $\mathcal{C}$-morfismo que acompaña a S_1 debe ser único y con ello se concluye que $\psi \circ \phi = Id_{S_1}$. Análogamente se procede para que $\phi \circ \psi = Id_{S_2}$ y demostrar así que ψ es una equivalencia con lo cual resulta que las soluciones S_1 y S_2 son esencialmente la misma.

1.7. Objeto inicial, terminal y cero

En esta sección veremos otra perspectiva las Definiciones 1.4.1, 1.4.3 y 1.6.1 ya que en este punto estamos en condiciones de decir que están definidos por medio de flechas universales. Veremos que esto proviene de un solo concepto que se mencionó en el Ejemplo 1.2.1.

Definición 1.7.1. Sean $\mathcal{C}$ una categoría e $I \in \mathcal{OB}_{\mathcal{C}}$. Decimos que I es un **objeto inicial** (o **universal**) si para todo $\mathcal{C}$-objeto C existe exactamente uno y sólo un $\mathcal{C}$-morfismo $I \to C$. De manera dual, un $\mathcal{C}$-objeto T se dice que es **objeto terminal** (o **couniversal**) si para cada $\mathcal{C}$-objeto C existe uno y sólo un morfismo $C \to T$.

Veamos algunos ejemplos para darnos cuenta que ya hemos estado en contacto con los objetos universales y sus duales.

Ejemplo 1.7.2.

1. Como lo vimos en el Ejemplo 1.2.1 el conjunto vacío $\emptyset$ es el único objeto inicial para la categoría **SET**, de la misma manera el conjunto vacío parcialmente ordenado es el único objeto inicial en **POS**.

2. Así como en el Ejemplo 1.2.1 obtuvimos que el conjunto vacío es el único objeto inicial en la categoría **SET**, procedamos para encontrar el o los objetos iniciales en la categoría **GRP**.

   Sea $I \in \mathcal{OB}_{\mathbf{GRP}}$, para que I sea objeto inicial es necesario que cumpla la Definición 1.7.1 esto significa que para todo grupo G existe exactamente uno y sólo un homomorfismo de grupos $f : I \to G$. Como I es un grupo entonces sabemos que al menos debe tener un elemento (el neutro e_I). Veamos que pasaría si I tuviera más de un elemento: Supongamos que $|I| > 1$ entonces es claro que si consideramos a $G = I$ entonces se pueden definir $f_1 : I \to I$ como $g \mapsto e_I$ para cualquier $g \in I$ y por otro

lado se puede definir $f_2 : I \to I$ como $f_2 = Id_I$. Entonces si $|I| > 1$, I no puede ser objeto inicial. Por tanto $I = \{e\}$ y es la única posibilidad, esto significa que **GRP** tiene un único objeto inicial que es el grupo trivial.

3. Analicemos ahora si **VEC** tiene o no objeto inicial: Al igual que en el inciso anterior sea $I \in \mathcal{OB}_{\mathbf{VEC}}$, para que I sea objeto inicial es necesario que cumpla la Definición 1.7.1 esto significa que para todo F-espacio vectorial V existe exactamente una y sólo una transformación lineal $T : I \to V$. Al igual que en el inciso anterior sabemos que como I es un F-espacio vectorial entonces debe tener al menos un elemento, el cero 0_I. Veamos que pasaría si I tuviera más de un elemento: Supongamos que $|I| > 1$ entonces es claro que si consideramos a $V = I$ entonces se pueden definir $T_1 : I \to I$ como $T_1 = T_0$ la transformación lineal cero y por otro lado se puede definir $T_2 : I \to I$ como $T_2 = Id_I$. Entonces si $|I| > 1$, I no puede ser objeto inicial. Por tanto $I = \{0\}$ y es la única posibilidad, esto significa que **VEC** tiene un único objeto inicial que es el F-espacio vectorial trivial.

Veamos ejemplos de objetos terminales:

4. En el Ejemplo 1.2.1 encontramos que los conjuntos unitarios son los objetos terminales para la categoría **SET**, de la misma manera el los unitarios resultan ser los objetos terminales en **POS**.

5. Hagamos el mismo análisis que en los incisos anteriores pero ahora para el objeto terminal en la categoría **GRP**. Sea $T \in \mathcal{OB}_{\mathbf{GRP}}$ por la Definición 1.7.1 para todo grupo G existe un único homomorfismo de grupos $f : G \to T$. Si dicho grupo existiera, debe tener al menos el elemento neutro. Si este grupo tuviese más de un elemento entonces estaríamos en la misma situación que en el caso de objeto inicial, por tanto el objeto terminal existe en la categoría **GRP** y es el grupo trivial.

6. De la misma manera el objeto terminal en la categoría **VEC** es el F espacio vectorial trivial $V_0 = \{0\}$.

Teorema 1.7.3. *Sea $\mathcal{C}$ una categoría. Cualesquiera dos $\mathcal{C}$-objetos iniciales [terminales] son esencialmente únicos, es decir:*

- *Si A y B son objetos iniciales [terminales], entonces A y B son equivalentes.*
- *Si A es un objeto inicial [terminal], entonces cualquier otro objeto equivalente a A también lo es.*

Demostración. Por definición de objeto inicial tenemos que si A y B son objetos iniciales entonces para cualquier $\mathcal{C}$-objeto C existe exactamente uno y sólo un $\mathcal{C}$-morfismo $A \xrightarrow{k} C$ y $B \xrightarrow{h} C$, utilizando a A y B en lugar de C obtenemos

$$A \xrightarrow{k} B \text{ y } B \xrightarrow{h} A.$$

Pero de hecho tenemos que $h \circ k = Id_A$ y $k \circ h = Id_B$ ya que Id_A y Id_B son los únicos morfismos de A en A y B en B respectivamente. Con lo cual k es un isomorfismo.

Supongamos ahora que A es un objeto inicial y que $k : A' \to A$ es un isomorfismo. Debido a que A es un objeto inicial tenemos que para cada objeto B, existe un único morfismo $f : A \to B$, entonces $f \circ k : A' \to B$ es un morfismo de A' en B. Para ver que A' es un objeto inicial basta verificar que $f \circ k$ es único, para ello observemos que si existiera otro morfismo $g : A' \to B$ entonces $g \circ k^{-1} : A \to B$ pero A es un objeto inicial y sabemos que para cada objeto B, existe un único morfismo $f : A \longrightarrow B$ y por tanto $g \circ k^{-1} = f$, es decir $g = f \circ k$.

■

Con estas dos definiciones de los objetos terminales e iniciales podemos definir aquellos objetos en las categorías que tienen la propiedad de ser tanto terminales como finales. Hay que notar que debido a que los objetos terminales son los duales de los objetos iniciales, la noción que se dará a continuación es sobre un objeto que es su propio dual, es decir, A tendrá la propiedad siguiente en $\mathcal{C}$ si y sólo si la tiene en $\mathcal{C}^{OP}$.

Definición 1.7.4. Sea $\mathcal{C}$ una categoría y sea $A \in \mathcal{OB}_{\mathcal{C}}$. Decimos que A es un **objeto cero** si A es tanto objeto inicial como objeto terminal.

Ejemplo 1.7.5. De los ejemplos que hemos trabajado es claro que:

1. La categoría **SET** y la categoría **POS** no tienen objetos cero.

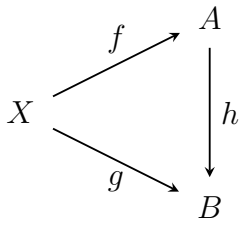
2. En la categoría **GRP** el grupo trivial es el objeto cero.

3. En la categoría **VEC** el F espacio vectorial trivial es el objeto cero.

4. Construyamos un objeto inicial en una categoría arbitraria que nos dará una visión general de lo que hemos estado trabajando: Consideremos $\mathcal{C}$ una construcción y $F \in \mathcal{OB}_{\mathcal{C}}$ un objeto libre en el conjunto X con $X \xrightarrow{i} F$ (tal como se definió en 1.6.1). Definamos una nueva categoría $\mathcal{D}$ como sigue:

   Los objetos de $\mathcal{D}$ son todas las funciones de conjuntos $f : X \to A$, donde A es el conjunto subyacente del objeto A de $\mathcal{C}$.

   Los morfismos en $\mathcal{D}$ de $f : X \to A$ a $g : X \to B$ los definiremos como los morfismos $h : A \to B$ de $\mathcal{C}$ tales que $h \circ f = g$ es decir, que el siguiente diagrama conmuta:



   Veamos que $Id_A^{\mathcal{C}} : A \to A$ es el morfismo identidad de f a f en $\mathcal{D}$, es decir, que funciona como $Id_f^{\mathcal{D}}$: Consideremos a $h \in Hom_{\mathcal{D}}(f, g)$, es decir consideremos $h \in Hom_{\mathcal{C}}(A, B)$, $f, g \in \mathcal{OB}_{\mathcal{D}}$. Por la definición de $Hom_{\mathcal{D}}$ tenemos que $f \in Hom_{\mathcal{C}}(X, A)$ y $g \in Hom_{\mathcal{C}}(X, B)$ con $A, B \in \mathcal{OB}_{\mathcal{C}}$. Hagamos la composición deseada:

$$Id_g \circ_{\mathcal{D}} h = Id_B \circ_{\mathcal{C}} h = h.$$

   De manera análoga obtenemos que

$$h \circ_{\mathcal{D}} Id_f = h \circ_{\mathcal{C}} Id_A = h.$$

   Las composiciones anteriores son claras debido a que $\mathcal{C}$ es una construcción y a que Id_A es la identidad para cada $A \in \mathcal{OB}_{\mathcal{C}}$. Por tanto $Id_A^{\mathcal{C}} : A \to A$ es el morfismo identidad f a f en $\mathcal{D}$ denotado por $Id_f^{\mathcal{D}}$.

Si h es una equivalencia en $\mathcal{D}$ entonces es claro que también lo es en $\mathcal{C}$. Mostremos que el recíproco también se cumple: Consideremos a $h \in Hom_{\mathcal{D}}(f, g)$ que a la vez es equivalencia en $\mathcal{C}$, entonces por ser equivalencia existe un morfismo k en $\mathcal{C}$ tal que

$$h \circ_{\mathcal{C}} k = Id_B \text{ y } k \circ_{\mathcal{C}} h = Id_A.$$

Hay que verificar que k es también el morfismo inverso de h en $\mathcal{D}$. Basta demostrar que $k \in Hom_{\mathcal{D}}(g, f)$. Como k es el morfismo inverso de h en $\mathcal{C}$ entonces $k \in Hom_{\mathcal{C}}(B, A)$, también como $h \in Hom_{\mathcal{D}}(f, g)$ tenemos a $f : X \to A$, $g : X \to B$ y $g = h \circ f$. Consideremos las funciones anteriores f y g y hagamos la composición con k:

$$k \circ_{\mathcal{C}} g = k \circ_{\mathcal{C}} (h \circ_{\mathcal{C}} f) = (k \circ_{\mathcal{C}} h) \circ_{\mathcal{C}} f = Id_A \circ_{\mathcal{C}} f = f.$$

Pero esto significa que

$$k \in Hom_{\mathcal{D}}(g, f).$$

Por tanto hemos demostrado que h es una equivalencia en $\mathcal{D}$ si y sólo si h es equivalencia en $\mathcal{C}$.

Ahora como F es libre en el conjunto X entonces para cada función $f : X \to A$ existe un único morfismo $\bar{f} : F \to A$ tal que $\bar{f} \circ i = f$. Pero esto significa entonces que $i : X \to F$ es un objeto inicial en la categoría $\mathcal{D}$.

5. Hagamos otra construcción categórica. Consideremos a la familia de objetos $\{A_i | i \in I\}$ en la categoría $\mathcal{C}$. Construyamos la categoría $\mathcal{E}$ donde:

   Los $\mathcal{E}$-objetos son las parejas $\big(B, \{f_i | i \in I\}\big)$, con B un $\mathcal{C}$-objeto y para cada i, $f_i : B \to A_i$ es un $\mathcal{C}$-morfismo.

   Los $\mathcal{E}$-morfismos del $\mathcal{E}$-objeto $\big(B, \{f_i | i \in I\}\big)$ al $\big(D, \{g_i | i \in I\}\big)$ los definimos como $\mathcal{C}$-morfismo $B \xrightarrow{h} D$ en $\mathcal{C}$ tales que $g_i \circ_{\mathcal{C}} h = f_i$ para toda $i \in I$.

   Verifiquemos que los Ib_B son el morfismo identidad de $\big(B, \{f_i | i \in I\}\big)$ en $\mathcal{E}$: Es claro que $h \circ_{\mathcal{C}} I_B = h$, además $f_i \circ_{\mathcal{C}} I_B = f_i$ y por tanto I_B es el morfismo identidad de $\big(B, \{f_i | i \in I\}\big)$ en $\mathcal{E}$.

Al igual que en el ejemplo anterior veamos que h es equivalencia en $\mathcal{C}$ si y sólo si es equivalencia en $\mathcal{E}$:

Consideremos $h \in Hom_{\mathcal{C}}\Big(\big(B, \{f_i | i \in I\}\big), \big(D, \{g_i | i \in I\}\big)\Big)$ tal que h es equivalencia en $\mathcal{C}$, es decir $h \in Hom_{\mathcal{C}}(B, D)$ y existe $k \in Hom_{\mathcal{C}}(D, B)$ tal que $h \circ_{\mathcal{C}} k = Id_D$ y $k \circ_{\mathcal{C}} h = Id_B$. Para cada $i \in I$ tenemos que

$$f_i \circ_{\mathcal{C}} k = (g_i \circ_{\mathcal{C}} h) \circ_{\mathcal{C}} k = g_i \circ_{\mathcal{C}} (h \circ_{\mathcal{C}} k) = g_i \circ_{\mathcal{C}} Id_D = g_i,$$

por lo tanto

$$k \in Hom_{\mathcal{C}}\Big(\big(B, \{f_i | i \in I\}\big), \big(D, \{g_i | i \in I\}\big)\Big).$$

Con ello hemos demostrado que h es equivalencia en $\mathcal{E}$ si lo es en $\mathcal{C}$. Ahora para el recíproco consideremos

$$h \in Hom_{\mathcal{C}}\Big(\big(B, \{f_i | i \in I\}\big), \big(D, \{g_i | i \in I\}\big)\Big) \text{ equivalencia en } \mathcal{E},$$

entonces por ser equivalencia sabemos que existe

$$k \in Hom_{\mathcal{C}}\Big(\big(B, \{f_i | i \in I\}\big), \big(D, \{g_i | i \in I\}\big)\Big)$$

y cumple $h \circ_{\mathcal{E}} k = Id_D$ y $k \circ_{\mathcal{E}} h = Id_B$. Por como esta definido $Hom(\mathcal{E})$ y la composición concluimos que h es equivalencia en $\mathcal{C}$.

Si el producto (tal como se definó en 1.4.1) de la familia $\{A_i | i \in I\}$ existe en $\mathcal{C}$ con las proyecciones $\pi_k : \prod A_i \to A_k$ para cada $k \in I$ entonces para toda pareja $(B, \{f_i\}_{i \in I})$ en $\mathcal{E}$ se tiene que por definición del producto existe un único morfismo $\varphi : B \to \prod A_i$ tal que $\pi_i \circ \varphi = f_i$ para toda $i \in I$. Pero con la Definición 1.7.1 sabemos entonces que $(\prod A_i, \{\pi | i \in I\})$ es objeto terminal en la categoría $\mathcal{E}$, con esto usando el Teorema 1.7.3 concluimos que el producto $\prod A_i$ de la familia $\{A_i | i \in I\}$ es único.

Capítulo 2

Grupos libres

Esta parte del trabajo se concentrará en mostrar que los objetos libres (llamados *grupos libres*) existen en la categoría concreta de los grupos (construcción). A través de este procedimiento se describirán grupos en términos de *generadores y relaciones*. Además se dará la construcción de coproducto (producto libre) en la categoría de grupos.

2.1. Construcción de grupos libres

En esta sección se construirá un objeto en la categoría de grupos, se le brindará una operación binaria con la que se le dotará de estructura de grupo. Este grupo se construirá con el fin de que cumpla la propiedad categórica de objeto libre (Definición 1.6.1).

Consideremos un conjunto dado X y construyamos un grupo F que es libre en el conjunto X en el sentido de la Definición 1.6.1. Analicemos los dos posibles casos para el conjunto X:

1. Si $X = \varnothing$ entonces definimos a F como el grupo trivial $\langle e \rangle$.

2. Si $X \neq \varnothing$ entonces denotemos por X^{-1} otro conjunto tal que $|X^{-1}| = |X|$ (debido a que X es no vacío entonces X^{-1} es no vacío).

   Como $|X^{-1}| = |X|$ escojamos una biyección $f : X \to X^{-1}$ (observemos que al menos existe una biyección dada por la igualdad de la cardinalidad de conjunto), sea $x \in X$ y denotemos su imagen bajo la biyección

f como x^{-1}. Por último escojámos un conjunto ajeno a $X \cup X^{-1}$ y que tenga un elemento, denotemos a este conjunto como 1.

Consideremos la unión de estos conjuntos como nuestro conjunto de trabajo, es decir, consideremos $X \cup X^{-1} \cup \{1\}$. Definimos una **palabra** en X como la sucesión $(a_1, a_2, \dots)$ con $a_i \in X \cup X^{-1} \cup \{1\}$,para toda $i \in \mathbb{N}$ que cumple:

a. Para alguna $n \in \mathbb{N}$ $a_k = 1$ para toda $k \geq n$.

b. La sucesión constante $(1, 1, \dots)$ la llamamos **palabra vacía** y se denota como **1**.

3. Una palabra $(a_1, a_2, \dots)$ en X se dice que es **reducida** siempre que:

   i. Para cualquier $x \in X$, x y x^{-1} son no adyacentes. Esto significa que si $a_i = x$ entonces $a_{i+1} \neq x^{-1}$ y si $a_i = x^{-1}$ entonces $a_{i+1} \neq x$ para toda $i \in \mathbb{N}$ y $x \in X$.

   ii. Si $a_k = 1$ entonces $a_i = 1$ para toda $i \geq k$.

Con estas definiciones obtenemos que la palabra vacía es reducida debido a que $a_i = 1$ para toda $i \in \mathbb{N}$ y con ello cumple por vacuidad el inciso i de la definición anterior.

Analicemos la forma de una palabra reducida, por el inciso i se tiene la sucesión $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, \dots)$ donde $n \in \mathbb{N}$, $x_i \in X$ y $\lambda_i = \pm 1$. Por convención tenemos que x^1 denota a x para toda $x \in X$. Para ser palabra se requiere que, a partir de algún término se estacione la sucesión en 1 y con la condición del inciso ii los 1 están acomodados al final de la sucesión, es decir se tiene que: $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$. Para simplificar la notación y sabiendo que cada palabra está determinada por los términos anteriores al primer 1 denotaremos a la palabra $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$ por

$$x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}.$$

Observación 2.1.1. Sean $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$ y $y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}$ palabras reducidas. Entonces $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$ es igual a $y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}$ si y sólo si ambas son 1 o $m = n$ y $x_i = y_i$, $\lambda_i = \delta_i$ para $i \in \{1, \dots, n\}$.

Demostración.

$\Longrightarrow$) Supongamos que $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}$ y $y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}$ son la misma palabra reducida.

Si $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}$ es 1 entonces como $y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}$ es igual a ella también debe ser 1.

Supongamos entonces que $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}$ y $y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}$ son la misma palabra reducida y son distintas de 1. Esto significa que las sucesiones subyacentes

$$(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_m^{\lambda_m}, 1, 1, \dots) \text{ y } (y_1^{\delta_1}, y_2^{\delta_2}, \dots, y_n^{\delta_n}, 1, 1, \dots),$$

son iguales; es decir, las sucesiones término a término son iguales, $x_i^{\lambda_i} = y_j^{\delta_j}$ para $i \in \{\ 1, \dots, m\ \}$ y $j \in \{\ 1, \dots, n\ \}$.

Si $m \neq n$ entonces $x_m^{\lambda_i} \neq 1$ y $y_n^{\delta_j} = 1$ lo cual es una contradicción debido a la igualdad de las sucesiones. Se tiene la misma contradicción si $x_m^{\lambda_i} = 1$ y $y_n^{\delta_j} \neq 1$ por lo cual la hipótesis de que $m \neq n$ es incorrecta, por tanto $m = n$.

Por la igualdad de las sucesiones obtenemos también que $i = j$ y que $x_i^{\lambda_i} = y_i^{\delta_i}$; como $\lambda_i = \pm 1 = \delta_i$ podemos analizar dos casos que son esencialmente el mismo:

Supongamos que $\lambda_i = 1$ entonces $x_i = y_i^{\delta_i}$. Si $\delta_i = -1$ entonces $x_i = y_i^{-1}$, lo cual es una contradicción ya que el conjunto X y el conjunto X^{-1} son ajenos.

De manera análoga se obtiene una contradicción similar cuando $\lambda_i = -1$ y $\delta_i = 1$, por lo tanto $\lambda_i{=}\delta_i$ para toda $i \in \{1, \dots, n\}$.

Con todo lo anterior obtenemos $x_k = y_k$ para toda $k \in \{1, \dots n\}$.

$\Longleftarrow$) Supongamos que $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}$ y $y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}$ palabras reducidas tales que ambas son 1 o $m = n$ y $x_i = y_i$, $\lambda_i = \delta_i$ para $i \in \{1, \dots, n\}$.

En el primer caso si ambas son 1 entonces ambas tienen como sucesión subyacente a

$$(1, 1, \dots)$$

eso quiere decir que son la misma sucesión y por tanto son la misma palabra reducida.

En el segundo caso, si $m = n$ y $x_i = y_i$, $\lambda_i = \delta_i$ para $i \in \{1, \dots, n\}$ entonces las sucesiones subyacentes son las mismas y por tanto son la misma palabra reducida.

■

Es claro a partir de esta observación que se puede dar una relación entre el conjunto X y el conjunto $F(X)$ de todas las palabras reducidas en X obteniendo el siguiente resultado.

Proposición 2.1.2. *Sean X un conjunto no vacío y $F(X)$ el conjunto de todas las palabras reducidas en X. Entonces la función*

$$X \xrightarrow{\phi} F(X)$$

dada por

$$x \xmapsto{\phi} x^1$$

es una función inyectiva.

Demostración. Es claro usando la Observación 2.1.1 que la función está bien definida. Por otro lado, si $\phi(x) = \phi(y)$ con $x, y \in X$ entonces $x^1 = y^1$ es decir ambas palabras son iguales y por la Observación 2.1.1 obtenemos que sus sucesiones subyacentes son iguales y por tanto $x = y$. De aquí que ϕ es una función inyectiva.

■

Identifiquemos a X con su imagen bajo ϕ y de esta manera consideremos a X como un subconjunto de $F(X)$. Definamos una operación binaria

$$* : F(X) \times F(X) \to F(X)$$

en el conjunto $F(X)$ de todas la palabras reducidas en X(para reducir notación y mientras no existan confusiones denotemos a $F(X)$ por F).

La palabra vacía 1 será el elemento identidad, es decir, para cualquier palabra reducida $x \in F$ se cumple que $x * 1 = 1 * x = x$.

De manera intuitiva lo que buscamos es dar una operación sencilla, una posibilidad es simplemente considerar la yuxtaposición (es decir, poniendo una palabra y pegarle la segunda), veamos si esto es posible. Consideremos $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$ y $y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}$ palabras reducidas, consideremos la yuxtaposición:

$$x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m} y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}.$$

El problema principal de esto es que podría darse el caso en el que $x_m^{\lambda_m} y_1^{\delta_1} = 1$, es decir que $\left(x_m^{\lambda_m}\right)^{-1} = y_1^{\delta_1}$ y esto significa que la palabra

$$x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m} y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}$$

no es reducida. Por tanto, no obtenemos una operación simplemente con la yuxtaposición de palabras reducidas. Para quitar este inconveniente podemos simplemente cancelar estos términos, es decir si tenemos las palabras $x_1^{-1} x_2^1 x_3^1 x_4^{-1} x_8^1$ y $x_8^{-1} x_4^1 x_3^{-1} x_1^1 x_5^{-1} x_6^1$ entonces

$$\left(x_1^{-1} x_2^1 x_3^1 x_4^{-1} x_8^1\right) * \left(x_8^{-1} x_4^1 x_3^{-1} x_1^1 x_5^{-1} x_6^1\right) = x_1^{-1} x_2^1 x_1^1 x_5^{-1} x_6^1,$$

de manera general definamos:

Sean $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$ y $y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}$ palabras reducidas no vacías en X:

- Si $m \leq n$ entonces consideremos k el entero mayor $(0 \leq k \leq m)$ tal que $x_{m-j}^{\lambda_{m-j}} = \left(y_{j+1}^{\delta_{j+1}}\right)^{-1} = y_{j+1}^{-\delta_{j+1}}$ para $j \in \{1, \ldots, k-1\}$. Entonces definimos:

$$\left(x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}\right) * \left(y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}\right) = \begin{cases} x_1^{\lambda_1} \cdots x_{m-k}^{\lambda_{m-k}} y_{k+1}^{\delta_{k+1}} \cdots y_n^{\delta_n} & si \quad k < m \\ y_{k+1}^{\delta_{k+1}} \cdots y_n^{\delta_n} & si \quad k = m < n \\ 1 & si \quad k = m = n \end{cases}$$

- Si $m \geq n$ entonces consideremos k el entero mayor $(0 \leq k \leq n)$ tal que $x_{m-j}^{\lambda_{m-j}} = \left(y_{j+1}^{\delta_{j+1}}\right)^{-1} = y_{j+1}^{-\delta_{j+1}}$ para $j \in \{1, \ldots, k-1\}$. Entonces definimos:

$$\left(x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}\right) * \left(y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}\right) = \begin{cases} x_1^{\lambda_1} \cdots x_{m-k}^{\lambda_{m-k}} y_{k+1}^{\delta_{k+1}} \cdots y_n^{\delta_n} & si \quad k < n \\ x_1^{\lambda_1} \cdots x_{k-1}^{\lambda_{k-1}} & si \quad k = n < m \\ 1 & si \quad k = m = n \end{cases}$$

Esta definición garantiza la cerradura del producto de palabras reducidas. Una vez que se tiene la operación en el conjunto, es posible preguntarnos si el conjunto F junto con la operación $*$ tiene estructura de grupo.

Teorema 2.1.3. *Si X es un conjunto no vacío y $F = F(X)$ es el conjunto de todas las palabras reducidas en X, entonces F es un grupo bajo la operación $*$ definida antes y $F = \langle X \rangle$.*

Demostración. Para verificar que $F = F(X)$ y la operación $*$ forman un grupo, hay que verificar tres cosas:

i. La **asociatividad** de $*$, es decir que para cada $x, y, z \in F$ se tiene que

$$x * (y * z) = (x * y) * z;$$

ii. Existe un elemento $e \in F$, llamado **identidad**, tal que $e*x = x = x*e$ para cada $x \in F$;

iii. Todo $x \in G$ tiene **inverso**, es decir existe $x' \in F$ con $x*x' = e = x'*x$.

Es claro que dada la definición de la operación $*$, la palabra vacía 1 es nuestro neutro, es decir $1 = e$.

También es claro que si tenemos la palabra reducida $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$, entonces su inverso será $x_m^{-\lambda_m} \cdots x_2^{-\lambda_2} x_1^{-\lambda_1}$. Por ello lo único que hay que demostrar es el inciso i.

Esto es posible demostrarlo de dos maneras, una es por inducción sobre la longitud de la primera palabra reducida y examinando casos y la segunda es dando una biyección de F y considerar a S_F el grupo de todas biyecciones de F. Demos ambas:

a. Consideremos $x, y, z \in F$, entoces $x = x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$, $y = y_1^{\gamma_1} y_2^{\gamma_2} \cdots y_n^{\gamma_n}$, y $z = z_1^{\delta_1} z_2^{\delta_2} \cdots z_p^{\delta_p}$, con $\lambda_i, \gamma_j, \delta_k = \pm 1$ con $1 \leq i \leq m$, $1 \leq j \leq n$ y $1 \leq k \leq p$. Procedamos por inducción sobre m:

- *Base:* $m = 1$ entonces $x = x_1^{\lambda_1}$, tenemos dos casos:

Caso 1: $n \leq p$

$$
\begin{aligned}
x*(y*z) &= x_1^{\lambda_1} * \left(y_1^{\gamma_1}\cdots y_n^{\gamma_n} * z_1^{\delta_1}\cdots z_p^{\delta_p}\right)\\
&= \begin{cases} x_1^{\lambda_1} * y_1^{\gamma_1}\cdots y_{n-k}^{\gamma_{n-k}} z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad k<n \\ x_1^{\lambda_1} * z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad k=n<p \\ x_1^{\lambda_1} * 1 & si \quad k=n=p \end{cases}\\
&= \begin{cases} x_1^{\lambda_1} y_1^{\gamma_1}\cdots y_{n-k}^{\gamma_{n-k}} z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad k<n \text{ y } x_1^{\lambda_1}\neq y_1^{-\gamma_1} \\ y_2^{\gamma_2}\cdots y_{n-k}^{\gamma_{n-k}} z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad k<n \text{ y } x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n-k\neq 1 \\ z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad k<n \text{ y } x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n-k= 1 \\ x_1^{\lambda_1} z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad k=n<p \text{ y } x_1^{\lambda_1}\neq z_{k+1}^{-\delta_{k+1}} \\ z_{k+2}^{\delta_{k+2}}\cdots z_p^{\delta_p} & si \quad k=n<p \text{ y } x_1^{\lambda_1}= z_{k+1}^{-\delta_{k+1}} \text{ y } k+1<p \\ 1 & si \quad k=n<p \text{ y } x_1^{\lambda_1}= z_{k+1}^{-\delta_{k+1}} \text{ y } k+1=p \\ x_1^{\lambda_1} & si \quad k=n=p \end{cases}
\end{aligned}
$$

Por otro lado

$$
\begin{aligned}
(x*y)*z &= \left(x_1^{\lambda_1} * y_1^{\gamma_1}\cdots y_n^{\gamma_n}\right) * z_1^{\delta_1}\cdots z_p^{\delta_p}\\
&= \begin{cases} x_1^{\lambda_1} y_1^{\gamma_1}\cdots y_n^{\gamma_n} * z_1^{\delta_1}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}\neq y_1^{-\gamma_1} \\ y_2^{\gamma_2}\cdots y_n^{\gamma_n} * z_1^{\delta_1}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n>1 \\ 1 * z_1^{\delta_1}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n=1 \end{cases}\\
&= \begin{cases} x_1^{\lambda_1} y_1^{\gamma_1}\cdots y_{n-k}^{\gamma_{n-k}} z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}\neq y_1^{-\gamma_1} \text{ y } k<n \\ x_1^{\lambda_1} z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}\neq y_1^{-\gamma_1} \text{ y } k=n<p \\ x_1^{\lambda_1} & si \quad x_1^{\lambda_1}\neq y_1^{-\gamma_1} \text{ y } k=n=p \\ y_2^{\gamma_2}\cdots y_n^{\gamma_n} z_1^{\delta_1}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n>1 \text{ y } k<p \\ z_{k+1}^{\delta_{k+1}}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n>1 \text{ y } k=n<p \\ 1 & si \quad x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n>1 \text{ y } k=n=p \\ z_1^{\delta_1}\cdots z_p^{\delta_p} & si \quad x_1^{\lambda_1}= y_1^{-\gamma_1} \text{ y } n=1, \end{cases}
\end{aligned}
$$

por lo tanto tendremos que $x*(y*z)=(x*y)*z$.

Caso 2: $n \geq p$. Este caso se resuelve de la misma forma que el caso anterior.
Es claro que

$$x*(y*z)=(x*y)*z$$

para el caso base.

- *Hipótesis Inductiva:* Supongamos que $x*(y*z)=(x*y)*z$ para x de longitud a lo más m, $y=y_1^{\gamma_1}y_2^{\gamma_2}\cdots y_n^{\gamma_n}$, y $z=z_1^{\delta_1}z_2^{\delta_2}\cdots z_p^{\delta_p}$, con $\lambda_i,\gamma_j,\delta_k=\pm 1$ con $1\leq i\leq m$, $1\leq j\leq n$ y $1\leq k\leq p$.
- *Paso Inductivo:* Consideremos $x=x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_{m+1}^{\lambda_{m+1}}$, $y=y_1^{\gamma_1}y_2^{\gamma_2}\cdots y_n^{\gamma_n}$, y $z=z_1^{\delta_1}z_2^{\delta_2}\cdots z_p^{\delta_p}$, con $\lambda_i,\gamma_j,\delta_k=\pm 1$ con $1\leq i\leq m$, $1\leq j\leq n$ y $1\leq k\leq p$.

  Calculemos $x*(y*z)$ y por otro lado $(x*y)*z$, consideremos $x=x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_{m+1}^{\lambda_{m+1}}=x'*x''=x_1^{\lambda_1}*x_2^{\lambda_2}\cdots x_{m+1}^{\lambda_{m+1}}$, claramente x'' es una palabra reducida de longitud m y como x también es reducida y $x=x'*x''$ entonces $x_1^{\lambda_1}\neq x_2^{-\lambda_2}$. Observemos que x' y x'' son palabras reducidas de longitud a lo más m, por tanto podremos aplicar hipótesis inductiva a ambas:

$$\begin{aligned}
x*(y*z) &= (x'*x'')*(y*z)\\
&= x'*(x''*(y*z)) \text{ por hipótesis inductiva aplicada a } x'\\
&= x'*((x''*y)*z) \text{ por hipótesis inductiva aplicada a } x''\\
&= (x'*(x''*y))*z \text{ por hipótesis inductiva aplicada a } x'\\
&= ((x'*x'')*y)*z \text{ por hipótesis inductiva aplicada a } x''\\
&= (x*y)*z
\end{aligned}$$

  Por lo tanto para cualesquiera palabras reducidas x,y,z en X se cumple que $x*(y*z)=(x*y)*z$. De esta manera hemos demostrado la asociatividad por inducción sobre la longitud de la primera palabra.

b. Consideremos $x\in X$ y $\delta=\pm 1$. Definamos la función $\phi_{x^\delta}:F\to F$ dada por:

$$\phi_{x^\delta}\left(x_1^{\delta_1}\cdots x_n^{\delta_n}\right)=\begin{cases} x^\delta x_1^{\delta_1}\cdots x_n^{\delta_n} & si \quad x^\delta\neq x_1^{-\delta_1}\\ x_2^{\delta_2}\cdots x_n^{\delta_n} & si \quad x^\delta=x_1^{-\delta_1} \text{ y } n>1\\ 1 & si \quad x^\delta=x_1^{-\delta_1} \text{ y } n=1\end{cases}$$

y

$$\phi_{x^\delta}(1)=x^\delta.$$

Es claro que $\phi_{x^\delta}^{-1}:F\to F$ está dada por:

$$\phi_{x^\delta}^{-1}\left(x_1^{\delta_1}\cdots x_n^{\delta_n}\right)=\begin{cases} x_n^{-\delta_n}\cdots x_1^{-\delta_1}x^{-\delta} & si \quad x^\delta\neq x_1^{-\delta_1}\\ x_n^{-\delta_n}\cdots x_2^{-\delta_2} & si \quad x^\delta=x_1^{-\delta_1} \text{ y } n>1\\ 1 & si \quad x^\delta=x_1^{-\delta_1} \text{ y } n=1\end{cases}$$

y

$$\phi_{x^\delta}^{-1}(1) = x^{-\delta}.$$

De esta manera

$$\phi_{x^\delta}\phi_{x^\delta}^{-1} = \phi_{x^\delta}^{-1}\phi_{x^\delta} = Id_F.$$

Esto significa que toda ϕ_{x^δ} es una biyección de F.

Consideremos S_F el grupo de todas las biyecciones de F y sea

$$F_0 = \langle\{\phi_x | x \in X\}\rangle \leq S_F.$$

La función $\varphi : F \to F_0$ dada por

$$\varphi\left(x_1^{\delta_1}\cdots x_n^{\delta_n}\right) = \begin{cases} \phi_{x_1^{\delta_1}} \circ \cdots \circ \phi_{x_n^{\delta_n}} \\ Id \qquad\qquad si \quad x_1^{\delta_1}\cdots x_n^{\delta_n} = 1 \end{cases}$$

Es claramente suprayectiva ya que si $\alpha \in F_0$ con $\alpha = \phi_{x_1} \circ \phi_{x_2} \ldots \phi_{x_m}$ con $x_1, x_2, \ldots x_m \in X$ entonces

$$\varphi\left(x_1 \cdots x_m\right) = \varphi\left(x_1^1 \cdots x_m^1\right) = \phi_{x_1^1} \circ \phi_{x_2^1} \ldots \phi_{x_m^1} = \phi_{x_1} \circ \phi_{x_2} \ldots \phi_{x_m}.$$

Es claro también que para cualesquiera $w_1, w_2 \in F$ con $w_1 = x_1^{\lambda_1}\cdots x_m^{\lambda_m}$ y $w_2 = y_1^{\delta_1}\cdots y_n^{\delta_m}$ se tiene

$$\varphi(w_1 * w_2) = \varphi\left(x_1^{\lambda_1}\cdots x_m^{\lambda_m} * y_1^{\delta_1}\cdots y_n^{\delta_m}\right)$$

$$= \begin{cases} \varphi\left(x_1^{\lambda_1}\cdots x_{m-k}^{\lambda_{m-k}} y_{k+1}^{\delta_{k+1}}\cdots y_n^{\delta_n}\right) & si \quad k < m \text{ y } m \leq n \\ \varphi\left(y_{k+1}^{\delta_{k+1}}\cdots y_n^{\delta_n}\right) & si \quad k = m < n \text{ y } m \leq n \\ \varphi(1) & si \quad k = m = n \end{cases}$$

$$= \begin{cases} \phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_{m-k}^{\lambda_{m-k}}} \circ \phi_{y_{k+1}^{\delta_{k+1}}} \circ \cdots \circ \phi_{y_n^{\delta_n}} & si \quad k < m \text{ y } m \leq n \\ \phi_{y_{k+1}^{\delta_{k+1}}} \circ \cdots \circ \phi_{y_n^{\delta_n}} & si \quad k = m < n \text{ y } m \leq n \\ Id & si \quad k = m = n \end{cases}$$

Como k es el entero mayor $(0 \leq k \leq m)$ tal que

$$x_{m-j}^{\lambda_{m-j}} = \left(y_{j+1}^{\delta_{j+1}}\right)^{-1} = y_{j+1}^{-\delta_{j+1}}$$

para $j \in \{1, \ldots, k-1\}$, entonces $\phi_{x_{m-j}^{\lambda_{m-j}}} = \phi_{y_{j+1}^{-\delta_{j+1}}}$ y así:

$$
\begin{aligned}
&= \begin{cases} \phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_{m-k}^{\lambda_{m-k}}} \circ Id \circ \phi_{y_{k+1}^{\delta_{k+1}}} \circ \cdots \circ \phi_{y_n^{\delta_n}} & si \quad k < m \text{ y } m \leq n \\ Id \circ \phi_{y_{k+1}^{\delta_{k+1}}} \circ \cdots \circ \phi_{y_n^{\delta_n}} & si \quad k = m < n \text{ y } m \leq n \\ Id \circ Id & si \quad k = m = n \end{cases} \\
&= \begin{cases} \phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_{m-k}^{\lambda_{m-k}}} \circ \left(\phi_{x_{m-(k-1)}^{\lambda_{m-(k-1)}}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \circ \phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_k^{\delta_k}} \right) \circ \phi_{y_{k+1}^{\delta_{k+1}}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \\ \left(\phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \circ \phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_k^{\delta_k}} \right) \circ \phi_{y_{k+1}^{\delta_{k+1}}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \\ \left(\phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \right) \circ \left(\phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \right) \end{cases} \\
&= \begin{cases} \left(\phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \right) \circ \left(\phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \right) & si \quad k < m \text{ y } m \leq n \\ \left(\phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \right) \circ \left(\phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \right) & si \quad k = m < n \text{ y } m \leq n \\ \left(\phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \right) \circ \left(\phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \right) & si \quad k = m = n \end{cases} \\
&= \left(\phi_{x_1^{\lambda_1}} \circ \cdots \circ \phi_{x_m^{\lambda_m}} \right) \circ \left(\phi_{y_1^{\delta_1}} \circ \cdots \circ \phi_{y_n^{\delta_n}} \right) \\
&= \varphi\left(x_1^{\lambda_1} \ldots x_m^{\lambda_m} \right) \circ \varphi\left(y_1^{\delta_1} \ldots y_n^{\delta_n} \right) \\
&= \varphi(w_1) \circ \varphi(w_2)
\end{aligned}
$$

Lo anterior nos dice que φ es un homomorfismo, para ver que es inyectivo es suficiente con mostrar que $Nuc\varphi = \{1_F\}$. Sea $x \in Nuc\varphi$ entonces $\varphi(x) = Id_{F_0}$. Como $x \in F$ entonces tiene la forma $x = x_1^{\delta_1} \cdots x_n^{\delta_n}$, sustituyendo obtenemos

$$
\begin{aligned}
\varphi(x) &= \varphi\left(x_1^{\delta_1} \cdots x_n^{\delta_n} \right) \\
&= Id_{F_0}.
\end{aligned}
$$

Y por definición de φ tenemos que

$$\varphi\left(x_1^{\delta_1} \cdots x_n^{\delta_n} \right) = Id_{F_0} \text{ si } x_1^{\delta_1} \cdots x_n^{\delta_n} = 1,$$

por lo tanto

$$Nuc\varphi = \{1_F\}.$$

De aquí que φ sea isomorfismo de grupos, por lo cual

$$F \cong F_0.$$

Como F es isomorfo a un grupo, entonces su operación es asociativa y debido a que

$$F_0 = \langle \{\phi_x | x \in X\} \rangle ,$$

entonces es claro que

$$F = \langle X \rangle .$$

■

De la Definición de grupo libre dada en 2.1.3 podemos dar varios resultados claros:

Observación 2.1.4. Si $|X| \geq 2$, entonces el grupo libre en X denotado por F es no conmutativo (no abeliano).

Demostración. Como $|X| \geq 2$ entonces existen $x, y \in X$ con $x \neq y$ y también por la contrucción de F es claro que $x^{-1} \neq y$ y $y^{-1} \neq x$. Consideremos el producto

$$x^{-1} * y^{-1} * x * y,$$

claramente la palabra obtenida es una palabra reducida debido a las razones expuestas al principio de la demostración y además $x^{-1} * y^{-1} * x * y \neq 1$ si multiplicamos por x del lado izquierdo por ambos lados de la expresión y después por y por la izquierda obtenemos que

$$x * y \neq y * x.$$

Es decir, el producto * es no conmutativo. ■

Observación 2.1.5. Sea F un grupo libre en X, con $|X| \geq 2$, entonces para cualquier $x \in F - \{1\}$ se tiene que $|x| > n$ para toda $n \in \mathbb{N}$, es decir todo elemento distinto de la identidad tiene orden infinito.

Demostración. Sea $x \in F - \{1\}$ entonces x tiene la forma $x = x_1^{\delta_1} \cdots x_m^{\delta_m}$ con $x_i \in X$ y $\delta_i = \pm 1$. Supongamos que $x^n = 1$ para alguna $n \in \mathbb{N}$, eso significa que

$$\begin{aligned} x^n &= \left(x_1^{\delta_1} \cdots x_m^{\delta_m}\right)^n \\ &= \underbrace{\left(x_1^{\delta_1} \cdots x_m^{\delta_m}\right) * \cdots * \left(x_1^{\delta_1} \cdots x_m^{\delta_m}\right)}_{n \text{ veces}} \\ &= 1. \end{aligned}$$

Esto quiere decir que:

- Si m es par entonces $x_k^{\delta_k} = x_{k+1}^{-\delta_{k+1}}$ con $1 \leq k \leq m-1$, lo cual es una contradicción al hecho de que x es una palabra reducida.
- Si m es impar y n es par entonces $x_k^{\delta_k} = x_k^{-\delta_k}$ con $1 \leq k \leq m$. Lo cual es una contradicción al hecho de que X y X^{-1} son ajenos.
- Si m es impar y n es impar entonces $x_k^{\delta_k} = 1$ con $1 \leq k \leq m$, lo cual es una contradicción al hecho de que x es una palabra reducida.

La contradicción viene de suponer que existe $n \in \mathbb{N}$ tal que $x^n = 1$, de aquí que para toda $n \in \mathbb{N}$ y para cualquier $x \in F - \{1\}$ se tiene que $x^n \neq 1$. Por tanto

$$|x| > n \text{ para toda } n \in \mathbb{N}.$$

■

2.2. Objetos libres en la categoría GRP

Hay que verificar que el conjunto, junto con las operaciones que acabamos de construir cumple con la Definición 1.6.1, que además por el Teorema 1.6.3 es único en la categoría **GRP**.

Teorema 2.2.1. *Sean F un grupo libre sobre el conjunto X e $\iota : X \to F$ la función inclusión. Si G es un grupo cualquiera y $f : X \to G$ es una función de conjuntos entonces existe un único homomorfismo de grupos $\hat{f} : F \to G$ tal que $\hat{f} \circ \iota = f$. Es decir F es objeto libre en el conjunto X en la categoría* **GRP**.

Demostración. Construyamos $\hat{f}$:

- $\hat{f}(1) = e_G$ y,
- Si $x_1^{\delta_1} \cdots x_n^{\delta_n}$ es una palabra reducida no vacía en X, definimos $\hat{f}(x_1^{\delta_1} \cdots x_n^{\delta_n}) = f(x_1)^{\delta_1} \cdots f(x_n)^{\delta_n}$.

Como G es grupo, f es función y $\delta_i = \pm 1$ entonces si $x_1^{\delta_1} \cdots x_n^{\delta_n} = y_1^{\delta_1} \cdots y_n^{\delta_n}$ son palabras reducidas obtenemos $f(x_1)^{\delta_1} \cdots f(x_n)^{\delta_n} = f(y_1)^{\delta_1} \cdots f(y_n)^{\delta_n}$ por lo tanto $\hat{f}\left(x_1^{\delta_1} \cdots x_n^{\delta_n}\right) = \hat{f}\left(y_1^{\delta_1} \cdots y_n^{\delta_n}\right)$.

De aquí que $\hat{f}$ está bien definida.

Ahora veamos que $\hat{f}$ es homomorfismo de grupos: Consideremos $x_1^{\lambda_1} \ldots x_m^{\lambda_m}$ y $y_1^{\delta_1} \ldots y_n^{\delta_n}$ palabras reducidas en X supongamos sin pérdida de generalidad que $m \leq n$ entonces:

$$\hat{f}\left(x_1^{\lambda_1} \cdots x_m^{\lambda_m} * y_1^{\delta_1} \ldots y_n^{\delta_n}\right) = \begin{cases} \hat{f}\left(x_1^{\lambda_1} \ldots x_{m-k}^{\lambda_{m-k}} y_{k+1}^{\delta_{k+1}} \ldots y_n^{\delta_n}\right) & \text{si} \quad k < m \\ \hat{f}\left(y_{k+1}^{\delta_{k+1}} \ldots y_n^{\delta_n}\right) & \text{si} \quad k = m < n \\ \hat{f}(1) & \text{si} \quad k = m = n \end{cases}$$

$$= \begin{cases} f\left(x_1^{\lambda_1}\right) \cdots f\left(x_{m-k}^{\lambda_{m-k}}\right) f\left(y_{k+1}^{\delta_{k+1}}\right) \cdots f\left(y_n^{\delta_n}\right) & \text{si} \quad k < m \\ f\left(y_{k+1}^{\delta_{k+1}}\right) \cdots f\left(y_n^{\delta_n}\right) & \text{si} \quad k = m < n \\ e_G & \text{si} \quad k = m = n \end{cases}$$

$$= \begin{cases} f\left(x_1^{\lambda_1}\right) \cdots f\left(x_{m-k}^{\lambda_{m-k}}\right) \cdot e_G \cdot f\left(y_{k+1}^{\delta_{k+1}}\right) \cdots f\left(y_n^{\delta_n}\right) & \text{si} \quad k < m \\ e_G \cdot f\left(y_{k+1}^{\delta_{k+1}}\right) \cdots f\left(y_n^{\delta_n}\right) & \text{si} \quad k = m < n \\ e_G & \text{si} \quad k = m = n \end{cases}$$

Sabemos que k es el entero mayor $(0 \leq k \leq m)$ tal que

$$x_{m-j}^{\lambda_{m-j}} = \left(y_{j+1}^{\delta_{j+1}}\right)^{-1} = y_{j+1}^{-\delta_{j+1}},$$

para $j \in \{1, \ldots, k-1\}$ entonces

$$x_m^{\lambda_m} y_1^{\delta_1} = 1, \; x_{m-1}^{\lambda_{m-1}} 1 y_2^{\delta_2} = 1, \; \ldots, \; x_{m-k+1}^{\lambda_{m-k+1}} 1 y_k^{\delta_k} = 1,$$

por lo cual

$$x_{m-k+1}^{\lambda_{m-k+1}} \ldots x_m^{\lambda_m} y_1^{\delta_1} \ldots y_k^{\delta_k} = 1.$$

De aquí que:

$$\begin{aligned}
&f\left(x_1^{\lambda_1}\right)\cdots f\left(x_{m-k}^{\lambda_{m-k}}\right)\cdot e_G\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_{m-k}^{\lambda_{m-k}}\right)\cdot \hat{f}(1)\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_{m-k}^{\lambda_{m-k}}\right)\cdot \hat{f}\left(x_{m-k+1}^{\lambda_{m-k+1}}\ldots x_m^{\lambda_m}y_1^{\delta_1}\ldots y_k^{\delta_k}\right)\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)
\end{aligned}$$

Por definición de $\hat{f}$ obtenemos:

$$\begin{aligned}
&f\left(x_1^{\lambda_1}\right)\cdots f\left(x_{m-k}^{\lambda_{m-k}}\right)\cdot \hat{f}\left(x_{m-k+1}^{\lambda_{m-k+1}}\ldots x_m^{\lambda_m}y_1^{\delta_1}\ldots y_k^{\delta_k}\right)\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_{m-k}^{\lambda_{m-k}}\right)\cdot f\left(x_{m-k+1}^{\lambda_{m-k+1}}\right)\cdots f\left(x_m^{\lambda_m}\right) f\left(y_1^{\delta_1}\right)\cdots f\left(y_k^{\delta_k}\right)\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_m^{\lambda_m}\right) f\left(y_1^{\delta_1}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= \hat{f}\left(x_1^{\lambda_1}\ldots x_m^{\lambda_m}\right)\cdot \hat{f}\left(y_1^{\delta_1}\ldots y_n^{\delta_n}\right)
\end{aligned}$$

De la misma manera obtenemos que

$$x_1^{\lambda_1}\ldots x_m^{\lambda_m}y_1^{\delta_1}\ldots y_k^{\delta_k}=1.$$

$$\begin{aligned}
&e_G\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= \hat{f}\left(x_1^{\lambda_1}\ldots x_m^{\lambda_m}y_1^{\delta_1}\ldots y_k^{\delta_k}\right)\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_m^{\lambda_m}\right)\cdot f\left(y_1^{\delta_1}\right)\cdots f\left(y_k^{\delta_k}\right)\cdot f\left(y_{k+1}^{\delta_{k+1}}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_m^{\lambda_m}\right)\cdot f\left(y_1^{\delta_1}\right)\cdots f\left(y_n^{\delta_n}\right)\\
&= \hat{f}\left(x_1^{\lambda_1}\ldots x_m^{\lambda_m}\right)\cdot \hat{f}\left(y_1^{\delta_1}\ldots y_n^{\delta_n}\right).
\end{aligned}$$

Análogamente si tenemos que

$$x_1^{\lambda_1}\ldots x_m^{\lambda_m}y_1^{\delta_1}\ldots y_n^{\delta_n}=1.$$

$$\begin{aligned}
e_G &= \hat{f}\left(x_1^{\lambda_1}\ldots x_m^{\lambda_m}y_1^{\delta_1}\ldots y_n^{\delta_n}\right)\\
&= f\left(x_1^{\lambda_1}\right)\cdots f\left(x_m^{\lambda_m}\right)\cdot f\left(y_1^{\delta_1}\right)\cdots f\left(y_m^{\delta_m}\right)\\
&= \hat{f}\left(x_1^{\lambda_1}\ldots x_m^{\lambda_m}\right)\cdot \hat{f}\left(y_1^{\delta_1}\ldots y_n^{\delta_n}\right).
\end{aligned}$$

De aquí que para cualesquiera $x_1^{\lambda_1} \dots x_m^{\lambda_m}$ y $y_1^{\delta_1} \dots y_n^{\delta_n}$ palabras reducidas en X

$$\hat{f}\left(x_1^{\lambda_1} \cdots x_m^{\lambda_m} * y_1^{\delta_1} \dots y_n^{\delta_n}\right) = \hat{f}\left(x_1^{\lambda_1} \dots x_m^{\lambda_m}\right) \cdot \hat{f}\left(y_1^{\delta_1} \dots y_n^{\delta_n}\right).$$

Por lo tanto $\hat{f}$ es un homomorfismo de grupos.

Para ver que es único, consideremos a $g : F \to G$ homomorfismo de grupos tal que $g \circ \iota = f$ y $x_1^{\lambda_1} \dots x_m^{\lambda_m}$ una palabra reducida en X entonces:

$$\begin{aligned} g\left(x_1^{\lambda_1} \dots x_m^{\lambda_m}\right) &= g\left(x_1^{\lambda_1}\right) \dots g\left(x_m^{\lambda_m}\right) \\ &= g(x_1)^{\lambda_1} \dots g\left(x_m\right)^{\lambda_m} \\ &= g \circ \iota(x_1)^{\lambda_1} \dots g \circ \iota\left(x_m\right)^{\lambda_m} \\ &= f(x_1)^{\lambda_1} \dots f\left(x_m\right)^{\lambda_m} \\ &= \hat{f}\left(x_1^{\lambda_1} \dots x_m^{\lambda_m}\right). \end{aligned}$$

Por lo tanto $\hat{f}$ es única. ■

Con este resultado es fácil observar que si tenemos un grupo G y construyendo de manera adecuada al grupo libre F:

Corolario 2.2.2. *Para todo grupo G existe $\hat{f} : F \to G$ morfismo suprayectivo tal que F es libre. Es decir, todo grupo G es la imagen bajo un homomorfismo de un grupo libre F.*

Demostración. Consideremos a X un conjunto de generadores del grupo G y sea F el grupo libre sobre el conjunto X. Por el Teorema 2.2.1 la función inclusión de X en G induce un homomorfismo $\hat{f} : F \to G$ tal que $\hat{f}(s) = s$ para todo elemento $s \in G$. Como $G = \langle X \rangle$ entonces

$$Im(\hat{f}) = \hat{f}[F] = \hat{f}\left[\langle X \rangle\right] = \langle X \rangle = G.$$

■

2.3. Generadores, relaciones y presentaciones

Con el resultado anterior podemos deducir fácilmente usando el Primer Teorema de Isomorfismo la siguiente:

Observación 2.3.1. Si G es un grupo entonces

$$G \cong F/N.$$

Donde $G = \langle X \rangle$, F es el grupo libre en X y N es el núcleo del morfismo suprayectivo $\bar{f} : F \to G$ del Corolario 2.2.2.

La demostración de esta observación se omitirá ya que es clara.

En este orden de ideas, para poder describir a un grupo G (salvo isomorfismos), necesitaríamos determinar el conjunto X, construir al grupo F y determinar a N.

Supongamos que $w = x_1^{\delta_1} \dots x_n^{\delta_n} \in F$ es un generador de N, entonces usando el morfismo suprayectivo natural

$$w \mapsto x_1^{\delta_1} \cdots x_n^{\delta_n} = e_G.$$

La ecuación

$$x_1^{\delta_1} \cdots x_n^{\delta_n} = e$$

en G es llamada **relación** de los generadores x_i. Dadas estas observaciones es claro que un grupo se puede describir completamente dando únicamente el conjunto X de generadores de G y un conjunto adecuado R de relaciones de estos generadores. Claramente esta manera de describir al grupo G no es única ya que hay muchas posibilidades para elegir tanto a X como a R para un grupo G.

Ejemplo 2.3.2. Para ilustrar esto último basta considerar al grupo cíclico de orden 6 $\mathbb{Z}_6$ por un lado y por otro a $\mathbb{Z}_2 \times \mathbb{Z}_3$ que es isomorfo al grupo G definido por $X = \{a, b\}$ y $R = \{a^2 = b^3 = a^{-1}b^{-1}ab = e\}$ bajo el isomorfismo $\varphi : G \to \mathbb{Z}_2 \times \mathbb{Z}_3$ dado por

$$\varphi(g) = \begin{cases} (1,0) & \text{si} \quad g = a \\ (0,1) & \text{si} \quad g = b \end{cases}$$

Es claro que:

$$\begin{aligned} (1,0) + (1,0) &= (0,0) \\ (0,1) + (0,1) + (0,1) &= (0,0) \\ (1,0) + (0,2) + (1,0) + (0,1) &= (0,0) \end{aligned}$$

Es decir que en $\mathbb{Z}_2 \times \mathbb{Z}_3$ se cumplen las relaciones de los generadores $(1,0)$ y $(0,1)$.

Y es claro que como $(2,3) = 1$ entonces $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Pero $\mathbb{Z}_6$ es isomorfo al grupo generado por $X = \{c\}$ con $R = \{c^6 = e\}$. De esta manera tenemos dos maneras de representar al grupo cíclico de orden 6 por medio de un conjunto de generadores y un conjunto de relaciones.

Por otro lado, supongamos que tenemos los conjuntos X y Y de palabras reducidas de elementos de X. La pregunta natural que surge es ¿Existe un grupo G tal que G es generado por X y todas las relaciones $w = e$ $(w \in Y)$ que son válidas (si $w = x_1^{\delta_1} \dots x_n^{\delta_n}$ entonces $w = e$ representará $x_1^{\delta_1} \cdots x_n^{\delta_n} = e$ el producto en G)? Es claro que esto es cierto, de hecho esto nos permite tener en G elementos de X que son iguales. Este hecho se da ya que si $a, b \in X$ y $a^1 b^{-1}$ es una palabra reducida en Y, entonces cualquier grupo que contiene a, b y satisface la relación $a^1 b^{-1} = e_G$ multiplicando por ambos lados del lado derecho a b obtenemos $a = b$.

Es decir un grupo definido a través de un conjunto de generadores y un conjunto de relaciones siempre existe.

De esta manera, dado un conjunto de generadores X y un conjunto Y de palabras reducidas con elementos de X, podemos construir un grupo de la siguiente manera:

- ★ Consideremos F el grupo libre en X y N el subgrupo normal de F generado por Y (el subgrupo normal generado por un conjunto $S \subseteq F$ es la intersección de todos los subgrupos normales de F que contienen a S.)

- ★ Sea $G = F/N$ e identifiquemos a X con su imágen en F/N bajo la función
$$X \subseteq F \to F/N.$$
Como ya se señaló en párrafos anteriores, esto requerirá identificar elementos de X con otros elementos de X.

- ★ G es el grupo generado por X y construyendo las relaciones $w = e$ que se satisfacen para $w \in Y$. (Si $w = x_1^{\delta_1} \dots x_n^{\delta_n}$ es un elemento de Y entonces como N es el grupo normal de F generado por Y tenemos que $x_1^{\delta_1} \dots x_n^{\delta_n} \in N$ como $w = e$ tenemos que $wN = N$ sustituyendo el valor de w y usando las propiedades de clases laterales obtenemos que $x_1^{\delta_1} N \dots x_n^{\delta_n} N = N$ es decir $x_1^{\delta_1} \dots x_n^{\delta_n} = e$ en $G = F/N$.)

Definición 2.3.3. Sean X un conjunto y Y un conjunto de palabras reducidas en X. Un grupo G se dice que es un **grupo definido por los generadores** $x \in X$ **y las relaciones** $w = e$ para $w \in Y$ siempre que

$$G \cong F/N.$$

Considerando a F el grupo libre en X y N el subgrupo normal de F generado por Y. Decimos que $(X|Y)$ es una **presentación** de G.

Ejemplo 2.3.4.

1. Ya se observó en 2.3.2 que $\mathbb{Z}_6$ puede expresarse usando un conjunto de generadores y un conjunto de relaciones:
   - $X = \{a, b\}$ y $R = \{a^2 = b^3 = a^{-1}b^{-1}ab = e\}$.
   - $X = \{c\}$ y $R = \{c^6 = e\}$.
2. Para $n \in \mathbb{N}$ el grupo $\mathbb{Z}_n$ es isomorfo a un grupo que se define con un conjunto de generadores $X = \{a\}$ y un conjunto de relaciones $R = \{a^n = e\}$.

Aunque ya vimos que siempre es posible obtener un grupo a través de un conjunto de generadores X y un conjunto de relaciones R podemos mejorar esta descripción demostrando que el grupo obtenido con estos conjuntos es el mayor en cierto sentido, veamos en qué sentido.

Teorema 2.3.5. *(**Van Dyck**) Sean X un conjunto, Y un conjunto de palabras reducidas en X y G el grupo definido por los generadores $x \in X$ y las relaciones $w = e$ con $w \in Y$. Si H es un grupo tal que $H = \langle X \rangle$ y H satisface todas las relaciones $w = e$ para $w \in Y$, entonces existe un epimorfismo $G \to H$.*

Demostración. Sea F el grupo libre en X, entonces la función inclusión $\iota : X \to H$ induce un isomorfismo φ por el Corolario 2.2.2. Como H satisface las relaciones $w = e$ con $w \in Y$ entonces $w \in Nuc(\varphi)$ por tanto $Y \subseteq Nuc(\varphi)$.

Con esto el subgrupo normal N generado por Y en F cumple que

$$N \subseteq Nuc(\varphi).$$

En Teoría de Grupos se ve que si $f : G \to H$ es un homomorfismo de grupos, $N \trianglelefteq G$, $M \trianglelefteq H$ y $f[N] \leq M$ entonces f induce un isomorfismo $\bar{f} : G/N \to H/M$, dado por

$$\bar{f}(aN) = f(a)M.$$

De hecho, $\bar{f}$ es isomorfismo si y sólo si $\langle Im(f) \cup M\rangle = H$ y $f^{-1}(M) \subseteq N$. En particular si f es un epimorfismo tal que $f[N] = M$ y $Nuc(f) \subseteq N$ entonces $\bar{f}$ es un isomorfismo.

Aplicando el resultado mencionado se obtiene que φ induce un epimorfismo de $F/N \to H/\{0\}$. Por 2.3.1 tenemos que $G \cong F/N$ y es claro que $H/\{0\} \cong H$ con lo cual:

$$G \overset{\tau}{\cong} F/N \xrightarrow{\bar{\varphi}} H/\{0\} \overset{\sigma}{\cong} H.$$

Con lo anterior es claro que $\sigma \circ \bar{\varphi} \circ \tau : G \to H$ es el epimorfismo buscado. ■

Los ejemplos que se presentan a continuación ilustran la manera única en la cual se dan las presentaciones.

Ejemplo 2.3.6. Sea G el grupo definido por los generadores a, b y las relaciones $a^4 = e$, $a^2b^{-2} = e$ y $abab^{-1} = e$. Sabemos que $\mathcal{Q}_8$ el grupo de cuaterniones de Hamilton es un grupo de orden 8 es generado por los elementos $i,\ j$ satisfacen las relaciones:

$$i^4 = 1,\ i^2j^{-2} = (-1)(-j)^2 = (-1)(-1),\ iji(-j) = k(-ij) = k(-k) = -k^2 = e.$$

Por el Teorema 2.3.5 sabemos que existe un epimorfismo $\varphi : G \to \mathcal{Q}_8$. Por el teorema de cardinalidad de conjuntos de Cantor-Bernstein-Schroeder tenemos que $|G| \geq |\mathcal{Q}_8| = 8$.

Consideremos a F el grupo libre en $X = \{a,\ b\}$ y al grupo normal $N = \langle\{a^4, a^2b^{-2}, abab^{-1}\}\rangle$ (N es un grupo normal, ya que $aN = \langle\{a\}\rangle$), es claro que los elementos del grupo cociente son de la forma a^ib^jN con $i \in \{0, \ldots, 3\}$ y $j \in \{0, 1\}$. Por tanto estamos con ello diciendo que hay a lo más 8 clases laterales. De esta manera como por el Teorema 2.3.5 tenemos que $G \cong F/N$ entonces

$$|G| = |F/N| \leq 8.$$

Con ambas desigualdades obtenemos que $|G| = 8$, por lo cual el epimorfismo encontrado arriba φ es en realidad un isomorfismo. Por tanto el grupo definido con $X = \{a,\ b\}$, $R = \{a^4 =\ a^2b^{-2} =\ abab^{-1} = e\}$ es isomorfo a $\mathcal{Q}_8$.

Ejemplo 2.3.7. Todo grupo libre F en el conjunto X es el grupo definido por los generadores $x \in X$ y las relaciones dadas por el conjunto $\emptyset$ (basta recordar que $\langle\emptyset\rangle = \langle e\rangle$).

El término libre proviene de esta libertad de relaciones con la cual se puede expresar este grupo, es decir, libre de relaciones.

Ejemplo 2.3.8. Es claro que todo grupo G no abeliano de orden 6 cumple que

$$G \cong S_3.$$

Esto se cumple ya que sabemos que G contiene elementos $a,\ b$ de órdenes 3 y 2 respectivamente. También es claro que $\langle a \rangle \lhd G$ ya que $[G : \langle a \rangle] = 2$ y por tanto el elemento $bab^{-1} = a$ o $bab^{-1} = a^{-1}$.

Si $bab^{-1} = a$ entonces G es abeliano lo cual no ocurre por hipótesis, por lo tanto $bab^{-1} = a^{-1}$ que es la presentación de D_6 y como $D_6 \cong S_3$ usando a Van Dyck obtenemos un epimorfismo $\varphi : D_6 \to G$. Como ambos grupos tienen el mismo orden entonces φ es un isomorfismo.

2.4. Coproductos o productos libres

Concluiremos este capítulo con la construcción del producto libre que es análoga a la construcción de los grupos libres.

Definición 2.4.1. Sea $\{G_i\}_{i \in I}$ una familia de grupos, supongamos sin pérdida de generalidad que son ajenos dos a dos (sabemos que dada una familia de conjuntos, siempre es posible ajenizarla tal como se mostró en la explicación previa de la Observación 1.4.4.) Consideremos $X = \bigcup_{i \in I} G_i$ y sea $\{1\}$ un conjunto unitario ajeno a X. Definiremos una **palabra** en X como una sucesión $(a_1,\ a_2, \dots)$ tal que $a_i \in X \cup \{1\}$ y para alguna $n \in \mathbb{N}$ se cumple que

$$a_i = 1 \text{ para toda } i \geq n.$$

Una palabra $(a_1,\ a_2, \dots)$ es **reducida** siempre que:

i. Ninguna $a_i \in X$ es el elemento identidad en su respectivo grupo G_j.

ii. Para cualesquiera $i,\ j \geq 1$ se tiene que a_i y a_{i+1} no están en el mismo grupo G_j.

iii. Si $a_k = 1$ entonces $a_i = 1$ para toda $i \geq k$.

En particular $1 = (1,\ 1,\ \dots)$ es reducida. Toda palabra reducida distinta de 1 puede escribirse de manera única como $a_1 a_2 \cdots a_n = (a_1,\ a_2, \dots, a_n,\ 1,\ 1,\ \dots)$ donde $a_i \in X$.

Consideremos el conjunto de todas las palabras reducidas en X y denotémoslo por

$$\prod_{i\in I}^{*} G_i.$$

En caso de que el conjunto de índices sea finito, este producto de denota como $G_1 * G_2 * \cdots * G_n$.

Definición 2.4.2. Al igual que en la construcción de los grupos libres, definiremos el **producto libre** o **coproducto** de la familia $\{G_i\}_{i\in I}$ como: Si $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}$ y $y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}$ son palabras reducidas en $X = \bigcup_{i\in I} G_i$ con $x_i, y_i \in G_i$ y $\lambda_i, \delta_j = \pm 1$ para toda $i,\ j \in I$:

- Si $m \leq n$ entonces consideremos k el entero mayor $(0 \leq k \leq m)$ tal que $x_{m-j}^{\lambda_{m-j}} = \left(y_{j+1}^{\delta_{j+1}}\right)^{-1} = y_{j+1}^{-\delta_{j+1}}$ para $j \in \{1,\ldots,k-1\}$ y consideremos también a l el entero mayor $(0 \leq l \leq m-k)$ tal que $x_{m-s}^{\lambda_{m-s}}, y_{s+1}^{\lambda_{s+1}} \in G_t$ para $s \in \{1,\ldots,k-1\}$ y $t \in I$. Entonces definimos:

$$\left(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}\right)*\left(y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}\right) = \begin{cases} x_1^{\lambda_1}\cdots x_{m-l}^{\lambda_{m-l}}c_l y_{l+1}^{\delta_{l+1}}\cdots y_n^{\delta_n} & si \quad k < m \\ y_{k+1}^{\delta_{k+1}}\cdots y_n^{\delta_n} & si \quad l = k = m < n \\ 1 & si \quad l = k = m = n \end{cases}$$

  Considerando a $c_l = x_{m-l+1}^{\lambda_{m-l+1}}\ldots y_l^{\delta_l}$. De la misma manera:

- Si $m \geq n$ es el caso análogo a la Definición 2.1.3 y al caso anterior.

Es claro que cualquier grupo libre puede ser incluido de manera natural en algún producto libre de grupos donde él se encuentre, es decir:

Observación 2.4.3. Si $\{G_i\}_{i\in I}$ una familia de grupos, el homomorfismo

$$\iota_k : G_k \to \prod_{i\in I}^{*} G_i \text{ dado por } e_{G_k} \mapsto 1 \text{ y } a \mapsto a = (a, 1, 1, \ldots)$$

es un monomorfismo.

Demostración. Es claro que si $k \in I$ y $G_k \in \{G_i\}_{i\in I}$ entonces

$$Nuc\,(\iota_k) = \{\, a \in G_k |\; \iota_k(a) = 1\}\,.$$

Consideremos $a \in Nuc\,(\iota_k)$ entonces aplicando la definición de ι tenemos que

$$\iota_k(a) = (a, 1, 1, \dots).$$

Por otro lado, como $a \in Nuc\,(\iota_k)$ tenemos que

$$\iota_k(a) = 1,$$

también sabemos que la sucesión $(1, 1, \dots)$ corresponde a la palabra vacía denotada por 1. Juntando esta información obtenemos que:

$$(a, 1, 1, \dots) = 1 = (1, 1, 1, \dots).$$

Sabemos que estas dos sucesiones son iguales si y sólo si $a = 1$, con lo cual concluimos que

$$Nuc\,(\iota_k) = \{1_{G_k}\}\,.$$

Y esto es equivalente a que ι_k sea monomorfismo.

■

Teorema 2.4.4. *Sea $\{G_i\}_{i\in I}$ una familia de grupos y $\prod^*_{i\in I} G_i$ su producto libre. Si $\{\psi_i : G_i \to H |\; i \in I\}$ es una familia de homomorfismos, entonces existe un único homomorfismo $\psi : \prod^*_{i\in I} G_i \to H$ tal que $\psi \circ \iota_i = \psi_i$ para cualquier $i \in I$ y esta propiedad determina de manera única a $\prod^*_{i\in I} G_i$ salvo isomorfismos. Esto significa que $\prod^*_{i\in I} G_i$ es el coproducto en la categoría* **GRP** *tal como se definió en 1.4.3.*

Demostración. Consideremos $\{G_i\}_{i\in I}$ una familia de grupos, $\prod^*_{i\in I} G_i$ su producto libre, $\{\psi_i : G_i \to H |\; i \in I\}$ una familia de homomorfismos. Si $a_1 a_2 \dots a_n$ es una palabra reducida en $\prod^*_{i\in I} G_i$ con $a_k \in G_{i_k}$, definamos

$$\psi\,(a_1 a_2 \dots a_n) = \psi_{i_1}\,(a_1)\,\psi_{i_2}\,(a_2) \dots \psi_{i_n}\,(a_n)\,.$$

Veamos que definida así, ψ cumple ser un homomorfismo tal que $\psi \circ \iota_i = \psi_i$ para toda $i \in I$ y es único con esta propiedad.

a. Consideremos $x_1x_2\dots x_m$ y $y_1y_2\dots y_n$ palabras reducidas en $\prod_{i\in I}^{*} G_i$ entonces al calcular

$$\psi\left((x_1x_2\dots x_m)*(y_1y_2\dots y_n)\right),$$

debemos fijarnos en los casos de la Definición 2.4.2 y retomando esa misma notación, denotemos $x_i = x_i^{\lambda_i}$ y a $y_j = y_j^{\delta_j}$ con $\lambda_i, \delta_j \in \pm 1$ para cualesquiera $1 \leq i \leq n$ y $1 \leq j \leq m$.

- Si $m \leq n$ consideremos k el entero mayor $(0 \leq k \leq m)$ tal que $a_{m-j}^{\lambda_{m-j}} = \left(b_{j+1}^{\delta_{j+1}}\right)^{-1} = b_{j+1}^{-\delta_{j+1}}$ para $j \in \{1,\dots,k-1\}$ y consideremos también a l el entero mayor $(0 \leq l \leq m-k)$ tal que $a_{m-s}^{\lambda_{m-s}}, b_{s+1}^{\lambda_{s+1}} \in G_t$ para $s \in \{1,\dots,k-1\}$ y $t \in I$. Entonces si $c_l = x_{m-l+1}^{\lambda_{m-l+1}}\dots y_l^{\delta_l}$, calculemos:
  i. $\psi\left(\left(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}\right)*\left(y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}\right)\right) = \psi\left(x_1^{\lambda_1}\cdots x_{m-l}^{\lambda_{m-l}}c_l y_{l+1}^{\delta_{l+1}}\cdots y_n^{\delta_n}\right)$ si $l < k < m$
  ii. $\psi\left(\left(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}\right)*\left(y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}\right)\right) = \psi\left(y_{k+1}^{\delta_{k+1}}\cdots y_n^{\delta_n}\right)$ si $l = k = m < n$
  iii. $\psi\left(\left(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}\right)*\left(y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}\right)\right) = \psi(1)$ si $l = k = m = n$

  Aplicando la definición que dimos de ψ obtenemos:
  i. $\psi\left(x_1^{\lambda_1}\cdots x_{m-l}^{\lambda_{m-l}}c_l y_{l+1}^{\delta_{l+1}}\cdots y_n^{\delta_n}\right) =$
  $\psi_{i_1}\left(x_1^{\lambda_1}\right)\dots\psi_{i_{m-l}}\left(x_{m-l}^{\lambda_{m-l}}\right)\psi_{i_l}\left(c_l\right)\psi_{i_{l+1}}\left(y_{l+1}^{\delta_{l+1}}\right)\dots\psi_{i_n}\left(y_n^{\delta_n}\right)$ si $l < k < m$.
  ii. $\psi\left(y_{k+1}^{\delta_{k+1}}\cdots y_n^{\delta_n}\right) = \psi_{i_{k+1}}\left(y_{k+1}^{\delta_{k+1}}\right)\dots\psi_{i_n}\left(y_n^{\delta_n}\right)$ si $l = k = m < n$.
  iii. $\psi(1) = \psi_i(1) = 1$ para toda $i \in I$ y considerando a $l = k = m = n$.

  Por otro lado, calculemos $\psi\left(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m}\right)*\psi\left(y_1^{\delta_1}y_2^{\delta_2}\cdots y_n^{\delta_n}\right)$ que por la manera en la que definimos a ψ obtenemos:

  $$\left(\psi_{i_1}\left(x_1^{\lambda_1}\right)\psi_{i_2}\left(x_2^{\lambda_2}\right)\cdots\psi_{i_m}\left(x_m^{\lambda_m}\right)\right)*\left(\psi_{j_1}\left(y_1^{\delta_1}\right)\psi_{j_2}\left(y_2^{\delta_2}\right)\cdots\psi_{j_n}\left(y_n^{\delta_n}\right)\right)$$

  Sabemos que $\psi_i : G_i \to H$ son homomorfismos para cualquier $i \in I$, entonces si:

i. $l < k < m$, considerando k el entero mayor $(0 \leq k \leq m)$ tal que $\psi_{m-j}\left(a_{m-j}^{\lambda_{m-j}}\right) = \psi_{j+1}\left(\left(b_{j+1}^{\delta_{j+1}}\right)^{-1}\right) = \left(\psi_{j+1}\left(b_{j+1}^{\delta_{j+1}}\right)^{-1}\right)$ para $j \in \{1, \ldots, k-1\}$ y l el entero mayor $(0 \leq l \leq m-k)$ tal que $a_{m-s}^{\lambda_{m-s}}, b_{s+1}^{\lambda_{s+1}} \in G_t$ para $s \in \{1, \ldots, k-1\}$ y $t \in I$. Entonces como $\psi_i : G_i \to H$ son homomorfismos para cualquier $i \in I$ obtenemos que $\psi_{m-l+1} = \cdots = \psi_l$ ya que $x_{m-l+1}, \ldots, y_l \in G_l$ para alguna $l \in I$ y de esta manera:

$$\psi_{m-l+1}\left(x_{m-l+1}^{\lambda_{m-l+1}}\right) \ldots \psi_l\left(y_l^{\delta_l}\right) = \psi_l\left(x_{m-l+1}^{\lambda_{m-l+1}} \ldots y_l^{\delta_l}\right) = \psi_l\left(c_l\right).$$

Entonces si calculamos:

$$\psi\left(x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}\right) * \psi\left(y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}\right),$$

obtenemos, usando la definición de ψ y los argumentos anteriores:

$$\psi_{i_1}\left(x_1^{\lambda_1}\right) \ldots \psi_{i_{m-l}}\left(x_{m-l}^{\lambda_{m-l}}\right) \psi_{i_l}\left(c_l\right) \psi_{i_{l+1}}\left(y_{l+1}^{\delta_{l+1}}\right) \ldots \psi_{i_n}\left(y_n^{\delta_n}\right).$$

Que es justamente

$$\psi\left(\left(x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}\right) * \left(y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}\right)\right).$$

Con esto concluimos que ψ es un homomorfismo.

ii. $l = k = m < n$ hacemos las consideraciones análogas al caso anterior y obtenemos que:

$$\psi_{m-j}\left(x_{m-j}^{\lambda_{m-j}}\right) = \psi_{j+1}\left(y_{j+1}^{\delta_{j+1}}\right)^{-1}$$

para toda $1 \leq j \leq k = m$. Con esto y aplicando la definición que dimos de ψ obtenemos que

$$\psi\left(x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}\right) * \psi\left(y_1^{\delta_1} y_2^{\delta_2} \cdots y_n^{\delta_n}\right) =$$

$$\left(\psi_1\left(x_1^{\lambda_1}\right) \psi_2\left(x_2^{\lambda_2}\right) \cdots \psi_m\left(x_m^{\lambda_m}\right)\right) * \left(\psi_1\left(y_1^{\delta_1}\right) \psi_2\left(y_2^{\delta_2}\right) \cdots \psi_n\left(y_n^{\delta_n}\right)\right) =$$

$$\psi_{i_{k+1}}\left(y_{k+1}^{\delta_{k+1}}\right) \ldots \psi_{i_n}\left(y_n^{\delta_n}\right).$$

Con lo cual concluimos que ψ es homomorfismo.

iii. De manera análoga al inciso anterior obtenemos que si $l = k = m = n$ entonces ψ es homomorfismo.

- De manera análoga se obtiene el caso $m \geq n$

b. Veamos que ψ cumple la propiedad

$$\psi \circ \iota_i = \psi_i.$$

Consideremos $x_i \in G_i$ y calculemos usando el hecho de que ι_i es homomorfismo de grupos para cualquier $i \in I$ según la Observación 2.4.3:

$$\begin{aligned}(\psi \circ \iota_i)(x_i) &= \psi(\iota_i(x_i)) \\ &= \psi((x_i, 1, 1, \dots)) \\ &= \psi(x_i) \\ &= \psi_i(x_i).\end{aligned}$$

c. La demostración de que ψ es único con esta propiedad es la misma que la realizada en el Teorema 1.4.5.

■

Capítulo 3

Módulos

Los módulos sobre un anillo son la generalización de los grupos abelianos (que son módulos sobre $\mathbb{Z}$). En este capítulo se verán los conceptos básicos sobre módulos y se dará la generalización del concepto de grupo libre pero en módulo.

3.1. Módulos y homomorfismos

Definición 3.1.1. Sea R un anillo. Un R **-módulo izquierdo (derecho)** es un grupo abeliano aditivo M equipado con una función **multiplicación por escalares** $R \times M \to M$ $(M \times R \to M)$ denotada por

$$(r, a) \mapsto ra \ ((a, r) \mapsto ar)$$

tal que cumple las siguientes propiedades para cualesquiera $r, s \in R$ y $a, b \in M$:

(i) $r(a + b) = ra + rb$ ($(a + b)r = ar + br$).

(ii) $(r + s)a = ra + sa$ $(a(r + s) = ar + as)$.

(iii) $r(sa) = (rs)a$ $((as)r = a(sr))$.

Si R tiene elemento unitario 1_R y

(iv) $1_R a = a$ para cualquier $a \in M$,

entonces se dice que M es un R **-módulo unitario izquierdo (derecho)**. En caso de que R sea un anillo con división, entonces el R-módulo unitario izquierdo es llamado **espacio vectorial izquierdo**.

Ejemplo 3.1.2. 1. Todo espacio vectorial sobre un campo F es un F-módulo izquierdo y derecho.

2. Todo grupo abeliano G es un $\mathbb{Z}$-módulo usando las leyes de los exponentes.

3. Todo anillo R es un R-módulo izquierdo o derecho sobre sí mismo definiendo la multiplicación por escalares como la multiplicación usual en R. De hecho, todo ideal izquierdo o derecho I de R es un R-módulo izquierdo o derecho respectivamente.

4. Si S es un subanillo de un anillo R, entonces R es un S-módulo con la multiplicación usual.

5. Si G es un grupo abeliano y $End(G)$ su anillo de endomorfismos, entonces G es $End(G)$-módulo definiendo la multiplicación por escalares $\cdot : End(G) \times G \to G$ por

$$f \cdot a = f(a) \text{ para cualesquiera } a \in G \text{ y } f \in End(G).$$

NOTACIÓN : Es conveniente, con el ánimo de hacer más fluida la lectura, hacer uso de la notación habitual para los R-módulos.

- Si M es un R-módulo izquierdo se denotará como

$$_RM.$$

- Si M es un R-módulo derecho se denotará como

$$M_R.$$

- Si M es un R-módulo derecho e izquierdo se denotará como

$$_RM_R.$$

Construyamos un módulo a partir de espacios vectoriales y esto nos permitirá dominar la Definición 3.1.1:

Observación 3.1.3. Si V es un F-espacio vectorial de dimensión finita y $T : V \to V$ una transformación lineal, entonces V es un $F[x]$-módulo izquierdo y es denotado por V^T.

Demostración. Definamos la multiplicación por escalares como la función

$$\cdot : F[x] \times V \to V$$

definida por: Si $f(x) \in F[x]$ está dado por $f(x) = \sum_{i=0}^{m} \alpha_i x^i$ y $v \in V$ entonces

$$f(x) \cdot v = \left(\sum_{i=0}^{m} \alpha_i x^i \right) \cdot v = \sum_{i=0}^{m} \alpha_i T^i(v).$$

Aquí hay que considerar que $T^0 = Id_V$ y que recursivamente se define T^i para $i \geq 1$ como $T^i = T \circ T^{i-1}$. Es claro que:

- Si $v, w \in V$ y $f(x) = \sum_{i=0}^{m} \alpha_i x^i \in F[x]$ entonces como T es lineal obtenemos que:

$$\begin{aligned} f(x) \cdot (v + w) &= \sum_{i=0}^{m} \alpha_i T^i(v + w) \\ &= \sum_{i=0}^{m} \alpha_i \left(T^i(v) + T^i(w) \right) \\ &= \sum_{i=0}^{m} \left(\alpha_i T^i(v) + \alpha_i T^i(w) \right) \\ &= \sum_{i=0}^{m} \alpha_i T^i(v) + \sum_{i=0}^{m} \alpha_i T^i(w) \\ &= f(x) \cdot v + f(x) \cdot w. \end{aligned}$$

- Si $v \in V$ y $f(x), g(x) \in F[x]$ con $f(x) = \sum_{i=0}^{m} \alpha_i x^i$ y $g(x) = \sum_{i=0}^{n} \beta_i x^i$ (supondremos sin pérdida de generalidad que $m \leq n$ y para $m < k \leq n$

consideraremos $\alpha_k = 0$) entonces como T es lineal obtenemos que:

$$\begin{aligned}
(f(x)+g(x))\cdot v &= \left(\sum_{i=0}^{m}\alpha_i x^i + \sum_{i=0}^{n}\beta_i x^i\right)\cdot v \\
&= \left(\sum_{i=0}^{n}(\alpha_i+\beta_i)\,x^i\right)\cdot v \\
&= \sum_{i=0}^{n}(\alpha_i+\beta_i)\,T^i(v) \\
&= \sum_{i=0}^{n}\left(\alpha_i T^i(v)+\beta_i T^i(v)\right) \\
&= \sum_{i=0}^{n}\alpha_i T^i(v) + \sum_{i=0}^{n}\beta_i T^i(v) \\
&= \sum_{i=0}^{m}\alpha_i T^i(v) + \sum_{i=0}^{n}\beta_i T^i(v) \\
&= f(x)\cdot v + g(x)\cdot v.
\end{aligned}$$

- Si $v \in V$ y $f(x), g(x) \in F[x]$ con $f(x) = \sum_{i=0}^{m}\alpha_i x^i$ y $g(x) = \sum_{i=0}^{n}\beta_i x^i$ entonces como T es lineal:

$$\begin{aligned}
f(x)\cdot(g(x)\cdot v) &= \left(\sum_{i=0}^{m}\alpha_i x^i\right)\cdot\left(\left(\sum_{j=0}^{n}\beta_j x^j\right)\cdot v\right)\\
&= \left(\sum_{i=0}^{m}\alpha_i x^i\right)\cdot\left(\sum_{j=0}^{n}\beta_j T^j(v)\right)\\
&= \sum_{i=0}^{m}\alpha_i T^i\left(\sum_{j=0}^{n}\beta_j T^j(v)\right)\\
&= \sum_{j=0}^{n}\beta_j\left(\sum_{i=0}^{m}\alpha_i T^{i+j}(v)\right)\\
&= \left(\sum_{j=0}^{n}\beta_j\left(\sum_{i=0}^{m}\alpha_i x^{i+j}\right)\right)\cdot v\\
&= \left(\left(\sum_{i=0}^{m}\alpha_i x^i\right)\left(\sum_{j=0}^{n}\beta_j x^j\right)\right)\cdot v\\
&= (f(x)g(x))\cdot v.
\end{aligned}$$

- Como $F[x]$ tiene elemento unitario $1 = \sum_{i=0}^{0} 1x^i$ la función constante entonces si consideramos $v \in V$ obtenemos:

$$\begin{aligned}
1\cdot v &= \left(\sum_{i=0}^{0} 1x^i\right)\cdot v\\
&= \sum_{i=0}^{0} 1T^i(v)\\
&= 1T^0(v)\\
&= Id_V(v)\\
&= v.
\end{aligned}$$

Por lo tanto V es un $F[x]$-módulo izquierdo. ■

Antes de seguir con las definiciones básicas de módulos es importante resaltar el siguiente resultado.

Observación 3.1.4. Sea R un anillo, entonces cualquier grupo G es un R-módulo izquierdo (derecho).

Demostración. Definamos la multiplicación por escalares $\cdot : R \times G \to G$ ($\cdot : G \times R \to G$) como:

$$r \cdot g = 0 \text{ para cualesquiera } r \in R \text{ y } g \in G.$$

(Análogamente se define $g \cdot r = 0$ para cualesquiera $r \in R$ y $g \in G$). Con esto es claro que para cualquier grupo G y cualquier anillo R,

$$G \text{ es un } R\text{-módulo.}$$

■

Es importante definir la noción de homomorfismo en estas estructuras:

Definición 3.1.5. Si R es un anillo y ${}_RM$, ${}_RN$ son R-módulos izquierdos, entonces una función $f :_R M \to_R N$ es un R-**homomorfismo de R-módulos** si para cualesquiera $m_1, m_2 \in M$ y toda $r \in R$ se cumple que

$$f(m_1 + m_2) = f(m_1) + f(m_2) \text{ y } f(rm_1) = rf(m_1).$$

Si R es un anillo con división, entonces un R-homomorfismo de R-módulos es llamado **transformación lineal**.

Cuando el contexto es claro, los R-homomorfismos de R-módulos se llamarán simplemente homomorfismos.

Observación 3.1.6. Si ${}_RM$ y ${}_RN$ son R-módulos y $f :_R M \to_R N$ es un homomorfismo entonces f es un homomorfismo de los grupos abelianos aditivos M y N.

Debido a esto, se usa la misma terminología usada en grupos:

Definición 3.1.7. Si ${}_RM$ y ${}_RN$ son R-módulos y $f :_R M \to_R N$ es un homomorfismo entonces:

i. Si f es inyectiva, f se conoce como R-**monomorfismo**.

ii. Si f es suprayectiva, f se conoce como R-**epimorfismo**.

iii. Si f es biyectiva, f se conoce como **R-isomorfismo** y cuando entre dos R-módulos M y N hay un isomorfismo f se dice que son **isomorfos** y se denota como

$$M \overset{f}{\cong} N.$$

También en analogía a los resultados de homomorfismos de grupos se obtiene:

Definición 3.1.8. Si ${}_RM$ y ${}_RN$ son R-módulos y $f :_R M \to_R N$ es un homomorfismo entonces se define el **núcleo de** f como:

$$Nuc(f) = \{m \in M | f(m) = 0_N\}.$$

También se define la **imagen de** f como:

$$Im(f) = \{n \in N | n = f(m) \text{ para } m \in M\}.$$

Teorema 3.1.9. *Si ${}_RM$ y ${}_RN$ son R-módulos y $f :_R M \to_R N$ es un homomorfismo entonces son equivalentes:*

a. f es R-monomorfismo.

b. $Nuc(f) = \{0_M\}$.

Demostración. Si f es R-monomorfismo y $m \in Nuc(f)$ entonces por definición de núcleo y debido a que cualquier R-homomorfismo cumple $f(0_M) = 0_N$ entonces

$$f(m) = 0_N = f(0_M).$$

Como f es monomorfismo concluimos que $m = 0_M$ y por lo tanto

$$Nuc(f) = \{0_M\}.$$

Recíprocamente, si $Nuc(f) = \{0_M\}$ y $f(m_1) = f(m_2)$ para $m_1, m_2 \in M$ entonces $0_M = f(m_1) - f(m_2)$. Por ser f R homomorfismo tenemos que $0_M = f(m_1 - m_2)$. Usando la hipótesis obtenemos que

$$m_1 - m_2 = 0_M.$$

Por lo tanto f es inyectiva y de esta manera f es monomorfismo. ■

Teorema 3.1.10. *Si ${}_RM$ y ${}_RN$ son R-módulos y $f :_R M \to_R N$ es un homomorfismo entonces son equivalentes:*

a. f es R-isomorfismo.

b. Existe un R-homomorfismo de R-módulos $g :_R N \to_R M$ tal que $g \circ f = Id_M$ y $f \circ g = Id_N$.

Demostración. Por ser f isomorfismo de grupos existe su inversa (izquierda y derecha) que es un homomorfismo de grupos que hereda su propiedad de R-homomorfismo con la propiedad deseada. ■

Ejemplo 3.1.11.

1. Como ya vimos los $\mathbb{Z}$-módulos son los grupos abelianos y claramente los $\mathbb{Z}$-homomorfismos son los homomorfismos de grupos.

2. Si M es un R-módulo izquierdo y $r \in R$ entonces la función **multiplicar por** r (también llamada **homotecia por** r)

$$\mu_r : M \to M \text{ dada por } \mu_r(m) = rm,$$

es un R-homomorfismo.

3. Para cualesquiera ${}_RM$ y ${}_RN$ R-módulos la función

$$0 : M \to N \text{ dada por } 0(m) = 0_N \text{ para toda } m \in M$$

es un R-homomorfismo.

Además se puede dar una estructura más amplia a la familia de todos los homomorfismos entre dos R-módulos izquierdos ${}_RM$ y ${}_RN$:

Definición 3.1.12. Sean ${}_RM$ y ${}_RN$ R-módulos izquierdos, entonces

$$Hom_R(M, N) = \{f : M \to N | f \text{ es } R\text{-homomorfismo}\}.$$

Si $f, g \in Hom_R(M, N)$ entonces se definen:

i. Una suma

$$+ : Hom_R(M, N) \times Hom_R(M, N) \to Hom_R(M, N) \text{ dada por:}$$

$$(f + g)(m) = f(m) + g(m) \text{ para cualquier } m \in M.$$

ii. Una multiplicación por escalares

$$\cdot : R \times Hom_R(M,N) \to Hom_R(M,N) \text{ dada por:}$$

$$(r \cdot f)(m) = f(rm) \text{ para cualquier } m \in M.$$

Dadas estas operaciones, podemos demostrar:

Teorema 3.1.13. *Si R es anillo conmutativo con unitario, ${}_RM$, ${}_RN$ R-módulos izquierdos entonces*

$$Hom_R(M,N) \text{ es } R\text{-módulo izquierdo.}$$

Demostración. Consideremos $r, s \in R$, $f, g \in Hom_R(M,N)$ y $m \in M$, entonces:

i.

$$\begin{aligned}(r \cdot (f+g))(m) &= (f+g)(rm)\\ &= f(rm) + g(rm)\\ &= (r \cdot f)(m) + (r \cdot g)(m)\\ &= (r \cdot f + r \cdot g)(m).\end{aligned}$$

Por lo tanto

$$r \cdot (f+g) = r \cdot f + r \cdot g.$$

ii. Por ser f homomorfismo se tiene que:

$$\begin{aligned}((r+s) \cdot f)(m) &= f((r+s)m)\\ &= f(rm + sm)\\ &= f(rm) + f(sm)\\ &= r \cdot f(m) + s \cdot f(m)\\ &= (r \cdot f + s \cdot f)(m).\end{aligned}$$

Por lo tanto

$$(r+s) \cdot f = r \cdot f + s \cdot f.$$

iii. Por ser R anillo conmutativo se tiene que:

$$\begin{aligned}((rs)\cdot f)(m) &= f((rs)m)\\ &= f((sr)m)\\ &= f(s(rm))\\ &= s\cdot f(rm)\\ &= r\cdot(s\cdot f(m))\end{aligned}$$

Por lo tanto

$$(rs)\cdot f = r\cdot(s\cdot f).$$

iv. Sea 1_R el elemento unitario de R, entonces

$$\begin{aligned}(1_R\cdot f)(m) &= f(1_R m)\\ &= f(m).\end{aligned}$$

Por lo tanto

$$1_R\cdot f = f.$$

■

Ejemplo 3.1.14. Quizá éste es uno de los ejemplos más conocidos desde los inicios formativos de todos los matemáticos y con el que tenemos una familiaridad mayor debido a su uso: Si V es un F-espacio vectorial entonces

$$Hom_F(V,F) = V^*.$$

El conjunto V^* es conocido como **espacio dual**. De hecho, si consideramos a V de dimensión finita con base $\beta = \{v_1,\ldots,v_n\}$ y si para cada $x\in V$ obtenemos su representación con respecto a la base β

$$x = \sum_{i=1}^{n}\alpha_i v_i,$$

construimos a $\beta^* = \{f_1,\ldots,f_n\}$ donde $f_i\in V^*$ está dada por $f_i(x) = \alpha_i$, esto es, $f_i(v_j) = \delta_{ij}$ para cualquier $v_j\in\beta$, $1\leq j\leq n$. Entonces

$$\beta^* \overset{base}{\hookrightarrow} V^*.$$

De hecho, para cualquier $f \in V^*$ se tiene que

$$f = \sum_{i=1}^{n} f(x_i) f_i.$$

Veamos las subestructuras análogas a los subgrupos pero en módulos:

Definición 3.1.15. Si ${}_RM$ es un R-módulo izquierdo, entonces un **submódulo izquierdo** ${}_RN$ de ${}_RM$ denotado por $N \leq M$ es un subgrupo N de M cerrado bajo la multiplicación escalar, es decir:

$$\text{Para cualquier } n \in N \text{ y } r \in R \text{ se tiene que } rn \in N.$$

La definición de submódulo derecho se hace con la multiplicación escalar del lado derecho.

Ejemplo 3.1.16.

i. Si M es un R-módulo izquierdo, entonces $\{0_M\}$ denotado simplemente por 0 es submódulo de M. Complementariamente se cumple que M es submódulo de M.

   Ambos son conocidos como **submódulos triviales**. Un submódulo N de M tal que $0 \neq N \neq M$ es llamado **submódulo propio no trivial**.

ii. Si consideramos a R como un R módulo sobre sí mismo, entonces cada ideal izquierdo ${}_RI$ de R es submódulo izquierdo, de la misma manera, si I_R es ideal derecho de R entonces I_R es submódulo derecho de R.

iii. En los $\mathbb{Z}$-módulos (los grupos abelianos) los submódulos son los subgrupos.

iv. En la Observación 3.1.3 los submódulos de V^T son precisamente los subespacios W que son T-invariantes (es decir, $T[W] \subseteq W$.)

v. Para R un anillo y $f : M \to N$ un R-homomorfismo de módulos izquierdos, entonces $Nuc(f)$ es submódulo de M y $Im(f)$ es submódulo de N. De hecho,

$$\text{si } P \leq N \text{ entonces } f^{-1}[P] \leq M,$$

   donde $f^{-1}[P] = \{m \in M | f(m) \in P\}$ es la imagen inversa bajo f de P.

vi. Si I es un ideal izquierdo de un anillo R, ${}_RM$ un R módulo y S un subconjunto no vacío de M entonces

$$IS = \left\{ \sum_{i=1}^{n} r_i m_i \middle| \, r_i \in I, \ m_i \in S, n \in \mathbb{N} - \{0\} \right\} \leq M.$$

Teorema 3.1.17. *Sea $\{B_i\}_{i\in I}$ una familia de submódulos de un R-módulo izquierdo M, entonces*

$$\bigcap_{i\in I} B_i \leq M.$$

Demostración. Consideremos $a \in \bigcap_{i\in I} B_i$ y $r \in R$. Sabemos que la intersección de una familia de subgrupos de un grupo dado es un subgrupo, por lo cual solo hay que demostrar que $\bigcap_{i\in I} B_i$ es cerrada bajo la multiplicación escalar.

Como $a \in \bigcap_{i\in I} B_i$ entonces $a \in B_i$ para toda $i \in I$, como $B_i \leq M$ para toda $i \in I$ entonces

$$ra \in B_i \text{ para toda } i \in I.$$

Por lo tanto

$$\bigcap_{i\in I} B_i \leq M.$$

■

Con este sencillo resultado podemos dar lo siguiente:

Definición 3.1.18. Si R es un anillo, M un R-módulo izquierdo y $X \subseteq M$ entonces la intersección de todos los submódulos de M que contienen a X es llamado el **submódulo generado por** X. Se denota este submódulo por

$$\langle X \rangle = \bigcap_{i\in I} \{ N_i \leq M | \, X \subseteq N_i \},$$

donde I es un conjunto de índices.

Es importante hacer las siguientes aclaraciones:

Observación 3.1.19.

i. Si X es un subconjunto finito y $\langle X \rangle = B$ entonces decimos que B es un submódulo **finitamente generado**.

ii. Si $X = \emptyset$ entonces $B = 0$ el submódulo cero.

iii. Si $X = \{a\}$ entonces $\langle X \rangle$ es llamado **submódulo cíclico generado por** a.

iv. Si $\{B_i\}_{i \in I}$ es una familia de submódulos de un R-módulo izquierdo M, entonces el submódulo generado por $X = \bigcup_{i \in I} B_i$ es llamado **suma de los módulos** B_i. Si el conjunto de índices I es finito, entonces la suma de $\{B_1, \ldots, B_n\}$ es denotada por $B_1 + \cdots + B_n$.

Teorema 3.1.20. *Sea R un anillo, M un R-módulo izquierdo, $X \subseteq M$, $\{B_i\}_{i \in I}$ una familia de submódulos M, $m \in M$ y $Rm = \{rm | r \in R\}$. Entonces:*

i. $Rm \leq M$ *y* $\Psi : R \to Rm$ *dada por* $\Psi(r) = rm$ *es un epimorfismo.*

ii. $\langle \{m\} \rangle = Rm$

iii. $\langle X \rangle = \{ \sum_{i=1}^{s} r_i a_i | \; s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R \}$.

iv. $\sum_{i \in I} B_i = \left\{ \sum_{j=1}^{n} b_{i_j} \middle| \, b_{i_k} \in B_{i_k} \right\}$.

Demostración. i. Veamos que $Rm = \{rm | r \in R\}$ es un R-submódulo de M:

a. Primero verifiquemos que Rm es un subgrupo aditivo de M.

- Como $0 \in R$ y M es R-módulo izquierdo entonces $0_R m = 0_M$, por lo cual
$$0_M \in Rm.$$
- Supongamos que $a, b \in Rm$ entonces $a = r_1 m$ y $b = r_2 m$ con $r_1, r_2 \in R$. Si sumamos y aplicamos que $m \in M$ obtenemos: $a + b = r_1 m + r_2 m = (r_1 + r_2)\, m = rm$ con $r \in R$. Por lo tanto:
$$\text{Si } a, b \in Rm \text{ entonces } a + b \in Rm.$$
- Consideremos $a \in Rm$ entonces $a = rm$ para alguna $r \in R$, entonces $-a = (-r)m$ ya que R es un anillo y $0_M = 0_R \cdot m = (r + (-r))m = rm + (-r)m$ por lo cual:
$$\text{Para cualquier } a \in Rm \text{ se cumple que } -a \in Rm.$$

Con esto demostramos que Rm es subgrupo aditivo de M.

b. Veamos que Rm es cerrado bajo la multiplicación por escalares de R. Consideremos $a \in Rm$ y $s \in R$ entonces $sa = s(rm)$ para alguna $r \in R$, además como $m \in M$ y M es módulo izquierdo entonces $s(rm) = (sr)m$ con $sr = t \in R$ por lo cual

$$sa \in Rm.$$

Con esto hemos demostrado que

$$Rm \leq M.$$

Para terminar con este inciso verifiquemos que efectivamente $\Psi : R \to Rm$ dada por $\Psi(r) = rm$ es un epimorfismo. Claramente Ψ es una función además:

a. Si consideramos $r, s \in R$ entonces como M es un R-módulo izquierdo obtenemos:

$$\Psi(r+s) = (r+s)m = rm + sm = \Psi(r) + \Psi(s).$$

b. Si consideramos $r, s \in R$ entonces como M es un R-módulo izquierdo obtenemos:

$$\Psi(rs) = (rs)m = r(sm) = r\Psi(s).$$

Con esto demostramos que

$$\Psi \text{ es un } R \text{ homomorfismo.}$$

Para verificar que efectivamente es suprayectivo, observemos que

$$\Psi[R] = \{\Psi(r) | r \in R\} = \{rm | r \in R\} = Rm.$$

ii. $a \in \langle\{m\}\rangle$ si y sólo si $a \in N \leq M$ para todo $N \leq M$ que cumple $\{m\} \subseteq N$. Esto significa que como $Rm \leq M$ y $\{m\} \subseteq Rm$ entonces $a \in Rm$. Es decir, hemos visto que

$$\langle\{m\}\rangle \subseteq Rm.$$

Para la otra contención, consideremos $a \in Rm$ entonces $a = rm$ para alguna $r \in R$. Si $N \leq M$ tal que $m \in N$ entonces $rm \in N$ por lo tanto $a \in \bigcap_{i\in I} \{ N_i \leq M | \{m\} \subseteq N_i\}$. Esto significa que $a \in \langle \{m\} \rangle$ y con ello hemos demostrado que

$$Rm \subseteq \langle \{m\} \rangle .$$

iii. Sea $m \in \langle X \rangle$, entonces $m \in \bigcap_{i\in I} \{ N_i \leq M | X \subseteq N_i\}$. Esto significa que como

$$\left\{ \sum_{i=1}^{s} r_i a_i \middle| s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R \right\} \leq M$$

y

$$X \subseteq \left\{ \sum_{i=1}^{s} r_i a_i \middle| s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R \right\},$$

entonces $m \in \{ \sum_{i=1}^{s} r_i a_i | \, s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R\}$. Por lo tanto

$$\langle X \rangle \subseteq \left\{ \sum_{i=1}^{s} r_i a_i \middle| s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R \right\}.$$

Recíprocamente, consideremos $m \in \{ \sum_{i=1}^{s} r_i a_i | \, s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R\}$ entonces

$$m = \sum_{i=1}^{s} r_i a_i \text{ con } a_i \in X, r_i \in R.$$

Consideremos la familia $\mathscr{A} = \{N \leq M | X \subseteq N\}$ entonces $r_i a_i \in N$ para cualquier $N \in \mathscr{A}$, esto significa que $\sum_{i=1}^{s} r_i a_i \in N$ para cualquier $N \in \mathscr{A}$ y por lo tanto $\sum_{i=1}^{s} r_i a_i \in \bigcap_{i\in I} \{ N_i \leq M | X \subseteq N_i\} = \langle X \rangle$ para algún conjunto de índices I. Con lo que demostramos que

$$\left\{ \sum_{i=1}^{s} r_i a_i \middle| s \in \mathbb{N} - \{0\}; a_i \in X, r_i \in R \right\} \subseteq \langle X \rangle .$$

iv. Este inciso se sigue de la definición dada en la Observación 3.1.19 en el inciso *iv*. y usando el inciso anterior de esta demostración.

■

Es importante antes de seguir, recordar una definición de teoría de grupos:

Definición 3.1.21. Si X es un conjunto y G es un grupo, entonces G **actúa** en X si existe una función de $G \times X \to X$ (usualmente denotada por $(g, x) \mapsto gx$) tal que para cualesquiera $x \in X$ y $g_1, g_2 \in G$ se cumple:

i. $ex = x$ con e el neutro en G.

ii. $(g_1 g_2)x = g_1(g_2 x)$.

La función dada también se conoce como **acción** del grupo G en el conjunto X. También suele decirse que X es un G**-conjunto**.

Teorema 3.1.22. *Sea N un submódulo de un R-módulo M. Entonces el grupo cociente M/N es un R-módulo con la acción de R en M/N dada por:*

$$r(m + N) = rm + N \text{ para cualesquiera } r \in R \text{ y } m \in M.$$

De hecho, la función $\pi : M \to M/N$ dada por $\pi(m) = m + N$ es un R-epimorfismo con $Nuc(\pi) = N$.

El homomorfismo π es llamado **epimorfismo canónico** ó **proyección**.

Demostración. Como M es un subgrupo abeliano aditivo y $N \trianglelefteq M$ entonces M/N es un grupo abeliano bien definido. Ahora falta ver que con la operación definida esto constituye un R-módulo izquierdo.

Sean $m + N, m' + N \in M/N$ y $r, s \in R$ entonces:

- $$\begin{aligned} r\left((m + N) + (m' + N)\right) &= r\left((m + m') + N\right) \\ &= r(m + m') + N \\ &= (rm + rm') + N \\ &= (rm + N) + (rm' + N). \end{aligned}$$

- $$\begin{aligned} (r + s)(m + N) &= (r + s)m + N \\ &= (rm + sm) + N \\ &= (rm + N) + (sm + N). \end{aligned}$$

- $$\begin{aligned}(rs)(m+N) &= (rs)m+N\\ &= (r(sm))+N\\ &= r(sm+N)\\ &= r(s(m+N))\end{aligned}$$

- $$\begin{aligned}(1_R)(m+N) &= (1_R)m+N\\ &= (m)+N\\ &= m+N.\end{aligned}$$

Resta ver que π es homomorfismo suprayectivo:

- Consideremos $m, m' \in M$ y $r \in R$, entonces

$$\begin{aligned}\pi(m+m') &= (m+m')+N\\ &= (m+N)+(m'+N)\\ &= \pi(m)+\pi(m').\end{aligned}$$

  Además

$$\begin{aligned}\pi(rm) &= (rm)+N\\ &= r(m+N)\\ &= r\pi(m).\end{aligned}$$

  Por lo tanto

$$\pi \text{ es un} R \text{ homomorfismo.}$$

- Es claro que

$$\begin{aligned}\pi[M] &= \{\pi(m)|m \in M\}\\ &= \{m+N|m \in M\}\\ &= M/N.\end{aligned}$$

■

3.2. Teoremas de isomorfismo de módulos

Con los resultados presentados y las definiciones del cociente de módulos podemos presentar las versiones de los tres teoremas de isomorfismo de grupos:

Teorema 3.2.1. Primer Teorema de Isomorfismo. *Si $f : M \to N$ es un R-homomorfismo de módulos entonces existe un R isomorfismo*

$$\Psi : M/Nuc(f) \to Im(f)$$

dado por

$$\Psi(m + Nuc(f)) = f(m).$$

Demostración. Consideremos ${}_RM$ y ${}_RN$ como grupos abelianos y es claro que el isomorfismo que existe entre ellos por el primer teorema de isomorfismo para grupos $\Psi : M/Nuc(f) \to Im(f)$ es también un R-homomorfismo ya que para $n + M \in M/N$ y $r \in R$ se tiene que como f es R-homomorfismo entonces:

$$\begin{aligned}\Psi(r(m+N)) &= \Psi(rm+N)\\ &= f(rm)\\ &= rf(m)\\ &= r\Psi(m+N).\end{aligned}$$

■

Teorema 3.2.2. Segundo Teorema de Isomorfismo *Si $S, T \leq M$ con M R-módulo izquierdo, entonces*

$$S/(S \cap T) \cong (S + T)/T.$$

Demostración. Sea $\pi : M \to M/T$ el epimorfismo canónico definido en el Teorema 3.1.22, entonces $Nuc(\pi) = T$. Definamos $h = \pi|_S$ la restricción de π al conjunto S, entonces $h : S \to M/T$ y es claramente un R-homomorfismo..

Observemos que $Nuc(h) = S \cap T$ y $Im(h) = (S + T)/T$, y por el primer teorema de isomorfismo 3.2.1 tenemos que existe un R-isomorfismo $\Psi : S/Nuc(h) \to Im(h)$ es decir existe un R-isomorfismo $\Psi : S/(S \cap T) \to (S + T)/T$, por lo cual

$$S/(S \cap T) \cong (S + T)/T.$$

■

Teorema 3.2.3. Tercer Teorema de Isomorfismo *Si $T \subseteq S \subseteq M$ es una cadena de submódulos de un R-módulo izquierdo M, entonces*

$$(M/T)/(S/T) \cong M/S.$$

Demostración. Definamos $g : M/T \to M/S$ como el **agrandamiento de clases**, es decir

$$g(m+T) = m+S.$$

Veamos que g está bien definida:

Consideremos $m+T = m'+T \in M/T$, entonces $m-m' \in T$ y por hipótesis $T \subseteq S$, por lo tanto $m+S = m'+S$.

Además g es un R-homomorfismo con:

$$\begin{aligned} Nug(g) &= \left\{m+T \in M/T \,\middle|\, g(m+T) = 0_{M/S}\right\} \\ &= \{m+T \in M/T \,|\, g(m+T) = S\} \\ &= \{m+T \in M/T \,|\, m+S = S\} \\ &= \{m+T \,|\, m \in S\} \\ &= S/T. \end{aligned}$$

También tenemos que

$$\begin{aligned} Im(g) &= \{g(m+T) \,|\, m+T \in M/T\} \\ &= \{m+S \,|\, m \in M\} \\ &= M/S, \end{aligned}$$

Usando el primer teorema de isomorfismo obtenemos que existe un isomorfismo

$$\Psi : (M/T)/Nuc(g) \to Im(g), \text{ es decir } \Psi : (M/T)/(S/T) \to M/S.$$

Por lo tanto

$$(M/T)/(S/T) \cong M/S.$$

■

Observación 3.2.4. Sean M y N R-módulos izquierdos, $S \leq N$ y $f : M \to N$ un R-homomorfismo, entonces

$$f^{-1}[S] \leq M, \text{ con } Nuc(f) \subseteq S.$$

Demostración. Consideremos $t \in f^{-1}[S]$ y $r \in R$, entonces $t \in M$ que además cumple $f(t) \in S$, entonces si hacemos las cuentas:

$$rt \in M \text{ ya que } M \text{ es } R-\text{módulo izquierdo}$$
$$f(rt) = rf(t) \text{ ya que } f \text{ es } R-\text{homomorfismo}$$
$$rf(t) \in S \text{ ya que } S \text{ es } R-\text{submódulo izquierdo.}$$

Por lo tanto,

$$f^{-1}[S] \leq M.$$

Veamos ahora que $Nuc(f) \subseteq S$:

Consideremos $m \in Nuc(f)$, entonces $f(m) = 0_N$ como $S \leq N$ entonces $0_N \in S$ por lo tanto $f(m) \in S$. De aquí que

$$Nuc(g) \subseteq S.$$

■

Teorema 3.2.5. Teorema de la Correspondencia Biyectiva. *Si $T \leq M$ entonces hay una biyección*

$$\phi : \{\text{submódulos intermedios } T \leq S \leq M\} \to \{ \text{ submódulos de } M/T\}$$

dada por

$$S \mapsto S/T.$$

De hecho, $S \leq S' \leq M$ si y sólo si $S/T \leq S'/T \leq M/T$.

Demostración. Como todo R-módulo izquierdo es un grupo abeliano aditivo, entonces todo submódulo es un subgrupo, y por ello podemos usar el teorema de la correspondencia biyectiva para grupos. En él, se demuestra que si se define la función

$$\phi : \{\text{subgrupos intermedios } T \leq S \leq M\} \to \{ \text{ subgrupos de } M/T\}$$

dada por

$$\phi(S) = S/T$$

entonces ϕ es una función biyectiva que preserva inclusiones, es decir $S \subseteq S' \subseteq M$ si y sólo si $S/T \subseteq S'/T \subseteq M/T$. La demostración es completamente análoga a la de grupos.

■

Con todas estas herramientas, es posible dar los productos y coproductos en la categoría ${}_R\mathbf{MOD}$.

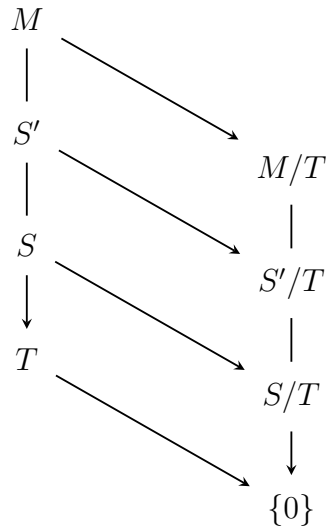


Figura 3.1: Diagrama del **Teorema de la Correspondencia Biyectiva** 3.2.5

3.3. Producto y coproducto de módulos

La noción de suma directa se discute en grupos abelianos, y se extiende a módulos. Un grupo abeliano G es una suma directa de subgrupos S y T si $S + T = G$ y $S \cap T = \{0\}$, mientras una suma directa externa es un grupo abeliano cuyo conjunto subyacente es el producto cartesiano $S \times T$, y cuya operación binaria está dada por la suma coordenada a coordenada, ambas versiones dadas son grupos abelianos isomorfos. La suma interna y externa se conserva en módulos y se verá con más detalle adelante.

Definición 3.3.1. Si S y T son $R-$módulos, donde R es un anillo, su **suma directa**, denotada por $S \sqcup T$, es el producto cartesiano $S \times T$ con operaciones coordenada a coordenada

$$(s,t) + (s',t') = (s+s', t+t');$$

$$r(s,t) = (rs, rt),$$

donde $s, s' \in S$, $t, t' \in T$ y $r \in R$.
Hay $R-$homomorfismos $\lambda_S : S \longrightarrow S \sqcup T$ y $\lambda_T : T \longrightarrow S \sqcup T$, dados, respectivamente, por $\lambda_S : s \longmapsto (s,0)$ y $\lambda_T : t \longmapsto (0,t)$.

Proposición 3.3.2. *Las siguientes afirmaciones son equivalentes para $R-$módulos M,S y T.*

(i) $S \sqcup T \cong M$.

(ii) *Existen $R-$homomorfismos inyectivos $i : S \longrightarrow M$ y $j : T \longrightarrow M$ tales que*

$$M = im\,(i) + im\,(j) \quad \textit{y también} \quad im\,(i) \cap im\,(j) = \{0\}.$$

(iii) *Existen $R-$homomorfismos $i : S \longrightarrow M$ y $j : T \longrightarrow M$ tales que, para cualquier $m \in M$, existen $s \in S$ y $t \in T$ únicos que cumplen:*

$$m = i(s) + j(t).$$

(iv) *Existen $R-$homomorfismos $i : S \longrightarrow M$, $j : T \longrightarrow M$, $p : M \longrightarrow S$, y $q : M \longrightarrow T$ tales que*

$$p \circ i = Id_S,\ q \circ j = Id_T,\ p \circ j = 0,\ q \circ i = 0,\ \textit{y también}\ \ i \circ p + j \circ q = Id_M.$$

Demostración.

$(i) \Rightarrow (ii)$ Sea $\varphi : S \sqcup T \longrightarrow M$ el isomorfismo de la hipótesis, y definamos

$$i = \varphi \circ \lambda_S,$$

con $\lambda_S : S \to S \sqcup T$ dada por $\lambda_S(s) = (s, 0)$ y

$$j = \varphi \circ \lambda_T$$

con $\lambda_T : T \to S \sqcup T$ dada por $\lambda_T(t) = (0, t)$.

Veamos que definidas de esta manera, estas funciones resultan ser R-homomorfismos inyectivos que cumplen que $M = im\,(i) + im\,(j)$ y también $im\,(i) \cap im\,(j) = \{0\}$:

- Tanto i como j son R-homomorfismos inyectivos ya que son composición de R-homomorfismos inyectivos.

- Consideremos $m \in M$, entonces por hipótesis existe una única pareja ordenada $(s,t) \in S \sqcup T$ tal que $m = \varphi((s,t))$. Por la manera en la que definimos i y j obtenemos:

$$\begin{aligned} m &= \varphi((s,t)) \\ &= \varphi((s,0)+(0,t)) \\ &= (\varphi \circ \lambda_S)(s) + (\varphi \circ \lambda_T)(t) \\ &= \iota(s) + j(t). \end{aligned}$$

Además es claro que $i(s) + j(t) \in im\,(i) + im\,(j)$ por lo cual

$$m \in im\,(i) + im\,(j)\,, \text{ es decir } M \subseteq im(i) + im(j).$$

También es claro que como $i : S \to M$ y $j : T \to M$ entonces $im(i) \subseteq M$ y $im(j) \subseteq M$ por lo cual

$$im(i) + im(j) \subseteq M.$$

Con estas dos contenciones obtenemos que

$$M = im(i) + im(j).$$

Ahora consideremos $x \in im\,(i) \cap im\,(j)$, esto significa que $x \in im(i)$ y $x \in im(j)$. Por la Definición 3.1.8 obtenemos que existen $s \in S$ y $t \in T$ tales que

$$x = i(s) \text{ y } x = j(t).$$

Por la manera en la que se definieron tanto i como j obtenemos:

$$(\varphi \circ \lambda_S)(s) = (\varphi \circ \lambda_T)(t).$$

Como φ es isomorfismo entonces

$$\lambda_S(s) = \lambda_T(t)$$

y por la definición de λ_S y λ_T obtenemos $(s,0) = (0,t)$ en $S \sqcup T$. Por lo tanto, $s = 0 = t$ y con ello $x = 0_{S \sqcup T}$. En conclusión $im\,(\iota) \cap im\,(j) = \{0_{S \sqcup T}\}$.

$(ii) \Longrightarrow (iii)$ Sea $m \in M$, por hipótesis tenemos que $m = i(s) + j(t)$ para $s \in S$ y $t \in T$. Falta demostrar que tanto s como t son únicos.

Para ello, supongamos que $m = i(s) + j(t)$ y $m = i(s') + j(t')$ con $s, s' \in S$ y $t, t' \in T$. Entonces

$$\begin{aligned} 0 &= (i(s) + j(t)) - (i(s') + j(t')) \\ &= i(s - s') - j(t' - t) \end{aligned}$$

y por lo tanto $i(s - s') = j(t' - t)$.

Como $im(i) \cap im(j) = \{0\}$ y $j(t - t') = i(s' - s) \in im(i) \cap im(j)$ entonces $i(s - s') = 0$ y $j(t - t') = 0$. Como i, j son homomorfismos inyectivos entonces $s - s' = 0$ y $t - t' = 0$. Por lo tanto

$$s = s' \text{ y } t = t'.$$

Es decir, dada $m \in M$ existen únicos $s \in S$ y $t \in T$ tales que

$$m = i(s) + j(t).$$

$(iii) \Longrightarrow (iv)$ Sabemos por hipótesis que para cada $m \in M$ existen únicos $s \in S$, $t \in T$ tales que $m = i(s) + j(t)$. Definamos para cada $m \in M$

$$p : M \to S \text{ y } q : M \to T \text{ dadas por:} p(m) = s \text{ y } q(m) = t.$$

Claramente p y q son funciones bien definidas. Veamos que son R-homomorfismos que cumplen las ecuaciones dadas.

- Veamos que p y q son R-homomorfismos. Consideremos $m, m' \in M$ y $r \in R$. Sabemos por hipótesis que existen únicos $s, s' \in S$ y $t, t' \in T$ tales que $m = i(s) + j(t)$ y $m' = i(s') + j(t')$, entonces como i y j son R-homomorfismos tenemos que $m + m' = i(s + s') + j(t + t')$. Luego

$$\begin{aligned} p(m + m') &= s + s' \\ &= p(m) + p(m'). \end{aligned}$$

Y también:

$$\begin{aligned} q(m+m') &= t+t' \\ &= q(m)+q(m'). \end{aligned}$$

Análogamente, si $r \in R$, entonces $rm = r(i(s)+j(t))$ como i y j son R-homomorfismos entonces

$$rm = i(rs)+j(rt).$$

Entonces

$$\begin{aligned} p(rm) &= rs \\ &= rp(m), \end{aligned}$$

y

$$\begin{aligned} q(rm) &= rt \\ &= rq(m). \end{aligned}$$

Por lo tanto p y q son R-homomorfismos.

- Veamos que $p \circ i = Id_S$. Consideremos $s \in S$ entonces:

$$\begin{aligned} (p \circ i)(s) &= p(i(s)) \\ &= p(i(s)+0) \\ &= p(i(s)+j(0)) \\ &= p(m) \text{ con } m = i(s)+j(0) \\ &= s \\ &= Id_S(s). \end{aligned}$$

Por lo tanto

$$p \circ i = Id_S.$$

- Veamos que $q \circ j = Id_T$. Consideremos $t \in T$ entonces:

$$\begin{aligned}(q \circ j)(t) &= q(j(t)) \\ &= q(0 + j(t)) \\ &= q(i(0) + j(t)) \\ &= q(m) \text{ con } m = i(0) + j(t) \\ &= t \\ &= Id_T(t).\end{aligned}$$

  Por lo tanto

$$q \circ j = Id_T.$$

- Veamos que $p \circ j = 0_S$. Consideremos $t \in T$ entonces:

$$\begin{aligned}(p \circ j)(t) &= p(j(t)) \\ &= p(0 + j(t)) \\ &= p(i(0) + j(t)) \\ &= p(m) \text{ con } m = i(0) + j(t) \\ &= 0.\end{aligned}$$

  Por lo tanto

$$p \circ j = 0.$$

- Veamos que $q \circ i = 0$. Consideremos $s \in S$ entonces:

$$\begin{aligned}(q \circ i)(s) &= q(i(s)) \\ &= q(i(s) + 0) \\ &= q(i(s) + j(0)) \\ &= q(m) \text{ con } m = i(s) + j(0) \\ &= 0.\end{aligned}$$

  Por lo tanto

$$q \circ i = 0.$$

- Por último, veamos que $i \circ p + j \circ q = Id_M$. Consideremos $m \in M$, entonces por hipótesis existen únicos $s \in S$ y $t \in T$ tales que $m = i(s) + j(t)$. Por la manera en la que se definieron los homomorfismos p y q tenemos que $m = i(p(m)) + j(q(m))$. Es decir, para cualquier $m \in M$:

$$Id(m) = m = (i \circ p)(m) + (j \circ q)(m) = (i \circ p + j \circ q)(m).$$

Con ello concluimos que

$$Id_M = i \circ p + j \circ q.$$

$(iv) \Longrightarrow (i)$ Definamos $\varphi : S \sqcup T \longrightarrow M$, como $\varphi((s,t)) = i(s) + j(t)$.

- Es claro que φ es un $R-$homomorfismo debido a que i y j lo son y la suma de R-homomorfismos es un R-homomorfismo.

  Veamos que φ es inyectiva y suprayectiva:

- Sea $(s,t) \in Nuc(\varphi)$ entonces

$$\begin{aligned} 0 &= \varphi((s,t)) \\ &= i(s) + j(t) \end{aligned}$$

Además

$$\begin{aligned} s &= p(i(s) + j(0)) \\ &= p(i(s)) \\ &= p(-j(t)) \\ &= -p(j(t)) \\ &= -(p \circ j)(t) \\ &= -0(t) \\ &= 0. \end{aligned}$$

Análogamente

$$\begin{aligned} t &= q(i(0) + j(t)) \\ &= q(j(t)) \\ &= q(-i(s)) \\ &= -q(i(s)) \\ &= -(q \circ i)(s) \\ &= -0(s) \\ &= 0. \end{aligned}$$

Por lo tanto $s = 0_S$ y $t = 0_T$ y así

$$Nuc(\varphi) = \{0_{S \sqcup T}\}.$$

Por el Teorema 3.1.9

$$\varphi \text{ es monomorfismo.}$$

- Para ver que φ es suprayectiva, recordemos que por hipótesis, $1_M = i \circ p + j \circ q$, entonces si $m \in M$

$$\begin{aligned} m &= (i \circ p + j \circ q)(m) \\ &= (i \circ p)(m) + (j \circ q)(m) \\ &= i(p(m)) + j(q(m)) \\ &= i(s) + j(t) \text{ con } s = p(m) \text{ y } t = q(m) \\ &= \varphi((s,t)) \text{ con } s \in S \text{ y } t \in T. \end{aligned}$$

Por lo tanto φ es epimorfismo.

Con ello

$$S \sqcup T \overset{\varphi}{\cong} M.$$

■

Definición 3.3.3. Los homomorfismos i y j del Teorema 3.3.2 son llamados **inclusiones**, y los homomorfismos p y q son llamados **proyecciones**. Las ecuaciones $p \circ i = Id_S$ y $q \circ j = Id_T$ demuestran que los homomorfismos i y j deben ser inyectivos (así que $im(i) \cong S$ y $im(j) \cong T$) y los homomorfismos p y q deben ser suprayectivos.

Definición 3.3.4. Si S y T son submódulos de un R-módulo izquierdo M, entonces M es su **suma directa interna** de S y T si $M \cong S \sqcup T$ con $i : S \to M$ y $j : T \to M$ las inclusiones. Denotaremos la suma directa interna por

$$M = S \oplus T.$$

Sólo en esta parte, usaremos la notación $S \sqcup T$ para denotar la suma directa externa (con conjunto subyacente el producto cartesiano de S y T) y la notación $M = S \oplus T$ para denotar la suma directa interna (S y T submódulos de M).

Corolario 3.3.5. *Son equivalentes para M un R-módulo izquierdo con submódulos S y T:*

(i) $M = S \oplus T$.

(ii) $S + T = M$ *y* $S \cap T = \{0_M\}$.

(iii) Cada $m \in M$ tiene una expresión única de la forma

$$m = s + t \text{ con } s \in S \text{ y } t \in T.$$

Demostración. Usemos el Teorema 3.3.2:

$(i) \Rightarrow (ii)$ Consideremos $M = S \oplus T$, por la Definición 3.3.4 $M \cong S \sqcup T$ y por la observación de la Definición 3.3.3 tenemos que $im(i) \cong S$ e $im(j) \cong T$. En este caso debido a que $S, T \leq M$ tenemos que $im(i) = S$ y que $im(j) = T$. Por el Teorema 3.3.2 se tiene que $M = im(i) + im(j)$ y también $im(i) \cap im(j) = \{0_M\}$. Entonces

$$M = S + T \text{ y } S \cap T = \{0_M\}.$$

$(ii) \Rightarrow (iii)$ Consideremos $S, T \leq {}_RM$ tales que $M = S + T$ y $S \cap T = \{0_M\}$. Consideremos también las inmersiones naturales $i : S \to M$ y $j : T \to M$ dadas por $i(s) = s$ y $j(t) = t$ para cualesquiera $s \in S$ y $t \in T$. Es claro que estamos bajo las hipótesis del inciso (ii) del Teorema 3.3.2, entonces para cada $m \in M$ se tiene que existen únicas $s \in S$ y $t \in T$ tales que:

$$m = i(s) + j(t) = s + t.$$

(iii) Finalmente por hipótesis se tiene que para cualquier $m \in M$, $m = s+t$ con $s \in S$ y $t \in T$ únicos. Es claro que si $m \in S \cap T$ entonces $m = s = s + 0$ y $m = t = 0 + t$ pero como la expresión es única entonces $s = t = 0$ Por lo tanto

$$M = S \oplus T.$$

■

Teorema 3.3.6. *Si M y N son R-módulos izquierdos, entonces su* **coproducto** *existe y es su suma directa $C = M \sqcup N$.*

Demostración. Sea $C = M \sqcup N$. Siguiendo la Definición 1.4.3, es necesario dar momorfismos inyectivos α y β de M a C y de N a C respectivamente. El conjunto subyacente de $C = M \sqcup N$ es el producto cartesiano $M \times N$ y de esta manera definimos

$$\alpha : M \to C \text{ dado por } \alpha(m) = (m, 0)$$

y

$$\beta : N \to C \text{ dado por } \beta(n) = (0, n).$$

Ahora, si X es un R-módulo izquierdo, $f : M \to X$ y $g : N \to X$ R-homomorfismos, entonces definimos

$$\theta : C \to X \text{ dado por } \theta\left((m, n)\right) = f(m) + g(n).$$

Es claro que si $m \in M$ entonces

$$(\theta \circ \alpha)(m) = \theta\left((m, 0)\right) = f(m).$$

De manera análoga, si $n \in N$ entonces

$$(\theta \circ \beta)(n) = \theta\left((0, n)\right) = g(m).$$

Es claro que θ es única ya que si $\Psi : C \to X$ es un R-homomorfismo tal que $\Psi \circ \alpha = f$ y $\Psi \circ \beta = g$ entonces $\Psi\left((m, 0)\right) = f(m)$ y $\Psi\left((0, n)\right) = g(n)$ para toda $m \in M$ y $n \in N$. Como Ψ es un R-homomorfismo entonces

$$\begin{aligned} \Psi\left((m, n)\right) &= \Psi\left((m, 0) + (0, n)\right) \\ &= \Psi\left((m, 0)\right) + \Psi\left((0, n)\right) \\ &= f(m) + g(n). \end{aligned}$$

Por lo tanto $\Psi = \theta$.

■

Los Teoremas 3.3.2, 3.3.6 y el Corolario 3.3.5, nos dan la forma que tiene el coproducto de dos objetos en la categoría ${}_R\mathbf{MOD}$. La pregunta que nos falta responder es ¿Qué es el producto de dos módulos? Para responder esta pregunta demos la siguiente:

Proposición 3.3.7. *Si R es un anillo asociativo con unitario y A, B son R-módulos izquierdos, entonces el producto de la Definición 1.4.1 $A \sqcap B$ existe y de hecho,*

$$A \sqcap B \cong A \sqcup B.$$

Demostración. Por el Teorema 3.3.2 sabemos que si $M \in \mathcal{OB}_{{}_R\mathbf{MOD}}$ es tal que $M \cong A \sqcup B$ entonces existen las inmersiones y las proyecciones $i : A \to M$, $j : B \to M$, $p : M \to A$ y $q : M \to B$ tales que

$$p \circ i = Id_A,\ q \circ j = Id_B,\ p \circ j = 0,\ q \circ i = 0, \text{ y también } \ i \circ p + j \circ q = Id_M.$$

Si $X \in \mathcal{OB}_{{}_R\mathbf{MOD}}$, $f \in Hom(X, A)$ y $g \in Hom(X, B)$ definimos

$$\theta \in Hom(X, A \sqcup B) \text{ como } \theta(x) = (i \circ f)(x) + (j \circ g)(x),$$

ya que

$$\begin{aligned}(p \circ \theta)(x) &= p(\theta(x)) \\ &= p((i \circ f)(x) + (j \circ g)(x)) \\ &= (p \circ i \circ f)(x) + (p \circ j \circ g)(x) \\ &= (Id_A \circ f)(x) + (0 \circ g)(x) \\ &= f(x) + 0 \\ &= f(x),\end{aligned}$$

y también:

$$\begin{aligned}(q \circ \theta)(x) &= q(\theta(x)) \\ &= q((i \circ f)(x) + (j \circ g)(x)) \\ &= (q \circ i \circ f)(x) + (q \circ j \circ g)(x) \\ &= (0 \circ f)(x) + (Id_B \circ g)(x) \\ &= 0 + g(x) \\ &= g(x),\end{aligned}$$

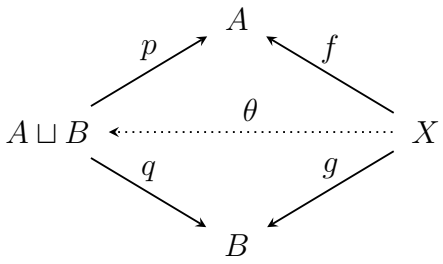


Figura 3.2: Diagrama del producto de A y B.

entonces

$$p \circ \theta = f \text{ y } q \circ \theta = g.$$

Esto significa que el Diagrama 3.2 conmuta.

Debido a que

$$Id_{A \sqcup B} = i \circ p + j \circ q,$$

si existiera $\psi : X \to A \sqcup B$ tal que $p \circ \psi = f$ y $q \circ \psi = g$ obtendríamos

$$\begin{aligned} \psi &= Id_{A \sqcup B} \circ \psi \\ &= (i \circ p + j \circ q) \circ \psi \\ &= (i \circ p) \circ \psi + (j \circ q) \circ \psi \\ &= i \circ (p \circ \psi) + j \circ (q \circ \psi) \\ &= i \circ f + j \circ g \\ &= \theta. \end{aligned}$$

Es decir, θ es única. ■

Extendamos la noción de suma directa de dos módulos a la suma directa de una familia de módulos:

Definición 3.3.8. Si R es un anillo asociativo con unitario, y $\{A_i\}_{i \in I}$ con I un conjunto de índices y A_i R-módulo izquierdo para toda $i \in I$, entonces el **producto directo** denotado por $\prod_{i \in I} A_i$ es el producto cartesiano (es decir, el conjunto de las I-ádas (a_i) cuya i-ésima coordenada $a_i \in A_i$ para toda $i \in I$) con una suma y producto por escalares entrada a entrada. Es decir, para $a_i, b_i \in A_i$ y $r \in R$ se tiene que

$$(a_i) + (b_i) = (a_i + b_i)$$
$$r(a_i) = (ra_i).$$

La **suma directa**, denotada por $\sum_{i\in I} A_i$ (también denotada por $\bigoplus_{i\in I} A_i$), es el un subconjunto de $\prod_{i\in I} A_i$ cuyos elementos son todas las i-ádas (a_i) cuyos elementos no cero forman un conjunto finito.

Teorema 3.3.9. *Sea R un anillo y $\{A_i\}_{i\in I}$ una familia no vacía de R-módulos izquierdos, entonces:*

(i) $\prod_{i\in I} A_i$ *es un R-módulo izquierdo con las operaciones descritas en la Definición 3.3.8.*

(ii) $\sum_{i\in I} A_i$ *es submódulo de* $\prod_{i\in I} A_i$.

(iii) Para cada $k \in I$ la proyección $\pi_k : \prod_{i\in I} A_i \to A_k$ dada por $\pi_k((a_i)) = a_k$ es un R-epimorfismo.

(iv) Para cada $k \in I$ la inclusión $\iota_k : A_k \to \sum_{i\in I} A_i$ dada por $\iota_k(a) = (a_i)$, donde $a_i = 0$ para $i \neq k$ y $a_k = a$ es un R-monomorfismo.

Demostración. (i) Consideremos $r, s \in R$ y $\{a_i\}, \{b_i\} \in \prod_{i\in I} A_i$ entonces:

- $$\begin{aligned} r(\{a_i\} + \{b_i\}) &= r\{a_i + b_i\} \\ &= \{ra_i + rb_i\} \\ &= \{ra_i\} + \{rb_i\} \\ &= r\{a_i\} + r\{b_i\}. \end{aligned}$$

- $$\begin{aligned} (r + s)\{a_i\} &= \{(r + s)a_i\} \\ &= \{ra_i + sa_i\} \\ &= \{ra_i\} + \{sa_i\} \\ &= r\{a_i\} + s\{a_i\}. \end{aligned}$$

- $$\begin{aligned} r(s\{a_i\}) &= r\{sa_i\} \\ &= \{r(sa_i)\} \\ &= \{(rs)a_i\} \\ &= (rs)\{a_i\}. \end{aligned}$$

- $$\begin{aligned} 1_R\{a_i\} &= \{1_R a_i\} \\ &= \{a_i\}. \end{aligned}$$

Por lo tanto $\prod_{i\in I} A_i$ es un R-módulo izquierdo unitario.

(ii) Es claro que si $r \in R$ y $\{a_i\} \in \sum_{i\in I} A_i$ entonces $r\{a_i\} = \{ra_i\}$ con $a_i = 0$ para casi toda $i \in I$, entonces $ra_i = 0$ para casi toda $i \in I$, por lo cual $\{ra_i\} \in \sum_{i\in I} A_i$.

Por lo tanto

$$\sum_{i\in I} A_i \leq \prod_{i\in I} A_i.$$

(iii) Es claro por la definición que π_k es un R-epimorfismo.

(iv) Es claro por la definición que ι_k es un R-monomorfismo.

■

Teorema 3.3.10. *Sea $\{A_i\}_{i\in I}$ una familia no vacía de R-módulos izquierdos entonces*

$$\sum_{i\in I} A_i \text{ es el } \textbf{coproducto} \text{ en } {}_R\mathbf{MOD}.$$

Demostración. Es claro por la Definición 1.4.3 que además de dar la familia $\{A_i\}_{i\in I}$ de R-módulos izquierdos, es necesario dar la familia de los R-homomorfismos (inyectivos) $\left\{\alpha_i : A_i \to \sum_{i\in I} A_i\right\}$. Definamos entonces $\alpha_i : A_i \to \sum_{i\in I} A_i$ dada por $\alpha_i(a_i) = \{\alpha_i(a)\} \in \sum_{i\in I} A_i$ donde si $a_i \in A_i$ entonces $\{\alpha_i(a)\}$ es la I-áda cuya i-ésima coordenada es a_i y cualquier otra es cero.

Consideremos X un R-módulo izquierdo y para cada $i \in I$ sean $f_i : A_i \to X$ R-homomorfismos. Definamos $\theta : \sum_{i\in I} A_i \to X$ dado por $\theta(\{a_i\}) = \sum_{i\in I} f_i(a_i)$.

Hay que hacer notar que $\sum_{i\in I} f_i(a_i)$ tiene sentido únicamente si $a_i \neq 0$ para un número finito de i's.

Veamos que $\theta \circ \alpha_i = f_i$ y que θ es único.

- Consideremos $a_i \in A_i$, entonces

$$\begin{aligned}(\theta \circ \alpha_i)(a_i) &= \theta(\alpha_i(a_i)) \\ &= \theta(\{\alpha_i(a)\}) \\ &= \sum_{i\in I} f_i(a_i) \\ &= f_i(a_i).\end{aligned}$$

  Por lo tanto

$$\theta \circ \alpha_i = f_i.$$

- Supongamos que $\psi : \sum_{i\in I} A_i \to X$ es tal que $\psi \circ \alpha_i = f_i$ para toda $i \in I$, entonces:

$$\begin{aligned}\psi(\{a_i\}) &= \psi\left(\sum_{i\in I}\{\alpha_i(a_i)\}\right) \\ &= \sum_{i\in I} \psi(\{\alpha_i(a_i)\}) \\ &= \sum_{i\in I} f_i(a_i) \\ &= \theta(\{a_i\}).\end{aligned}$$

  Por lo tanto $\theta = \psi$. Es decir, θ es el único R-homomorfismo con esa propiedad.

■

Teorema 3.3.11. *Sea $\{A_i\}_{i\in I}$ una familia no vacía de R-módulos izquierdos entonces*

$$\prod_{i\in I} A_i \text{ es el } \textbf{producto} \text{ en } {}_R\textbf{MOD}.$$

Demostración. Al igual que en la demostración del Teorema 3.3.10 hay que dar la familia de proyecciones $\left\{p_j : \prod_{i\in I} A_i \to A_j\right\}$.

Para cada $j \in I$ definamos

$$p_j : \prod_{i\in I} A_i \to A_j \text{ como } p_j\left(\{a_i\}\right) = a_j.$$

Consideremos X un R-módulo izquierdo y para cada $i \in I$ sean $f_i : X \to A_i$ R-homomorfismos. Definamos

$$\theta : X \to \prod_{i\in I} A_i \text{ como } \theta(x) = \left\{f_i(x)\right\}.$$

Demostremos que para cada $i \in I$, $p_i \circ \theta = f_i$ y que θ es un R-homomorfismo único con esta propiedad:

- Consideremos $x \in X$ entonces

$$\begin{aligned}(p_i \circ \theta)(x) &= p_i(\theta(x)) \\ &= p_i(\{f_i(x)\}) \\ &= f_i(x).\end{aligned}$$

  Por lo tanto $p_i \circ \theta = f_i$.

- Supongamos que $\psi : X \to \prod_{i\in I} A_i$ es tal que $p_i \circ \psi = f_i$ para toda $i \in I$. Entonces para cada $i \in I$ la i-ésima coordenada de $\psi(x)$ es $f_i(x)$ que coincide con la i-ésima coordenada de $\theta(x)$. Por lo tanto $\psi(x) = \theta(x)$ para toda $x \in X$, de aquí que $\psi = \theta$.

  Es decir, θ es el único R-homomorfismo con esa propiedad.

■

Finalmente, presentaremos el concepto de módulo libre, con lo cual la comparación entre grupos libres y módulos libres puede concluirse.

3.4. Módulos libres

Los módulos más sencillos son los módulos libres y también tenemos la propiedad de que todo módulo es cociente de un módulo libre.

Definición 3.4.1. Un R-módulo izquierdo F es llamado **R-módulo libre** (F es objeto libre en la categoría ${}_{\mathbf{R}}\mathbf{MOD}$) si F es isomorfo a una suma directa de copias de R. Es decir, existe un conjunto I tal que

$$F = \sum_{i \in I} R_i,$$

donde $R_i = \langle \{b_i\} \rangle \cong R$ para toda $i \in I$.

Suele llamarse a $B = \{ b_i | \, i \in I \}$ una **base** de F.

Observación 3.4.2. Los $\mathbb{Z}$-módulos libres son los grupos abelianos libres.

Demostración. Es claro que, debido a que los grupos libres cumplen la propiedad categórica de objeto libre, entonces cuando se extiende su estructura sigue cumpliendo la propiedad. ■

Observación 3.4.3. Si R es un anillo conmutativo entonces R es un R-módulo libre (considerando a R como un R-módulo sobre sí mismo).

Demostración. $R = \langle \{1\} \rangle$ y con ello cumple la definición. ■

Generalizando la propiedad de objeto libre:

Teorema 3.4.4. *Sea F un R-módulo libre, y sea $B = \{b_i | i \in I\}$ una base para F. Si M es un R-módulo y si $\gamma : B \to M$ es una función, entonces existe un R-homomorfismo $g : F \to M$ único tal que $g(b_i) = \gamma(b_i)$ para cualquier $i \in I$.*

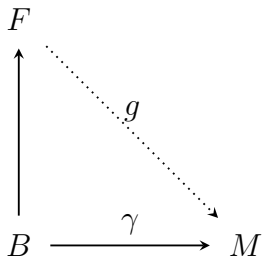


Figura 3.3: Diagrama del módulo libre F

Este resultado puede resumirse diciendo que existe un único R-homomorfismo γ que hace que el Diagrama 3.3 conmute.

Demostración. Debido a que F tiene una base B, entonces para cada $v \in F$ existen únicos $r_i \in R$ tales que

$$v = \sum_{i \in I} r_i b_i$$

donde $r_i \neq 0$ para un número finito de elementos. Definamos $g : F \to M$ por

$$g(v) = \sum_{i \in I} r_i \gamma(b_i).$$

Con esta definición es claro que g está bien definida ya que para cada $v \in F$ su representación con respecto a la base B es única.

Consideremos $v, u \in F$ y $r \in R$, con únicas $r_i', r_i \in R$ tales que $v = \sum_{i \in I} r_i' b_i$ y $u = \sum_{i \in I} r_i b_i$, entonces

$$\begin{aligned} g(v+u) &= \sum_{i \in I} (r_i' + r_i)\gamma(b_i) \\ &= \sum_{i \in I} (r_i'\gamma(b_i) + r_i\gamma(b_i)) \\ &= \sum_{i \in I} r_i'\gamma(b_i) + \sum_{i \in I} r_i\gamma(b_i) \\ &= g(v) + g(u). \end{aligned}$$

También

$$\begin{aligned} g(ru) &= \sum_{i \in I} (rr_i)\gamma(b_i) \\ &= r\sum_{i \in I} r_i\gamma(b_i) \\ &= rg(u). \end{aligned}$$

Si $\widehat{g} : F \to M$ es un R-homomorfismo tal que $\widehat{g}(b_i) = \gamma(b_i)$ para toda $i \in I$, entonces

$$\begin{aligned} g(v) &= \sum_{i\in I} r_i'\gamma(b_i) \\ &= \sum_{i\in I} r_i'\widehat{g}(b_i) \\ &= \widehat{g}\left(\sum_{i\in I} r_i' b_i\right) \\ &= \widehat{g}(v). \end{aligned}$$

Otra manera de demostrar este resultado es considerar a F como el coproducto de $\{\langle\{b_i\}\rangle \,|\, i \in I\}$ con los R-monomorfismos

$$\alpha_i : \langle\{b_i\}\rangle \to F$$

dados por

$$\alpha_i\left(r_i b_i\right) = \{r_i b_i\},$$

donde $\{r_i b_i\}$ es la I-áda cuyo i-ésimo elemento es $r_i b_i$ y cualquier otro es cero. Por el Teorema 3.3.10 existe un único R-homomorfismo $\theta : F \to M$ tal que $\theta\left(b_i\right) = \gamma\left(b_i\right)$. ■

Con esto terminamos de presentar los resultados de objeto libre, producto y coproducto en la categoría ${}_{\mathbf{R}}\mathbf{MOD}$.

Capítulo 4

Conclusiones

Durante este trabajo se presentaron tres objetos importantes en categorías concretas:

a) Sean I un conjunto de índices, $\mathcal{C}$ una categoría arbitraria y $\{A_i | i \in I\}$ una familia de $\mathcal{C}$-objetos con subíndices en el conjunto I. El **producto** de la familia $\{A_i | i \in I\}$ es un $\mathcal{C}$-objeto P junto con una familia de $\mathcal{C}$-morfismos llamados *proyecciones*, $\{\pi_i : P \to A_i | i \in I\}$ tal que para cualquier $\mathcal{C}$-objeto B y cualquier familia de $\mathcal{C}$-morfismos $\{\varphi_i : B \to A_i | i \in I\}$ existe un único $\mathcal{C}$-morfismo $\varphi : B \to P$ tal que $\pi_i \circ \varphi = \varphi_i$ para toda $i \in I$.

   El *producto* P de la familia $\{A_i | i \in I\}$, normalmente se denota como $\prod_{\mathbf{i \in I}} \mathbf{A_i}$.

b) El **coproducto** también conocido como **suma** de una familia $\{A_i | i \in I\}$ de $\mathcal{C}$-objetos, es un $\mathcal{C}$-objeto S, junto con una familia de $\mathcal{C}$-morfismos $\{\iota_i : A_i \to S | i \in I\}$ llamados *inyecciones* tales que para cualquier $\mathcal{C}$-objeto B y cualquier familia de $\mathcal{C}$-morfismos $\{\psi_i : A_i \to B | i \in I\}$ existe un único $\mathcal{C}$-morfismo $\psi : S \to B$ tal que $\psi \circ \iota_i = \psi_i$ para toda $i \in I$.

c) Sean F un objeto en una construcción $\mathcal{C}$, X un conjunto no vacío e $i : X \to F$ una función (de conjuntos). F es **libre en el conjunto** X siempre que para cualquier $\mathcal{C}$-objeto A y cualquier función (de conjuntos) $f : X \to A$ exista un único morfismo en $\mathcal{C}$, $\bar{f} : F \to A$ tal que $\bar{f} \circ i = f$ (como función de conjuntos $X \to A$).

Una vez que se dieron ejemplos en categorías como **SET** y **VEC**, centramos nuestra atención en hacer la construcción en **GRP** y ${}_R\mathbf{MOD}$.

La construcción de las tres estructuras en **GRP** requirieron una atención especial debido a que en los cursos formativos poco se da al respecto. Además en esta parte se explicaron ejemplos de manera extensa y precisa para dejar claro su uso.

El paso de transición de **GRP** a ${}_R\mathbf{MOD}$ fue mucho menos complicado ya que con la estructura mayor de los módulos se hace mucho más fácil el manejo tanto de los productos y coproductos como de los objetos libres.

Aún puede ofrecerse un espectro más profundo en **GRP** donde se presenten los grupos abelianos libres y dar una mejor caracterización. Para los propósitos de este trabajo es suficiente con el material presentado para crear en los lectores la inquietud de estudiar objetos que se muestran en el capítulo 1 de categorías.

Los grupos y los módulos tienen muchos resultados asociados a las estructuras presentadas pero estas tienen el propósito de caracterizar por un lado a los grupos y por otro a los anillos.

Es claro por los resultados presentados que la estructura en **GRP** se amplia de manera natural a ${}_R\mathbf{MOD}$ y por ello los resultados son casi los mismos.

Bibliografía

[1] Jiri Adamek, Horts Herrlich and George E. Strecker. "Abstract and concrete categories: the joy of cats", Mineolam New York: Dover, (2009).

[2] F.W Anderson and K.R. Fuller. "Rings and Categories of Modules" Springer-Verlag, (1991).

[3] Enderton, Herbert. "A mathematical introduction to logic", Academic Press, 2^{nd} Edition, (2001).

[4] T. W. Hungerford. "Algebra", Springer-Verlag, (1974).

[5] Saunders Mac Lane. "Categories for the Working Mathematician", Springer-Verlag, Second Edition, (1998).

[6] Mendelson, Elliott. "Introduction to Mathematical Logic", Chapman and Hall, 4^{th} Edition, (1997).

[7] J. J. Rotman. "Advanced Modern Algebra", Prentice Hall, 1^{st} Edition, (2002).