UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA DE MATEMÁTICA

TRABAJO DE GRADUACIÓN:

"DESARROLLO DE LA TEORIA BASICA DE GRUPOS LIBRES Y SUS TEOREMAS FUNDAMENTALES"

PRESENTADO POR:

BR. CLARA VICTORIA REGALADO BONILLA.

PARA OPTAR AL TÍTULO DE:

LICENCIADA EN MATEMÁTICA.

ASESORES:

Licda. CLAUDIA PATRICIA CORCIO LÓPEZ DE BELTRÁN

Licda. INGRID CAROLINA MARTÍNEZ BARAHONA

CIUDAD UNIVERSITARIA, 13 DE FEBRERO DE 2011

UNIVERSIDAD DE EL SALVADOR

Autoridades Universitarias 2008-2011

Msc. Rufino Antonio Quezada Sánchez

RECTOR

Msc. Miguel Ángel Pérez Ramos

VICERRECTOR ACADÉMICO

Msc. Óscar Noé Navarrete

VICERRECTOR ADMINISTRATIVO

Lic. Douglas Vladimir Alfaro Chávez

SECRETARIO GENERAL

Dr. René Medecadel Perla Jiménez

FISCAL GENERAL

Lic. Nelson Boanerges López Carrillo

DEFENSOR DE LOS DERECHOS UNIVERSITARIOS

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

Dr. Rafael Antonio Gómez Escoto

DECANO

Ms.D. Marta Noemí Martínez Hernández

VICEDECANA

Ing. Carlos Mauricio Canjura

DIRECTOR DE ESCUELA DE MATEMÁTICA

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

TRABAJO DE GRADUACIÓN:

"DESARROLLO DE LA TEORIA BASICA DE GRUPOS LIBRES Y SUS TEOREMAS FUNDAMENTALES"

PRESENTADO POR:

BR. CLARA VICTORIA REGALADO BONILLA

PARA OPTAR POR EL TITULO DE:

LICENCIADA EN MATEMÁTICA.

ASESORES:

Licda. CLAUDIA PATRICIA CORCIO LÓPEZ DE BELTRÁN

Licda. INGRID CAROLINA MARTÍNEZ BARAHONA

Dedicatoria

Dedicado a mis padres, quienes me inculcaron el amor al conocimiento y por quienes estoy aquí.

Agradecimientos

Agradezco a Dios por haberme permitido llegar con buena salud y gozando de vida hasta esta etapa de mi existencia, por regalarme un padre que siempre me apoyó ardua e incansablemente y a quien le debo y agradezco por lo que ahora soy, ya que me dedicó todo su tiempo.

A mi madre por enseñarme la base del conocimiento: leer, escribir y ... los números.

A mi esposo, familiares, amigos y profesores por ser parte de mi recorrido en diferentes etapas de mi trayectoria estudiantil.

Al Ingeniero Francisco Marroquín por proporcionarme los instrumento necesarios para realizar el trabajo e iluminar el camino que debía seguir.

Índice

Introducción

Los Grupos Libres son una área de la Teoría de Grupos, que no es profundizada en la Licenciatura en Matemática, esto, debido al bajo contenido en álgebra que posee el pensum, razón por la cual, el propósito del trabajo es mostrarse como una opción para una materia electiva.

Con toda la investigación y desarrollo realizado, se ha creado un trabajo apto para que un estudiante pueda leerlo y comprenderlo por si solo, ya que posee todas las herramientas básicas para su completo entendimiento. Se ha descrito paso a paso, el proceso realizado para la demostración de los teoremas, lemas, proposiciones y corolarios, al igual que los ejercicios, que ayudan a la comprensión de los capítulos.

Algúnos de los ejemplos presentados son de utilidad para la demostración de los teoremas más importantes. Estos resultados relevantes fueron los objetivos trazados al inicio de la investigación.

Dentro del proceso realizado durante el desarrollo del tema está, la intensa busqueda bibliográfica en libros, revistas y artículos en internet, del cual se escogió lo más importante que permitió obtener como resultado los capítulos con la información principal, en la que se fueron desarrollando los teoremas, corolarios, lemas y proposiciones, a esto se le agregaron los diferentes tipos de ejercicios resueltos. Finalizando con la presentación de los resultados.

El trabajo inicia con una introducción a los Grupos Libres, que es un enlace entre la Teoría de los Grupos Libres y la Teoría de grupos y anillos. Contiene los nuevos conceptos y resultados a partir de los ya conocidos, lo que nos permite comprender de forma fácil las nuevas definiciones. Luego pasamos a la teoría de los grupos libres trabajando con resultados y ejercicios. Una propiedad conocida con anterioridad es la de Abel, la que nos mostrará la nueva estructura de los Grupos Libres, pero con la condición abeliana. Continuamos con el grupo cociente entre un grupo libre y un subgrupo de él, a esto lo llamaremos Grupo Factor. Para finalizar con diferentes procesos de reescritura para la presentación de subgrupos normales y concluyendo con el teorema principal.

Se logró cubrir toda la teoría necesaria para comprender los resultados principales de los Grupos Libres, pasando por los subgrupos, grupos cocientes, grupo factor y presentación para subgrupos. El trabajo finaliza con la demostración del teorema central del documento, que un subgrupo de un grupo libre es libre.

1. Introducción a los Grupos Libres

Una idea intuitiva bajo la definición de categoría es que varios de los objetos matemáticos introducidos en cursos de Álgebra Moderna (conjuntos, grupos, monoides, anillos, módulos, etc) junto con un mapeo apropiado de estos objetos (funciones para conjuntos; homomorfismos para grupos, etc) tienen un número formal de propiedades en común.

Definición 1.1 *Una **categoría** es una clase $\mathscr{C}$ de objetos (denotados por A,B,C, ...) junto con:*

1. *Una clase de conjuntos disjuntos denotada por $hom(A, B)$ para cada par de objetos en $\mathscr{C}$ (un elemento f de $hom(A, B)$ es llamado* morfismo *de A a B y es denotado por $f : A \to B$).*
2. *Para cada trio (A, B, C) de objetos de $\mathscr{C}$, existe una función*

$$hom(B, C) \times hom(A, B) \to hom(A, C)$$

(para morfismos $f : A \to B$ $g : B \to C$, esta función se escribe $(g, f) \mapsto g \circ f$ y $g \circ f : A \to C$ es llamada la composición *de f y g); sujeta a los dos axiomas:*

   a) *Asociatividad. Si $f : A \to B$, $g : B \to C$, $h : C \to D$ son morfismos de $\mathscr{C}$, entonces $h \circ (g \circ f) = (h \circ g) \circ f$*

   b) *Identidad. Para cada objeto B de $\mathscr{C}$ existe un morfismo $1_B : B \to B$ tal que para algún $f : A \to B$, $g : B \to C$,*

$$1_B \circ f = f \qquad y \qquad g \circ 1_B = g$$

Definición 1.2 *En una categoría $\mathscr{C}$, un morfismo $f : A \to B$ es llamado una **equivalencia** si existe en $\mathscr{C}$ un morfismo $g : B \to A$ tal que $g \circ f = 1_A$ y $f \circ g = 1_B$. Si $f : A \to B$ es una equivalencia, A y B se dice que son **equivalentes**.*

Con esta última definición podemos obtener nuestro primer resultado.

Proposición 1.1 *La composición de dos equivalencias es una equivalencia.*

Demostración

Sea $f : A \to B$ y $f' : B \to A$ su morfismo asociado, tal que $f' \circ f = 1_A$ y $f \circ f' = 1_B$.

Y sea $g : B \to C$ y $g' : C \to B$ su morfismo asociado, tal que $g' \circ g = 1_B$ y $g \circ g' = 1_C$, las dos equivalencias, entonces, la composición de ellas es $g \circ f : A \to C$ a la que llamaremos h, luego si ahora hacemos la composición de f' y g' obtenemos la función $f' \circ g' : C \to A$, a la que llamaremos k. Probemos ahora que el morfismo que hace que la función h sea equivalente, es la composición k, para ello hagamos la composición $k \circ h$:

$$k \circ h : A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{g'} B \xrightarrow{f'} A$$

$$k \circ h = 1_A$$

y también la composición $h \circ k$:

$$h \circ k : C \xrightarrow{g'} B \xrightarrow{f'} A \xrightarrow{f} B \xrightarrow{g} C$$

$$h \circ k = 1_C$$

Lo que por definición muestra que en efecto es una equivalencia. $\star$

EJEMPLO 1

Sea $\mathscr{S}$ la clase de todos los conjuntos; para A, $B \in \mathscr{S}$, $hom(A, B)$ es el conjunto de todas las funciones $f : A \to B$. Entonces $\mathscr{S}$ es una categoría. Un morfismo f de $\mathscr{S}$ es una equivalencia si y solo si f es una biyección, ya que su función inversa es la que hace que al componerlas resulte la identidad y para que posea inversa se necesita que sea biyectiva.

EJEMPLO 2

Sea $\mathscr{G}$ la categoría donde sus objetos son grupos; $hom(A, B)$ es el conjunto de todos los grupos homomórficos $f : A \to B$. Un morfismo f es una equivalencia si y solo si f es un isomorfismo, al igual que en el ejemplo anterior se necesita la biyección, pero dado que son homomorfismos la conclusión se tiene. La categoría $\mathscr{A}$ de todos los grupos abelianos este definida similarmente.

EJEMPLO 3

Sean los objetos de todos los conjuntos parcialmente ordenados $(S, \leq)$. Un morfismo $(S, \leq) \to (T, \leq)$ es una función $f : S \to T$ tal que para $x, y \in S$, $x \leq y \Rightarrow f(x) \leq f(y)$.

EJEMPLO 4

Sea $\mathscr{C}$ algúna categoría y definamos la categoría $\mathscr{D}$ donde sus objetos son todos los morfismo de $\mathscr{C}$. Si $f : A \to B$ y $g : C \to D$ son morfismos de $\mathscr{C}$, entonces $hom(f, g)$ consiste de todos los pares (α, β), donde $\alpha : A \to C$, $\beta : B \to D$ son morfismos de $\mathscr{C}$, tal que el siguiente diagrama es conmutativo:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\ C \arrow[r, "g"] & D \end{tikzcd}$$

Definición 1.3 *Sea $\mathscr{C}$ una categoría y $\{A_i/i \in I\}$ una familia de objetos de $\mathscr{C}$. Un **producto** para la familia $\{A_i/i \in I\}$, es un objeto P de $\mathscr{C}$ junto con una familia de morfismos $\{\pi_i : P \to A_i/i \in I\}$ tal que para algún objeto B y una familia de morfismos $\{\varphi_i : B \to A_i/i \in I\}$, existe un único morfismo $\varphi : B \to P$ tal que $\pi_i \circ \varphi = \varphi_i$, para todo $i \in I$.*

Un producto P de $\{A_i/i \in I\}$ es usualmente denotado por $\prod_{i \in I} A_i$. Esto a veces ayuda a describir un producto en términos de un diagrama conmutativo, especialmente en el caso $I = \{1, 2\}$. Un producto para $\{A_1, A_2\}$ es un diagrama (de objetos y morfismos) $A_1 \overset{\pi_1}{\leftarrow} P \overset{\pi_2}{\rightarrow} A_2$ tal que para algún otro diagrama de la forma $A_1 \overset{\varphi_1}{\leftarrow} B \overset{\varphi_2}{\rightarrow} A_2$ existe un único morfismo $\varphi : B \to P$ tal que el siguiente diagrama es conmutativo:

$$\begin{tikzcd} & B \arrow[dl, "\varphi_1"'] \arrow[d, "\varphi"] \arrow[dr, "\varphi_2"] & \\ A_1 & P \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & A_2 \end{tikzcd}$$

Teorema 1.1 *Si $(P, \{\pi_i\})$ y $(Q, \{\psi_i\})$ son ambos productos de la familia $\{A_i/i \in I\}$ de objetos de una categoría $\mathscr{C}$, entonces P y Q son equivalentes.*

Demostración

Dado que P y Q son ambos productos, entonces existe un morfismo $f : P \to Q$ y $g : Q \to P$, tal que el diagrama es conmutativo para cada $i \in I$:

$$\begin{tikzcd} P \arrow[r, "f"] \arrow[dr, "\pi_i"'] & Q \arrow[d, "\psi_i"] \\ & A_i \end{tikzcd} \qquad \begin{tikzcd} Q \arrow[r, "g"] \arrow[d, "\psi_i"'] & P \arrow[dl, "\pi_i"] \\ A_i & \end{tikzcd}$$

La composición de estos dos morfismo para cada $i \in I$ es un diagrama conmutativo.

$$\begin{tikzcd} P \arrow[rr, "g \circ f"] \arrow[dr, "\pi_i"'] & & P \arrow[dl, "\pi_i"] \\ & A_i & \end{tikzcd}$$

Así $g \circ f : P \to P$ es un morfismo tal que $\pi_i \circ (g \circ f) = \pi_i$, para todo $i \in I$. Pero por la definición de producto existe un único morfismo con esta propiedad. Dada la función $1_P : P \to P$, es también que $\pi_i \circ 1_P = \pi_i$ para todo $i \in I$, debemos tener que $g \circ f = 1_P$ por unicidad. Similarmente, usando el hecho que Q es un producto, eso muestra que $f \circ g = 1_Q$. De aquí $f : P \to Q$ es una equivalencia. $\star$

Dado que la categoría abstracta envuelve solo objetos y morfismos (no elementos), todo estado sobre ellos tiene un estado dual, obtenido al invertir todas las flechas (morfismos) en estado original. Por ejemplo, el dual de la definición (1.3) es:

Definición 1.4 *Un* ***coproducto*** *(o* ***suma****) para la familia* $\{A_i/i \in I\}$ *de objetos en una categoría* $\mathscr{C}$ *es un objeto* S *de* $\mathscr{C}$*, junto con una familia de morfismos* $\{k_i : A_i \to S/i \in I\}$ *tal que para algún objeto* B *y una familia de morfismos* $\{\psi_i : A_i \to B/i \in I\}$*, existe un único morfismo* $\psi : S \to B$ *tal que* $\psi \circ k_i = \psi_i$ *para todo* $i \in I$*.*

No existe una notación uniforme para coproductos, aunque $\coprod_{i \in I} A_i$ es usada a veces.

El siguiente teorema puede ser probado usando el argumento dual usado en la prueba del teorema (1.1).

Teorema 1.2 *Si* $(S, \{\psi_i\})$ *y* $(S', \{\lambda_i\})$ *son ambos coproductos de la familia* $\{A_i/i \in I\}$ *de objetos de una categoría* $\mathscr{C}$*, entonces* S *y* S' *son equivalentes.*

Demostración

Similar al teorema (1.1). $\star$

En varias de las categorías mencionadas anteriormente (por ejemplo, grupos), los objetos en ellas son de hecho un conjunto (usualmente con algúna estructura adicional) y todo morfismo $f : A \to B$ en la categoría es una función (usualmente con algúna otra propiedad). Formalizamos esta idea en:

Definición 1.5 *Una* ***categoría concreta*** *es una categoría* $\mathscr{C}$ *junto con una función* σ *que asigna a cada objeto* A *de* $\mathscr{C}$ *un conjunto* $\sigma(A)$ *(llamada el conjunto fundamental de* A*) de tal manera que:*

1. *Todo morfismo* $A \to B$ *de* $\mathscr{C}$ *es una función en el conjunto fundamental* $\sigma(A) \to \sigma(B)$*.*

2. *El morfismo identidad de cada objeto* A *de* $\mathscr{C}$ *es la función identidad en el conjunto fundamental* $\sigma(A)$*.*

3. *La composición de morfismos en* $\mathscr{C}$ *esta relacionada con composición de funciones en los conjuntos fundamentales.*

EJEMPLO 5

La categoría de grupos, equipada con la función que asígna a cada grupo su conjunto subyacente en el sentido usual, es una categoría concreta. Similarmente la categoría de grupos abelianos y los conjuntos parcialmente ordenados, con obviamente los conjuntos subyacentes, son una categoría concreta. En el tercer ejemplo después de la definición (1.1), si la función σ asigna al grupo G el usual conjunto subyacente G, entonces la categoría en cuestión no es una categoría concreta (dado que el homomorfismo no es una función en el conjunto G).

Las categorías concretas son frecuentemente usadas ya que tienen disponible no solo las propiedades de categoría, sino también ciertas propiedades de conjuntos, subconjuntos, etc. Como estamos interesados en toda categoría concreta, la función σ asígna a un objeto su conjunto subyacente en el sentido usual (como en el ejemplo anterior), denotaremos ambos objetos y sus conjuntos subyacentes por el mismo símbolo y omitiremos algúna referencia explícita a σ. Existe una pequeña oportunidad de confusión, por lo que debemos ser cuidadosos en una categoría concreta $\mathscr{C}$ para distinguir morfismo de $\mathscr{C}$ (que están definidos también como funciones en los conjuntos subyacentes) y mapeos (funciones en los conjuntos subyacentes, los cuales puede que no sean morfismos de $\mathscr{C}$).

Definición 1.6 *Sea F un objeto en una categoría concreta $\mathscr{C}$, X un conjunto no vacío y una función (de conjuntos) $i : X \to F$. F es **libre en el conjunto** X siempre que para algún objeto A de $\mathscr{C}$ y una función (de conjuntos) $f : X \to A$, hay un único morfismo de $\mathscr{C}$, $\overline{f} : F \to A$ tal que $\overline{f}i = f$ (como un mapeo de conjuntos $X \to A$).*

Un hecho esencial sobre un objeto libre F es que con el fin de definir un morfismo con dominio F, es suficiente especificar la imagen de el subconjunto $i(X)$ como se verá en el siguiente ejemplo.

EJEMPLO 6

Sea G algún grupo y $g \in G$. Entonces la función $\bar{f} : Z \to G$ definida por $\bar{f}(n) = g^n$, es fácil ver que será el único morfismo de $Z \to G$ tal que $1 \mapsto g$. Consecuentemente, si $X = \{1\}$ y $i : X \to Z$ es la función inclusión, entonces Z es libre en X en la categoría de grupos; (dado $f : X \to G$, sea $g = f(1)$ y definamos $\bar{f}$ como anteriormente). En otras palabras, para determinar un único morfismo de Z a G necesitamos solo especificar la imagen de $1 \in Z$ (esto es, la imagen de $i(X)$). El grupo (aditivo) Q de los números racionales no tiene esta propiedad. No es difícil ver que no existe un homomorfismo no trivial $Q \to S_3$. Así para algún conjunto X, la función $i : X \to Q$ y la función $f : X \to S_3$ con $f(x_1) \neq (1)$ para algún $x_1 \in X$, no existe un homomorfismo $\bar{f} : Q \to S_3$ con $\bar{f}i = f$.

Teorema 1.3 *Si $\mathscr{C}$ es una categoría concreta, F y F' son objetos de $\mathscr{C}$ tal que F es libre en el conjunto X y F' es libre en el conjunto X' y $\mid X \mid = \mid X' \mid$ [1], entonces F es equivalente a F'.*

[1]Donde $\mid X \mid$ es el orden del conjunto.

Note que las hipótesis son satisfechas cuando F y F' son ambos libres en el mismo conjunto X.

Demostración

Dado que F y F' son libres y $|X| = |X'|$, existe una biyeccion $f : X \to X'$ y funciones $i : X \to F$ y $j : X' \to F'$. Considere la función $j \circ f : X \to F'$. Dado que F es libre, existe un morfismo $\varphi : F \to F'$ tal que el diagrama es conmutativo.

$$\begin{tikzcd} F \arrow[r, "\varphi"] & F' \\ X \arrow[u, "i"] \arrow[r, "f"'] & X' \arrow[u, "j"'] \end{tikzcd}$$

Similarmente, dada la biyección de f, tiene inversa $f^{-1} : X' \to X$ y F' es libre, existe un morfismo $\psi : F' \to F$ tal que es conmutativo.

$$\begin{tikzcd} F' \arrow[r, "\psi"] & F \\ X' \arrow[u, "j"] \arrow[r, "f^{-1}"'] & X \arrow[u, "i"'] \end{tikzcd}$$

Combinando estos diagramas, resulta el siguiente diagrama conmutativo.

$$\begin{tikzcd} F \arrow[r, "\psi \circ \varphi"] & F \\ X \arrow[u, "i"] \arrow[r, "f^{-1}f = 1_X"'] & X \arrow[u, "i"'] \end{tikzcd}$$

De aquí que $(\psi \circ \varphi)i = i1_x = i$. Pero $1_F i = i$. Así por la propiedad de unicidad de objetos libres tenemos que $\psi \circ \varphi = 1_F$. De igual forma $(\varphi \circ \psi)j = j1_{X'} = j$, pero como $1_{F'}j = j$ nuevamente por la unicidad tenemos que $\varphi \circ \psi = 1_{F'}$. $\star$

Productos, coproductos, y objetos libres son todos definidos via **propiedades universales de funciones** (esto es, en términos de existencia de ciertos morfismos determinados únicamente). También podemos ver que para dos productos (o coproductos) para una familia dada de objetos son actualmente equivalentes (teorema (1.1) y (1.2)). Asimismo dos objetos libres en el mismo conjunto son equivalentes (teorema (1.3)). Además existen ciertas similitudes entre las pruebas de los teoremas (1.1) y (1.3). Consecuentemente no es sorprendente que todas las nociones mencionadas son hechos de casos especiales de un único concepto.

Definición 1.7 *Un objeto I en una categoría $\mathscr{C}$ se dice que será* ***universal*** *(o* ***inicial****) si para cada objeto C de $\mathscr{C}$ existe uno y solo un morfismo $I \to C$. Un objeto T de $\mathscr{C}$ se dice que será* ***couniversal*** *(o* ***terminal****) si para cada objeto C de $\mathscr{C}$ existe uno y solo un morfismo $C \to T$*

Teorema 1.4 *Para dos cualesquiera objetos universales (couniversales respectivamente) en una categoría $\mathscr{C}$ son equivalentes.*

Demostración

Sea I y J un objeto universal en $\mathscr{C}$. Dado que I es universal, existe un único morfismo $f : I \to J$. Similarmente, dado que J es universal, existe un único morfismo $g : J \to I$. La composición $g \circ f : I \to I$ es un morfismo de $\mathscr{C}$. Pero $1_I : I \to I$ es también un morfismo de $\mathscr{C}$. La universalidad de I implica que existe un único morfismo $I \to I$, donde $g \circ f = 1_I$. Similarmente la universalidad de J implica que $f \circ g = 1_J$. Además $f : I \to J$ es una equivalencia.

La prueba para objetos couniversales es análoga. $\star$

EJEMPLO 7

El grupo trivial $\langle e \rangle$ es ambas cosas universal y couniversal en la categoría de grupos.

EJEMPLO 8

Sea F un objeto libre en el conjunto X (con $i : X \to F$) en una categoría concreta $\mathscr{C}$. Definamos una nueva categoría $\mathscr{D}$ como sigue. Los objetos de $\mathscr{D}$ son todas las funciones de conjuntos $f : X \to A$, donde A es un objeto de $\mathscr{C}$. Un morfismo en $\mathscr{D}$ de $f : X \to A$ a $g : X \to B$ se define que será un morfismo $h : A \to B$ de $\mathscr{C}$ tal que el diagrama:

$$\begin{tikzcd} & A \arrow[dd, "h"] \\ X \arrow[ur, "f"] \arrow[dr, "g"'] & \\ & B \end{tikzcd}$$

es conmutativo (esto es, $hf = g$). Verifiquemos que $1_A : A \to A$ es el morfismo identidad de f a f en $\mathscr{D}$ y que h es una equivalencia en $\mathscr{D}$ si y solo si h es una equivalencia en $\mathscr{C}$. Dado que F es libre en el conjunto X, hay para cada función $f : X \to A$ un único morfismo $\bar{f} : F \to A$ tal que $\bar{f}i = f$. Esto es precisamente el hecho que $i : X \to F$ es un objeto universal en la categoría $\mathscr{D}$.

EJEMPLO 9

Sea $\{A_i/i \in I\}$ una familia de objetos en una categoría $\mathscr{C}$. Definamos una categoría $\mathscr{E}$ donde sus objetos son los pares $(B, \{f_i/i \in I\})$, donde B es un objeto de $\mathscr{C}$ y para cada i, $f_i : B \to A$ es un morfismo de $\mathscr{C}$. Un morfismo en $\mathscr{E}$ de $(B, \{f_i/i \in I\})$ a $(D, \{g_i/i \in I\})$ es definido por un morfismo $h : B \to D$ de $\mathscr{C}$ tal que $g_i \circ h = f_i$ para todo $i \in I$. Veriquemos que 1_B es el morfismo identidad de $(B, \{f_i\})$ a $(B, \{f_i\})$ en $\mathscr{E}$ y que h es una equivalencia en $\mathscr{E}$ si y solo si h es una equivalencia en $\mathscr{C}$. Si un producto existe en $\mathscr{C}$ para la familia $\{A_i/i \in I\}$ (con función $\pi_k : \prod A_i \to A_k$ para cada $k \in I$), entonces para todo $(B, \{f_i\})$ en $\mathscr{E}$ existe un único morfismo $f : B \to \prod A_i$ tal que $\pi_i \circ f = f_i$ para todo $i \in I$. Pero esto dice que $(\prod A_i, \{\pi_i/i \in I\})$ es un objeto couniversal en la categoría $\mathscr{E}$. Similarmente el coproducto de una familia de objetos en $\mathscr{C}$ puede ser considerado como un objeto universal en una categoría construida apropiadamente.

Un producto $\prod A_i$ de una familia $\{A_i/i \in I\}$ en una categoría puede ser considerado como un objeto couniversal en una categoría adecuada, se sigue inmediatamente del teorema (1.4) que $\prod A_i$ esta únicamente determinado bajo la equivalencia. Análogamente los resultados se mantienen para coproductos y objetos libres.

2. Grupos libres

Dado un conjunto X debemos construir un grupo F que es libre en el conjunto X, en el sentido de la definición (1.6). Si $X = \phi$, F es el grupo trivial $\langle e\rangle^2$. Si $X \neq \phi$, y sea X^{-1} un conjunto disjunto de X tal que $\mid X \mid=\mid X^{-1} \mid$. Eligiendo una biyección $X \to X^{-1}$ y denotando la imagen de $x \in X$ por x^{-1}. Finalmente eligiendo un conjunto disjunto de $X \cup X^{-1}$ y tiene exactamente un elemento, denotando este elemento por 1.

Definición 2.1 *Una **palabra** en X es una sucesión $(a_1, a_2, \dots)$ con $a_i \in X \cup X^{-1} \cup \{1\}$ tal que para algún $n \in \aleph^*$.*[3]

Definición 2.2 *La sucesión constante $(1, 1, \dots)$ es llamada **una palabra vacía** y es denotada por 1.*

Definición 2.3 *Dos elementos x y x^{-1} son **adyacentes** si cumplen que $a_i = x$ entonces $a_{i+1} = x^{-1}$ y si $a_i = x^{-1}$ entonces $a_{i+1} = x$ para todo $i \in \aleph^*$, $x \in X$.*

Definición 2.4 *Una palabra $(a_1, a_2, \dots)$ en X se dice que es **reducida** si se prueba que:*

1. *Para todo $x \in X$, x y x^{-1} son no adyacentes.*
2. *$a_k = 1$ implica que $a_i = 1$ para todo $i \geq k$.*

En particular, la palabra vacía 1 es reducida porque para todo a_i es igual a 1.

Toda palabra reducida no vacía es de la forma $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$, donde $n \in \aleph^*$, $x_i \in X$ y $\lambda = \pm 1$ (y de aquí en adelante por convención x^1 lo denotaremos simplemente x para toda $x_i \in X$). De aquí en adelante denotaremos esta palabra por $x_1^{\lambda_1} x_2^{\lambda_2} \dots x_n^{\lambda_n}$. Esta nueva notación es más tratable y más sugestiva. Obsérvese que la definición de igualdad de ecuaciones, muestra que dos palabras reducidas $x_1^{\lambda_1} x_2^{\lambda_2} \dots x_n^{\lambda_n}$ y $y_1^{\delta_1} y_2^{\delta_2} \dots y_m^{\delta_m}$ (x_i, $y_i \in X$ y λ_i, $\delta_i = \pm 1$) son iguales si y solo si ambas son 1 o $m = n$ y $x_i = y_i$, $\lambda_i = \delta_i$ para cada $i = 1, 2, \dots, n$. Consecuentemente la función de X en el conjunto $F(X)$ de todas las palabras reducidas en X dadas por $x \mapsto x^1 = x$ es inyectiva.

Identificaremos a X con su imagen y consideraremos a X un subconjunto de $F(X)$.

Ahora definiremos una operación binaria en el conjunto $F = F(X)$ de todas las palabras reducidas en X. La palabra vacía 1 actuará como elemento identidad ($w1 = 1w = w$ para cada $w \in F$). Informalmente nos gustaría tener el producto de palabras reducidas no vacías dadas por la yuxtaposición, así:

[2] Donde $\langle e\rangle$ es el grupo generado por e que es el uno del conjunto

[3] $\aleph^*$ simboliza los naturales exceptuando el cero.

$$(x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n})(y_1^{\delta_1}y_2^{\delta_2}\dots y_m^{\delta_m}) = x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n}y_1^{\delta_1}y_2^{\delta_2}\dots y_m^{\delta_m}$$

Desafortunadamente la palabra en el lado derecho de la ecuación puede que no sea reducida (por ejemplo, si $x_m^{\lambda_m} = y_1^{-\delta_1}$). Además, hemos definido el producto por una yuxtaposición y (si es necesario) la cancelación de términos adyacentes de la forma xx^{-1} o $x^{-1}x$; por ejemplo $(x_1^1x_2^{-1}x_2^1)(x_2^{-1}x_2^1x_1^1) = x_1^1x_1^1$. Más precisamente, si $x_1^{\lambda_1}\dots x_n^{\lambda_n}$ y $y_1^{\delta_1}\dots y_m^{\delta_m}$ son palabras reducidas no vacías en X con $n \leq m$, sea k el más grande entero ($0 \leq k \leq n$) tal que $x_{n-j}^{\lambda_{n-j}} = y_{j+1}^{-\lambda_{j+1}}$ para $j = 0, 1, \dots, k-1$. Entonces definimos:

$$(x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n})(y_1^{\delta_1}y_2^{\delta_2}\dots y_m^{\delta_m}) = \begin{cases} x_1^{\lambda_1}\dots x_{n-j}^{\lambda_{n-j}}y_{k+1}^{\delta_{k+1}}\dots y_m^{\delta_m} & ; \text{si } k < n \\ y_{n+1}^{\delta_{n+1}}\dots y_m^{\delta_m} & ; \text{si } k = n < m \\ 1 & ; \text{si } k = n = m \end{cases}$$

Si $n > m$, el producto se define de manera análoga. La definición asegura que el producto de palabras reducidas es una palabra reducida.

Proposición 2.1 *El producto de palabras reducidas es una palabra reducida*

Demostración

Sea $x = (x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n})$ y $y = (y_1^{\delta_1}y_2^{\delta_2}\dots y_m^{\delta_m})$ dos palabras reducidas no vacías, por definición su producto es:

$$\begin{aligned} xy &= (x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n})(y_1^{\delta_1}y_2^{\delta_2}\dots y_m^{\delta_m}) \\ &= (x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n}y_1^{\delta_1}y_2^{\delta_2}\dots y_m^{\delta_m}) \\ &= z \end{aligned}$$

z es no vacía ya que x y y son no vacías, note que z es ese producto si los $x_i^{\lambda_i}$ son no adyacentes para todo i de igual forma con los $y_i^{\delta_i}$ y que $x_n \neq y_1$ y $\lambda_n \neq -\delta_1$. En caso que existan términos adyacentes entonces tenemos.

$$z = \begin{cases} x_1^{\lambda_1}\dots x_{n-j}^{\lambda_{n-j}}y_{k+1}^{\delta_{k+1}}\dots y_m^{\delta_m} & ; \text{si } k < n \\ y_{n+1}^{\delta_{n+1}}\dots y_m^{\delta_m} & ; \text{si } k = n < m \\ 1 & ; \text{si } k = n = m \end{cases}$$

Por la forma en que se ha obtenido el producto tenemos que la parte 1 de (2.4) de la definición se cumple, luego la única forma que $a_k = 1$, es que si a_k es un término de z, entonces $k = m$ y de ahi en adelante y está compuesta de unos, por lo tanto se cumple 2 de la definición (2.4).

$\star$

Teorema 2.1 *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 binaria definida anteriormente y $F = \langle X \rangle$.*

Demostración

Primero probaremos que es un grupo, para ello nótese que 1 es el elemento identidad y que $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ tiene elemento inverso y es $x_n^{-\lambda_n} \dots x_1^{-\lambda_1}$, en efecto comprobemos que al multiplicarlos obtenemos el elemento identidad.

$$\begin{aligned}
(x_1^{\lambda_1} \dots x_n^{\lambda_n})(x_n^{-\lambda_n} \dots x_1^{-\lambda_1}) &= x_1^{\lambda_1} \dots x_n^{\lambda_n} x_n^{-\lambda_n} \dots x_1^{-\lambda_1} && \text{dado que } x_n^{\lambda_n} x_n^{-\lambda_n} = 1 \text{ tenemos} \\
&= x_1^{\lambda_1} \dots x_{n-1}^{\lambda_{n-1}} x_{n-1}^{-\lambda_{n-1}} \dots x_1^{-\lambda_1} && \text{y nuevamente } x_{n-1}^{\lambda_{n-1}} x_{n-1}^{-\lambda_{n-1}} = 1 \\
&= x_1^{\lambda_1} x_1^{-\lambda_1} && \text{repitiendo este} \\
&= 1 && \text{proceso sucesivamente}
\end{aligned}$$

ahora solo necesitamos verificar la asociatividad. Puede realizarse por inducción pero resulta mucho más sencillo y menos tedioso de la siguiente manera:

Para cada $x \in X$ y $\delta = \pm 1$, sea $|x^\delta|$ sea la función $F \to F$ dada por $1 \mapsto x^\delta$ y

$$x_1^{\delta_1} \dots x_n^{\delta_n} \mapsto \begin{cases} x^\delta x_1^{\lambda_1} \dots x_n^{\lambda_n} & ; \text{Si } x^\delta \neq x_1^{-\delta_1} \\ x_2^{\lambda_2} \dots x_n^{\lambda_n} & ; \text{Si } x^\delta = x_1^{-\delta_1} (= 1 \text{ si } n = 1) \end{cases} \tag{1}$$

Dado que $|x||x^{-1}| = 1_F = |x^{-1}||x|$, todo $|x^\delta|$ es una permutación (biyección) de F (con inverso $|x^{-\delta|}$). Sea $A(F)$ el grupo de todas las permutaciones de F y F_0 el grupo generado por $\{|x|; x \in X\}$. La función $\varphi : F \to F_0$ dada por $1 \mapsto 1_F$ y $x_1^{\delta_1} \dots x_n^{\delta_n} \mapsto |x_1^{\delta_1}| \dots |x_n^{\delta_n}|$ es claramente sobreyectiva tal que $\varphi(w_1 w_2) = \varphi(w_1)\varphi(w_2)$ para todo $w_i \in F$. Dado $1 \mapsto x_1^{\delta_1} \dots x_n^{\delta_n}$ bajo la función $|x_1^{\delta_1}| \dots |x_n^{\delta_n}|$, se sigue que φ es inyectiva. El hecho que F_0 es un grupo implica que la asociatividad se mantiene en F y que φ es un isomorfismo de grupos. Obviamente $F = \langle X \rangle$.

$\star$

Definición 2.5 *El grupo $F = F(X)$ es llamado **grupo libre en el conjunto** X.*

Las propiedades de los grupos libres son fáciles de derivar. Por ejemplo si $|X| \geq 2$, entonces el grupo libre en X es no abeliano ($x, y \in X$ y $x \neq y \Rightarrow x^{-1}y^{-1}xy$ es reducida $\Rightarrow x^{-1}y^{-1}xy \neq 1 \Rightarrow xy \neq yx$).

Proposición 2.2 *Todo elemento en un grupo libre tiene orden infinito (excepto el orden del elemento identidad)*

Demostración

Sea $w = x_1^{\lambda_1} x_2^{\lambda_2} \dots x_n^{\lambda_n}$, si en w los elementos $x_1^{\lambda_1}$ y $x_n^{\lambda_n}$ son inversos y $x_2^{\lambda_2}$ y $x_{n-1}^{\lambda_{n-1}}$ son inversos, así sucesivamente hasta que $x_k^{\lambda_k}$ y $x_{n-k+1}^{\lambda_{n-k+1}}$ son los últimos que cumplen con ser inversos, es decir que $x_{k+1}^{\lambda_{k+1}}$ y $x_{n-k}^{\lambda_{n-k}}$ no es inverso uno del otro y tomando $z = x_{k+1}^{\lambda_{k+1}} x_{k+2}^{\lambda_{k+2}} \dots x_{n-k}^{\lambda_{n-k}}$ con k que cumple la inecuación $0 \leq k \leq \frac{n}{2}$, este valor k existe debido a que w no es una palabra vacía. Ahora para $s > 0$ (el orden de w), tenemos que:

$$\begin{aligned}
w^s &= \underbrace{x_1^{\lambda_1} \dots x_n^{\lambda_n} x_1^{\lambda_1} \dots x_n^{\lambda_n} \dots x_1^{\lambda_1} \dots x_n^{\lambda_n}}_{s \text{ veces}} \\
&= x_1^{\lambda_1} \dots \underbrace{x_{k+1}^{\lambda_{k+1}} x_{k+2}^{\lambda_{k+2}} \dots x_{n-k}^{\lambda_{n-k}} x_{k+1}^{\lambda_{k+1}} x_{k+2}^{\lambda_{k+2}} \dots x_{n-k}^{\lambda_{n-k}} \dots x_{k+1}^{\lambda_{k+1}} x_{k+2}^{\lambda_{k+2}} \dots x_{n-k}^{\lambda_{n-k}}}_{s \text{ veces}} \dots x_n^{\lambda_n} \\
&= x_1^{\lambda_1} \dots x_k^{\lambda_k} \underbrace{zz \dots z}_{s \text{ veces}} x_{n-k+1}^{\lambda_{n-k+1}} \dots x_n^{\lambda_n} \\
&= x_1^{\lambda_1} \dots x_k^{\lambda_k} z^s x_{n-k+1}^{\lambda_{n-k+1}} \dots x_n^{\lambda_n}
\end{aligned}$$

La expresión del lado derecho de esta ecuación no admite algúna cancelación, esto es, es una palabra reducida no vacía. De aquí se sigue que $w^s \neq 1$.

Si $X = \{a\}$, entonces el grupo libre en X es el grupo infinito cíclico $\langle a \rangle$.

$\star$

Un hecho no trivial es que todo subgrupo de un grupo libre es el mismo un grupo libre en algún conjunto.

Teorema 2.2 *Sea F un grupo libre en un conjunto X y la función inclusión $i : X \to F$, si G es un grupo y $f : X \to G$ una función de conjuntos, entonces existe un único homomorfismo de grupos $\bar{f} : F \to G$, tal que $\bar{f}i = f$. En otras palabras, F es un objeto libre en el conjunto X en la categoría de grupos.*

Demostración

Definamos $\bar{f} = e$ y si $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ es una palabra reducida no vacía en X y por lo tanto, pertenece a $F(X)$, definamos $\bar{f}(x_1^{\lambda_1} \dots x_n^{\lambda_n}) = f(x_1)^{\lambda_1} \dots f(x_n)^{\lambda_n}$. Dado que G es un grupo y $\lambda_i = \pm 1$, el producto $f(x_1)^{\lambda_1} \dots f(x_n)^{\lambda_n}$ es un elemento bien definido de G, ya que el producto de elementos de G se queda en G. Verifiquemos $\bar{f}$ es un homomorfismo único tal que $\bar{f}i = f$. Para ello supongamos que existe $g : F \to G$, que es algún homomorfismo tal que $gi = f$, entonces

$$\begin{aligned}
g(x_1^{\lambda_1}\dots x_n^{\lambda_n}) &= g(x_1^{\lambda_1})\dots g(x_n^{\lambda_n}) \text{ por ser homomorfismo}\\
&= g(\underbrace{x_1x_1\dots x_1}_{\lambda_1 \text{ veces}})\dots g(\underbrace{x_nx_n\dots x_n}_{\lambda_n \text{ veces}})\\
&= \underbrace{g(x_1)g(x_1)\dots g(x_1)}_{\lambda_1 \text{ veces}}\dots \underbrace{g(x_n)g(x_n)\dots g(x_n)}_{\lambda_n \text{ veces}}\\
&= g(x_1)^{\lambda_1}\dots g(x_n)^{\lambda_n}\\
&= gi(x_1)^{\lambda_1}\dots gi(x_n)^{\lambda_n}\\
&= f(x_1)^{\lambda_1}\dots f(x_n)^{\lambda_n}\\
&= \bar{f}(x_1^{\lambda_1}\dots x_n^{\lambda_n})
\end{aligned}$$

Entonces $\bar{f}$ es única.

Si F' es otro objeto libre en el conjunto X en la categoría de grupos (con $\lambda : X \to F'$), entonces los teoremas (1.3) y (2.2) implican que existe un isomorfismo $\varphi : F \cong F'$ tal que $\varphi i = \lambda$. En particular $\lambda(X)$ es un conjunto de generadores de F'; este hecho también puede ser provado directamente de la definición de objeto libre.

$\star$

Proposición 2.3 *Todo grupo G es imagen homomórfica de un grupo libre*

Demostración

Sea X el conjunto de los generadores de G y sea F el grupo libre en el conjunto X. Por el teorema anterior la inclusión de la función $X \to G$ induce un homomorfismo $\bar{f} : F \to G$ tal que $x \mapsto x \in G$. Dado que $G = \langle X \rangle$, la prueba del teorema anterior muestra que $\bar{f}$ es un epimorfismo [4].

$\star$

Una consecuencia inmediata de la proposición (2.3) y el primer teorema de isomorfía es que algún grupo G es isomorfo a un grupo cociente F/N, donde $G = \langle X \rangle$, F es el grupo libre en X y N es el núcleo del epimorfismo $F \to G$ de la proposición (2.3). Además, el orden para describir G sobre un isomorfismo necesitamos especificar X, F y N. Pero F esta determinado sobre un isomorfismo por X y N está determinado por algún subconjunto que lo genere como un subgrupo de F. Ahora si $w = x_1^{\lambda_1}\dots x_n^{\lambda_n} \in F$ es un generador de N , entonces bajo el epimorfismo $F \to G$, $w \mapsto x_1^{\lambda_1}\dots x_n^{\lambda_n} = e \in G$.

Definición 2.6 *La ecuación $x_1^{\lambda_1}\dots x_n^{\lambda_n} = e$ en G es llamada una **relación** en los generadores x_i.*

[4] Recordemos que un epimorfismo es un homomorfismo sobreyectivo

Claramente un grupo dado G, puede ser completamente descrito por un conjunto X específico de generadores de G y un conjunto adecuado R de relaciones en esos generadores. Esta descripción no es única dado que hay muchas posibles elecciones de X y R dado por algún grupo G.

Dado el conjunto de "generadores" X y el conjunto Y de las palabras (reducidas) de los elementos de X, construiremos un grupo tal como sigue: Sea F el grupo libre en X y N el subgrupo normal de F generado por Y[5]. Sea G el grupo cociente F/N e identifiquemos X con su imagen F/N bajo la función $X \subset F \to F/N$; como se denotó anteriormente, esto puede implicar identificar algúnos elementos de X con algúnos otros. Entonces G es un grupo generado por X y por construcción todas las relaciones $w = e(w \in Y)$ satisfacen ($w = x_1^{\lambda_1} \dots x_n^{\lambda_n} \in Y \Rightarrow x_1^{\lambda_1} \dots x_n^{\lambda_n} \in N \Rightarrow x_1^{\lambda_1} N \dots x_n^{\lambda_n} N = N$; esto es, $x_1^{\lambda_1} \dots x_n^{\lambda_n} = e$ en $G = F/N$).

Definición 2.7 *Sea X un conjunto y Y un conjunto de palabras (reducidas) en X. Un grupo G se dice que será un **grupo definido por los generadores** $x \in X$ y las **relaciones** $w = e$ $(w \in Y)$ siempre que $G \cong F/N$ donde F es el grupo libre en X y N el subgrupo normal de F generado por Y . Diremos que $(X|Y)$ es una **presentación** de G.*

Para la demostración del siguiente teorema nos vemos en la necesidad de utilizar un resultado de grupos el cual es la proposición siguiente:

Proposición 2.4 *Si $f : G \to H$ es un homomorfismo de grupos, $N \lhd G$, $M \lhd H$ y $f(N) < M$, entonces f induce un homomorfismo $\bar{f} : G/N \to H/M$, dado por $aN \mapsto f(a)M$, con $a \in G$. $\bar{f}$ es un isomorfismo si y solo si $Im\ f\ \cup M = H$ y $f^{-1}(M) \subset N$. En particular si f es un epimorfismo tal que $f(N) = M$ y $Kerf \subset N$, entonces $\bar{f}$ es un isomorfismo.*

La discusión precedente muestra que el grupo definido por los generadores y las relaciones siempre existe. Además es más posible tal grupo en la siguiente forma:

Teorema 2.3 *(Van Dyck) Sea X un conjunto y Y el conjunto de las palabras (reducidas) en X y G el grupo definido por los generadores $x \in X$ y las relaciones $w = e$ $(w \in Y)$. Si H es algún grupo tal que $H = \langle X \rangle$ y H satisface todas las relaciones $w = e$ $(w \in Y)$, entonces existe un epimorfismo $G \to H$*

Demostración

Si F es el grupo libre en X la inclusión $X \to H$ induce un epimorfismo $\varphi : F \to H$ por la proposición (1.1). Dado que H satisface la relación $w = e$ $(w \in Y)$, $Y \subset Ker\varphi$. Consecuentemente,

[5]El subgrupo normal generado por un conjunto $S \subset F$ es la intersección de todos los subgrupos normales de F que contienen a S

el subgrupo normal N generado por Y en F esta contenido en $Ker\varphi$. Por la proposición (2.4), φ induce un epimorfismo $F/N \to H/0$. Además la composición $G \cong F/N \to H/0 \cong H$ es un epimorfismo.

$\star$

Los elementos de Y están siendo interpretados como palabras en X, productos en G y productos en H como el contexto lo indique.

Los siguientes ejemplos de grupos definidos por generadores y relaciones. Por conveniencia utilizaremos notación exponencial para las palabras (por ejemplo, x^2y^{-3} en lugar de $x^1x^1y^{-1}y^{-1}y^{-1}$).

EJEMPLO 1

Sea G el grupo definido por los generadores a, b y las relaciones $a^4 = e$, $a^2b^{-2} = e$ y $abab^{-1} = e$. Dado que Q_8 es el grupo cuaternión de orden 8, es generado por los elementos a, b, satisfaciendo las relaciones, existe un epimorfismo $\varphi : G \to Q_8$ por el teorema (2.3). De aquí $|G| \geq |Q_8| = 8$. Sea F el grupo libre en $\{a, b\}$ y N el subgrupo normal generado por $\{a^4, a^2b^{-2}, abab^{-1}\}$. No es difícil ver que todo elemento de F/N es de la forma a^ib^iN con $0 \leq i \leq 3$ y $j = 0, 1$, de donde $|G| = |F/N| \geq 8$. Además $|G| = 8$ y φ es un isomorfismo. Así el grupo definido por los generadores y relaciones es Q_8 o isomórfo a él.

EJEMPLO 2

El grupo definido por los generadores a, b y las relaciones $a^n = e$ $(3 \geq n \in N^*)$, $b^2 = e$ y $abab = e$ (o $ba = a^{-1}b$) es el dihedral grupo D_n.

EJEMPLO 3

El grupo definido por un generador b y la relación única $b^m = e$ $(m \in N^*)$ es Z_m.

EJEMPLO 4

El grupo libre F en un conjunto X es el grupo definido por los generadores $x \in X$ y no hay relaciones (recalcando que $\langle \phi \rangle = \langle e \rangle$). La terminología libre viene del hecho que F es una relación-libre.

Cerramos este capítulo con una breve discusión de coproductos (productos libres) en la categoría de grupos.

Dada una familia de grupos $\{G_i/i \in I\}$ asumiendo que los G_i son conjuntos disjuntos dos a dos. Sea $X = \cup_{i \in I} G_i$ y sea $\{1\}$ el conjunto unitario disjunto de X. Una palabra en X es una sucesión $(a_1, a_2, \ldots)$ tal que $a_i \in X \cup \{1\}$ y para algún $n \in N^*$, $a_i = 1$ para todo $i \geq n$.

Definición 2.8 *Una palabra $(a_1, a_2, \ldots)$ es **reducida** si cumple:*

(i) *$a_i \in X$ no es el elemento identidad en su grupo G_i.*

(ii *Para todo $i, j \geq 1$, a_i y a_{i+1} no están en el mismo grupo G_j.*

(iii) *$a_k = 1$ implica que $a_i = 1$ para todo $i \geq k$.*

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

Definición 2.9 *Sea $\prod_{i\in I}^{*} G_i$ (o $G_1 * G_2 * \cdots * G_n$ si I es finito) el conjunto de todas las palabras reducidas en X. $\prod_{i\in I}^{*} G_i$ forma un grupo, llamado el* ***producto libre*** *de una familia $\{G_i/i \in I\}$, bajo la operación binaria definida como sigue:*

1 es el elemento identidad y el producto de dos palabras reducidas diferente de 1 esencialmente es una yuxtaposición. Dada que la yuxtaposición producto de dos palabras reducidas puede ser no reducida, podemos hacer las cancelaciones y contracciones necesarias. Por ejemplo, si a_i, $b_i \in G_i$, para $i = 1, 2, 3$, entonces $(a_1 a_2 a_3)(a_3^{-1} b_2 b_1 b_3) = a_1 c_2 b_1 b_3 = (a_1, c_2, b_1, b_3, 1, 1, \dots)$, donde $c_2 = a_2 b_2 \in G$. Finalmente, para cada $k \in I$, la función $\phi_k : G_k \to \prod_{i\in I}^{*} G_i$ dada por $e \mapsto 1$ y $a \mapsto a = (a, 1, 1, \dots)$ es un monomorfismo de grupos. Consecuentemente, a veces identificamos G_k con su imagen isomórfica en $\prod_{i\in I}^{*} G_i$.

Teorema 2.4 *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 grupos homomórficos, entonces existe un único homomorfismo $\psi : \prod_{i\in I}^{*} G_i \to H$ tal que $\psi\phi_i = \psi_i$ para todo $i \in I$ (ya que para cada $k \in I$ se tiene la función $\phi_k : G_k \to \prod_{i\in I}^{*} G_i$) y sus propiedades están determinadas $\prod_{i\in I}^{*} G_i$ únicamente por el isomorfismo. En otras palabras, $\prod_{i\in I}^{*} G_i$ es un coproducto en la categoría de grupos.*

Demostración

Si $a_1 a_2 \dots a_n$ es una palabra reducida en $\prod_{i\in I}^{*} G_i$ con $a_k \in Gi_k$, definimos $\psi(a_1 a_2 \dots a_n)$ que será $\psi_{i_1}(a_1)\psi_{i_2}(a_2) \dots \psi_{i_n}(a_n) \in H$.

$\star$

Veamos otros ejemplos de grupos libres:

EJEMPLO 5

Considere las funciónes α y β en el conjunto $\mathbb{C} \cup \{\infty\}$ definido por las reglas:

$$(x)\alpha = x + 2 \qquad \text{y} \qquad (x)\beta = \frac{x}{2x+1}$$

Aquí el símbolo ∞ esta sujeto a ciertas reglas formales como $1/0 = \infty$ y $\infty/\infty = 1$. Entonces α y β son biyecciones dado que ellos tienen inversos, llamados $(x)\alpha^{-1} = x - 2$ y $(x)\beta^{-1} = \dfrac{x}{1-2x}$. Así α y β generan un grupo de permutaciones F de $\mathbb{C} \cup \{\infty\}$; veremos que F es libre en el conjunto $\{\alpha, \beta\}$.

Para ver esto observe que, una potencia no cero de α, lleva al interior del círculo unidad $|z| = 1$ al exterior y una potencia no cero de β, lleva del exterior del círculo al interior, sin el cero: la segunda parte es mas fácil de comprender de la ecuación $(1/x)\beta = 1/(x+2)$. De esto se ve que una palabra reducida no trivial en $\{\alpha, \beta\}$ puede ser igual a 1. De aquí todo elemento de F tiene una única expresión como palabra reducida. Entonces F es libre en $\{\alpha, \beta\}$.

EJEMPLO 6

Este ejemplo es de un grupo libre generado por matrices. La función α y β discutida en el ejemplo anterior nos intuye de una función de $\mathbb{C} \cup \{\infty\}$ dada por:

$$\lambda(a, b, c, d) : x \mapsto \frac{ax + b}{cx + d}$$

donde $ad - bc \neq 0$ y $a, b, c, d \in \mathbb{C}$. A tal función se le conoce como una *transformación fraccional lineal.* Ahora podemos ver que la función

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \lambda(a, b, c, d)$$

es un homomorfismo de $GL(2, \mathbb{C})$ al grupo de todas las transformaciones fraccionales lineales de $\mathbb{C}$ en el cual

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

son las funciones de α y β respectivamente. Dado que la palabra reducida no trivial en $\{\alpha, \beta\}$ puede ser igual a 1, la misma idea es cierta para las palabras reducidas en $\{A, B\}$. Consecuentemente el grupo $\langle \alpha, \beta \rangle$ es libre en $\{\alpha, \beta\}$.

3. Grupos libres abelianos

En este capítulo se estudiará un poco sobre objetos libres en la categoría de grupos *abelianos*. Como es usual cuando hablamos de grupos abelianos **la notación aditiva será usada**. Abajo, presentamos algúnas de las notaciones a utilizar y el significado que tendrán.

$$ab \to a + b \text{ El producto significará la suma.}$$

$$a^{-1} \to -a \text{ El inverso, el opuesto}$$

$$e \to 0 \text{ El neutro, el nulo}$$

$$a^n \to na \text{ El exponente del elemento, será el exponente por el elemento}$$

$$ab^{-1} \to a - b \text{ Un elemento por el inverso de otro, es la diferencia de ambos elementos}$$

$$HK \to H + K \text{ El producto de conjuntos, la suma de ellos, es decir, la unión}$$

$$aH \to a + H \text{ Un elemento por un grupo, es el grupo unido al elemento}$$

$$G \times H \to G \oplus H \text{ El producto de grupos, es la unión de los grupos}$$

$$\prod_{i \in I} G_i \to \sum_{i \in I} G_i \text{ El producto directo de grupos, será la suma directa de grupos}$$

Para algún grupo G en notación aditiva, $(m + n)a = ma + na(a \in G; m, n \in Z)$. Si el grupo es abeliano, entonces $m(a+b) = ma+mb$. Si X es un conjunto no vacío de G, entonces el subgrupo $\langle X \rangle$ generado por X en notación aditiva consiste de todas las **combinaciones lineales** $n_1x_1 + n_2x_2 + \cdots + n_kx_k$ $(n_i \in Z, x_i \in X)$. En particular, el grupo cíclico $\langle x \rangle$ es $\{nx/n \in Z\}$.

Comenzaremos por extender la definición del producto directo $G \times H$ de grupos G y H a una familia arbitraria de grupos (posiblemente infinita) $\{G_i/i \in I\}$. Define una operación binaria en el producto cartesiano (de conjuntos) $\prod_{i \in I} G_i$ como sigue. Si $f, g \in \prod_{i \in I} G_i$ (esto es, $f, g : I \to \bigcup_{i \in I} G_i$ y $f(i), g(i) \in G_i$ para cada i), entonces $fg : I \to \bigcup_{i \in I} G_i$ es la función dada por $i \to f(i)g(i)$. Dado que cada G_i es un grupo, $f(i), g(i) \in G_i$ para todo i, dado que $fg \in \prod_{i \in I} G_i$. Si identificamos $f \in \prod_{i \in I} G_i$ con su imagen $\{a_i\}$ $(a_i = f(i)$ para cada $i \in I)$ como es usualmente hacerlo en el caso cuando I es finito, entonces la operación binaria en $\prod_{i \in I} G_i$ es la familia de la multiplicación de componentes: $\{a_i\}\{b_i\} = \{a_ib_i\}$.

$\prod_{i \in I} G_i$ junto con esta operación binaria, es llamada el **producto directo** (o **suma directa completa**) de la familia de grupos $\{G_i/i \in I\}$. Si $I = \{1, 2, \ldots, n\}$, $\prod_{i \in I} G_i$ es usualmente denotado $G_1 \times G_2 \times \cdots \times G_n$ (o en notación aditiva, $G_1 \oplus G_2 \oplus \cdots \oplus G_n$).

Teorema 3.1 *Si $\{G_i/i \in I\}$ es una familia de grupos, entonces:*

1. *El producto directo $\prod_{i\in I} G_i$ es un grupo.*

2. *Para cada $k \in I$, la función $\pi_k : \prod_{i\in I} G_i \to G_k$ dada por $f \mapsto f(k)$ (o $\{a_i\} \mapsto a_k$) es un epimorfismo de grupos.*

Demostración

1. Sea $f, g \in \prod_{i\in I} G_i$, para ver que es grupo verifiquemos que su producto y diferencia estan ahi:

$$\begin{aligned} (f-g)(i) &= f(i) - g(i) \in G_i \text{ y este es grupo} \\ &= h(i) \in G_i \text{ para todo } i \end{aligned}$$

entonces $f - g \in \prod_{i\in I} G_i$. Ahora veamos el producto

$$\begin{aligned} (fg)(i) &= f(i)g(i) \in G_i \text{ y este es grupo} \\ &= h(i) \in G_i \text{ para todo } i \end{aligned}$$

para la asociatividad, como cada G_i es grupo entonces es asociativo para todo i entonces, la asociatividad de $\prod_{i\in I} G_i$ se deriva de la asociatividad de cada grupo.

2. Para que π_k sea epimorfismo veamos que sea homomorfismo y sobreyectiva:

Sea $f, g \in \prod_{i\in I} G_i$

a)

$$\begin{aligned} \pi_k(fg)(k) &= (fg)(k) \\ &= f(k)g(k) \\ &= \pi_k(f)\pi_k(g) \end{aligned}$$

b)

$$\begin{aligned} \pi_k(f+g)(k) &= (f+g)(k) \\ &= f(k) + g(k) \\ &= \pi_k(f) + \pi_k(g) \end{aligned}$$

Ahora veamos sobreyectividad. Sea $a_k \in G_k$, luego por estar en G_k $a_k \in \prod_{i\in I} G_i$, esto se cumple para todo k, entonces al menos $G_K \in \prod_{i\in I} G_i \neq \emptyset$ y tenemos la función identidad por lo tanto es sobre (si en $\prod_{i\in I} G_i$ solo esta G_k entonces la función es biyectiva).

$\star$

La función π_k en el teorema (3.1) es llamada la **proyección canónica** del producto directo.

Teorema 3.2 *Sea $\{G_i/i \in I\}$ una familia de grupos y $\{\varphi_i : H \to G_i/i \in I\}$ una familia de homomorfismos de grupo. Entonces existe un único homomorfismo $\varphi : H \to \prod_{i\in I} G_i$ tal que $\pi_i\varphi = \varphi_i$ para todo $i \in I$ (y donde $\pi_k : \prod_{i\in I} G_i \to G_k$) y esta propiedad determina $\prod_{i\in I} G_i$ únicamente bajo el isomorfismo. En otras palabras, $\prod_{i\in I} G_i$ es un producto en la categoría de grupos.*

Demostración

Sea $\varphi : H \to \prod_{i\in I} G_i$ una función de conjuntos dada por $\varphi(a) = \{\varphi_i(a)\}_{i\in I} \in \prod_{i\in I} G_i$ la única función tal que $\pi_i\varphi = \varphi_i$ para todo $i \in I$. Esto es fácil de verificar que φ es un homomorfismo, ya que, sea $a, b \in H$ y recordando que la operación binaria en $\prod_{i\in I} G_i$ es la familia de la multiplicación de componentes: $\{a_i\}\{b_i\} = \{a_ib_i\}$.

$$\begin{aligned}
\varphi(ab) &= \{\varphi_i(ab)\}_{i\in I} \in \prod_{i\in I} G_i \\
&= \{\varphi_i(a)\}_{i\in I}\{\varphi_i(b)\}_{i\in I} \in \prod_{i\in I} G_i \\
&= \varphi(a)\varphi(b)
\end{aligned}$$

y como φ_i es una familia de homomorfismos, tenemos que la propiedad homomórfica de φ se deriva de los φ_i. De aquí $\prod_{i\in I} G_i$ es un producto (en el sentido de la categoría) y además determinado bajo el isomorfismo (equivalencia) por el teorema (1.1).

$\star$

Dado el producto directo de grupos abelianos es claramente abeliano, se sigue que el producto directo de grupos abelianos es un producto en la categoría de grupos abelianos también.

Definición 3.1 *El **producto directo débil (externo)** (denotado por $\prod_{i\in I}^{w} G_i$), de una familia de grupos $\{G_i/i \in I\}$, es el conjunto de todas las funciones $f \in \prod_{i\in I} G_i$ tal que $f(i) = e_i$, donde los e_i son la identidad en G_i, para todo i, pero un número finito de $i \in I$. Si todos los grupos G_i son abelianos (aditivos), $\prod_{i\in I}^{w} G_i$ es usualmente llamado la **suma directa (externa)** y está denotado por $\sum_{i\in I} G_i$.*

EJEMPLO 1

Sean G_1 y G_2 grupos cíclicos de orden 2, $G_1 = \{1, x_1\}$ y $G_2 = \{1, x_2\}$ entonces todo elemento $g \neq 1$ de su producto libre puede escribirse unívocamente como un producto de x_1 y x_2, alternados, por ejemplo:

$$x_1, x_1x_2, x_1x_2x_1, x_1x_2x_1x_2, \text{ etc.}$$

$$x_2, x_2x_1, x_2x_1x_2, x_2x_1x_2x_1, \text{ etc.}$$

obsérvese que los elementos x_1x_2 y x_2x_1 son ambos de orden finito y distintos, obsérvese también la gran diferencia entre el producto directo débil de G_1 y G_2 y su producto directo, en este caso el producto directo débil es un grupo abeliano de orden 4, mientras que el producto directo es un grupo abeliano con elementos de orden finito.

Si I es finito, el producto directo débil coincide con el producto directo. En algúnos casos tenemos:

Teorema 3.3 *Si $\{G_i/i \in I\}$ es una familia de grupos, entonces:*

1. *$\prod_{i\in I}^{w} G_i$ es un subgrupo normal de $\prod_{i\in I} G_i$.*

2. *Para cada $k \in I$, la función $j_k : G_k \to \prod_{i\in I}^{w} G_i$ dada por $j_k(a) = \{a_i\}_{i\in I}$, donde $a_i = e$ para $i \neq k$ y $a_k = a$, es un monomorfismo[6] de grupos.*

3. *Para cada $i \in I$, $j_i(G_i)$ es un subgrupo normal de $\prod_{i\in I} G_i$.*

Demostración

1. Sea $f, g \in \prod_{i\in I}^{w} G_i$, para probar que es subgrupo veamos que $fg^{-1} \in \prod_{i\in I}^{w} G_i$

$$\begin{aligned} (fg^{-1})(i) &= f(i)g^{-1}(i) \qquad \text{por definición} \\ &= e_i(e_i)^{-1} \\ &= e_i \text{ para todo } i \end{aligned}$$

de aquí que $fg^{-1} \in \prod_{i\in I}^{w} G_i$. Ahora comprobemos que es normal, para ello veamos que $f \prod_{i\in I}^{w} G_i f^{-1} \in \prod_{i\in I}^{w} G_i$.

[6]Un monomorfismo es un homomorfismo inyectivo

$$\begin{aligned}
(f\prod_{i\in I}^{w} G_i f^{-1})(i) &= f(i)(\prod_{i\in I}^{w} G_i)(i)f^{-1}(i)\\
&= e_i(\prod_{i\in I}^{w} G_i)(i)e_i\\
&= (\prod_{i\in I}^{w} G_i)(i) \in \prod_{i\in I}^{w} G_i
\end{aligned}$$

2. Sea $a, b \in G_k$ y probemos la inyectividad:

$$\begin{aligned}
j_k(a) &= j_k(b)\\
\{a_i\}_{i\in I} &= \{b_i\}_{i\in I}\\
&= \begin{cases} e = e & \text{, si } i \neq k \text{ ya que } a_i = e \text{ y } b_i = e\\ a = b & \text{, si } i = k \text{ ya que } a_k = a \text{ y } b_k = b \end{cases}
\end{aligned}$$

lo que indica que es inyectivo y por definición de producto directo es homomorfismo.

3. Probemos que $j_i(G_i)$ es subgrupo. Sea $a, b \in G_i$

$$\begin{aligned}
j_i(a)j_i(b)^{-1} &= \{a_i\}_{i\in I}\{b_i\}_{i\in I}^{-1}\\
&= \begin{cases} ee^{-1} & \text{, si } i \neq k\\ ab^{-1} & \text{, si } i = k \end{cases}\\
&= \begin{cases} e & \text{, si } i \neq k \in G_i \text{ por ser } G_i \text{ grupo}\\ ab^{-1} & \text{, si } i = k \in G_i \text{ por ser } G_i \text{ grupo} \end{cases}
\end{aligned}$$

con esto queda demostrado, ahora veamos que es normal:

$$\begin{aligned}
j_i(a)j_i(G_i)j_i(a)^{-1} &= \begin{cases} ej_i(G_i)e^{-1} & \text{, si } i \neq k\\ aj_i(G_i)a^{-1} & \text{, si } i = k \end{cases}\\
&= \begin{cases} j_i(G_i) \in j_i(G_i) & \text{, si } i \neq k\\ aj_i(G_i)a^{-1} \in j_i(G_i) & \text{, si } i = k \in G_i \text{ por ser } G_i \text{ grupo} \end{cases}
\end{aligned}$$

Con lo anterior, se concluye la prueba del teorema. ⋆

La función j_k en el teorema (3.3) es llamada la **inyección canónica**.

Teorema 3.4 *Sea $\{A_i/i \in I\}$ una familia de grupos abelianos (escritos en forma aditiva). Si B es un grupo abeliano y $\{\psi_i : A_i \to B/i \in I\}$ una familia de homomorfismos, entonces existe un único homomorfismo $\psi : \sum_{i\in I} A_i \to B$ tal que $\psi j_i = \psi_i$ para todo $i \in I$*[7] *y esta propiedad determinada $\sum_{i\in I} A_i$ únicamente bajo el isomorfismo. En otras palabras, $\sum_{i\in I} A_i$ es un coproducto en la categoría de grupos abelianos.*

Demostración

Totalmente en esta prueba todos los grupos serán escritos aditivamente. Si $0 \neq \{a_i\} \in \sum A_i$, entonces solo un número finito de a_i son no cero, es decir $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$. Definamos $\psi : \sum A_i \to B$ por $\psi\{0\} = 0$ y $\psi(\{a_i\}) = \psi_{i_1}(a_{i_1}) + \psi_{i_2}(a_{i_2}) + \cdots + \psi_{i_r}(a_{i_r}) = \sum_{i\in I_0} \psi_i(a_i)$, donde I_0 es el conjunto $\{i_{1,2}, \ldots, i_r\} = \{i \in I/a_i \neq 0\}$. Dado que B es abeliano, es fácilmente verificar que ψ es un homomorfismo y que $\psi j_i = \psi_i$, para todo $i \in I$. Para cada $\{a_i\} \in \sum A_i$, $\{a_i\} = \sum_{i\in I_0} j_i(a_i)$, I_0 finito como antes. Probemos que ψ es única y supongamos que existe ξ de manera que $\xi : \sum A_i \to B$ es un homomorfismo tal que $\xi j_i = \psi_i$ para todo i, entonces,

$$\begin{aligned}
\xi(\{a_i\}) &= \xi(\sum_{I_0} j_i(a)) \\
&= \sum_{I_0} \xi j_i(a) \\
&= \sum_{I_0} \psi_i(a_i) \\
&= \sum_{I_0} \psi j_i(a_i) \\
&= \psi(\sum_{I_0} j_i(a_i)) \\
&= \psi(\{a_i\})
\end{aligned}$$

De aquí $\xi = \psi$ y ψ es única. Además $\sum A_i$ es un coproducto en la categoría de grupos abelianos y también está determinado bajo el isomorfismo (equivalencia) por el teorema (1.2).

⋆

El teorema es falso si la palabra abeliano es omitida. El producto directo débil externo no es un coproducto en la categoría de todos los grupos.

Ahora veremos bajo que condiciones un grupo G es isomorfo al producto directo débil de una familia de subgrupos.

[7] Donde j_i es la función definida en el teorema (3.3), sustituyendo la familia de los G_i por los A_i

Teorema 3.5 *Sea $\{N_i/i \in I\}$ una familia de subgrupos normales de un grupo G tal que:*

1. $G = \langle \bigcup_{i\in I} N_i \rangle$.

2. *Para cada* $k \in I$, $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$.

Entonces $G \cong \prod_{i\in I}^{w} N_i$

Antes de probar el teorema veamos un caso especial que es frecuentemente usado: observe que para subgrupos normales $N_1, N_2, \ldots, N_r$ de un grupo G, $\langle N_1 \cap N_2 \cap \cdots \cap N_r \rangle = N_1N_2\ldots N_r = \{n_1n_2\ldots n_r/n_i \in N_i\}$. En notación aditiva $N_1N_2\ldots N_r$ se escribe como $N_1 + N_2 + \cdots + N_r$. Es de mucha ayuda tener en mente la siguiente proposición, dado que la prueba del caso general es esencialmente la misma.

Proposición 3.1 *Si $N_1N_2\ldots N_r$ son subgrupos normales de un grupo G tal que $G = N_1N_2\ldots N_r$ y para cada $1 \leq k \leq r$, $N_k \cap (N_1\ldots N_{k-1}N_{k+1}\ldots N_r) = \langle e \rangle$, entonces $G \cong N_1 \times N_2 \times \cdots \times N_r$.*

Demostración del teorema (3.5)

Si $\{a_i\} \in \prod^{w} N_i$, entonces $a_i = e$ para todo i, pero un número finito de $i \in I$. Sea I_0 el conjunto finito $\{i \in I/a_i \neq e\}$. Entonces $\prod_{i\in I_0} a_i$ son elementos bien definidos de G, dado para $a \in N_i$ y $b \in N_j$, $(i \neq j)$, $ab = ba$. Consecuentemente la función $\varphi : \prod^{w} N_i \to G$, dado por $\{a_i\} \mapsto \prod_{i\in I_0} a_i \in G$ (y $\{e\} \mapsto e$), es un homomorfismo tal que $\varphi j_i(a_i) = a_i$ para $a_i \in N_i$.

Dado que G es generado por los subgrupos N_i, todo elemento a de G es un producto finito de elementos de varios N_i. Dado los elementos de N_i y N_j conmutan (para $i \neq j$), a puede ser escrito como un producto $\prod_{i\in I_0} a_i$, donde $a_i \in N_i$ e I_0 es algún subconjunto finito de I. De aquí $\prod_{i\in I_0} j_i(a_i) \in \prod^{w} N_i$ y $\varphi(\prod_{i\in I_0} j_i(a_i)) = \prod_{i\in I_0} \varphi j_i(a_i) = \prod_{i\in I_0} a_i = a$. Además, φ es un epimorfismo.

Supóngase que $\varphi(\{a_i\}) = \prod_{i\in I_0} a_i = e \in G$. Claramente podemos asumir por conveniencia de notación que $I_0 = \{1, 2, \ldots, n\}$. Entonces $\prod_{i\in I_0} a_i = a_1a_2\ldots a_n = e$, con $a_i \in N_i$. Luego $a_1^{-1} = a_2\ldots a_n \in N_1 \cap \langle_{i\neq 1} N_i \rangle = \langle e \rangle$ y además $a_1 = e$. La repetición de este argumento muestra que $a_i = e$ para todo $i \in I$. De aquí que φ es un monomorfismo.

$\star$

El teorema (3.5) motiva a la siguiente definición:

Definición 3.2 *Sea $\{N_i/i \in I\}$ una familia de subgrupos normales de un grupo G tal que $G = \langle \bigcup_{i\in I} N_i \rangle$ y para cada $k \in I$, $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$. Entonces G se dice que es **el producto interno** de una familia $\{N_i/i \in I\}$ (o la **suma directa interna** si G es abeliano(aditivo)).*

Como un resultado del teorema (3.5) tenemos la siguiente caracterización del producto directo interno débil.

Teorema 3.6 *Sea $\{N_i/i \in I\}$ una familia de subgrupos normales de un grupo G. G es el producto directo interno débil de una familia $\{N_i/i \in I\}$ si y solo si todo elemento no identidad de G es un producto único $a_{i_1}a_{i_2}\ldots a_{i_n}$ con $i_1, i_2, \ldots, i_n$ elementos distintos de I y $e \neq a_{i_k} \in N_{i_k}$ para cada $k = 1, 2, \ldots, n$.*

Existe una distinción entre el producto directo interno y externo débil. Si un grupo G es el producto directo interno débil de grupos N_i, entonces por definición cada N_i es un subgrupo de G y G es isomórfico al producto directo externo débil $\prod_{i\in I}^{w} N_i$. Luego, el producto directo externo débil $\prod_{i\in I}^{w} N_i$ no contiene los grupos N_i solo a copias isomórfica de ellos (llamadas el $j_i(N_i)$ vea el teorema (3.3)). Prácticamente hablando esta distinción no es muy importante y los adjetivos "interno" y "externo" serán omitidos cuando la confusión no sea posible. De hecho usaremos la siguiente notación.

NOTACIÓN

Escribirémos $G = \prod_{i\in I}^{w} N_i$ para indicar que el grupo G es un producto directo interno débil de la familia de subgrupos $\{N_i/i \in I\}$.

Teorema 3.7 *Sea $\{f_i : G_i \to H_i/i \in I\}$ una familia de homomorfismos de un grupo y sea $f = \prod f_i$ la función de $\prod_{i\in I} G_i \to \prod_{i\in I} H_i$, dada por $\{a_i\} \mapsto \{f_i(a_i)\}$. Entonces f es un homomorfismo de grupos tal que $f(\prod_{i\in I}^{w} G_i) \subset \prod_{i\in I}^{w} H_i$, $Kerf = \prod_{i\in I} Kerf_i$ y $Im\ \ f = \prod_{i\in I} Im\ \ f_i$. Consecuentemente f es un monomorfismo si y solo si cada f_i también es monomorfismo.*

Proposición 3.2 *Sea $\{G_i/i \in I\}$ y $\{N_i/i \in I\}$ familias de grupos tales que N_i es un subgrupo normal de G_i para cada $i \in I$*

1. *$\prod_{i\in I} N_i$ es un subgrupo normal de $\prod_{i\in I} G_i$ y $\prod_{i\in I} G_i / \prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$.*
2. *$\prod_{i\in I}^{w} N_i$ es un subgrupo normal de $\prod_{i\in I}^{w} G_i$ y $\prod_{i\in I}^{w} G_i / \prod_{i\in I}^{w} N_i \cong \prod_{i\in I}^{w} G_i/N_i$.*

Demostración

1. Para cada i, sea $\pi_i : G_i \to G_i/N_i$ el epimorfismo canónico. Por el teorema (3.7), la función $\prod \pi_i : \prod_{i\in I} G_i \to \prod_{i\in I} G_i/N_i$ es un epimorfismo con kernel $\prod_{i\in I} N_i$. Además $\prod_{i\in I} G_i / \prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$ por el primer teorema de isomorfía[8].
2. De manera similar a 1.

$\star$

[8]Primer Teorema de Isomorfía: Sea $f : G \to H$ un homomorfismo de grupos. Entonces existe un isomorfismo $g : G/(kerf) \to Im\ f$ y por tanto $G/(kerf) \approx Im\ f$

Definición 3.3 *Una **Base** de un grupo abeliano F es un subconjunto X de F tal que:*

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

ii) *Para distintos $x_1, x_2, \ldots, x_k \in X$ y $n_i \in Z$, $n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0 \Rightarrow n_i = 0$ para todo i.*

Antes de proceder a la demostración del siguiente teorema necesitamos algúnos resultados, los cuales enunciaremos a continuación (algúnos de ellos se aceptarán sin demostración, debido a que su prueba se ha realizado en cursos básicos de Álgebra Moderna).

Teorema 3.8 *Todo subgrupo H de un grupo aditivo Z es cíclico. También $H = \langle 0 \rangle$ o $H = \langle m \rangle$, donde m es el menor entero positivo en H. Si $H \neq \langle 0 \rangle$, entonces H es infinito.*

Demostración

Si $H = \langle 0 \rangle$ o H contiene un menor entero positivo m. Claramente $\langle m \rangle = \{km/k \in Z\} \subset H$. Opuestamente si $h \in H$, entonces $h = qm + r$ con $q, r \in Z$ y $0 \leq r \leq m-1$ (algoritmo de la división). Dado que $r = h - qm \in H$ la minimalidad de m implica $r = 0$ y $h = mq$. De aquí $H \subset \langle m \rangle$. Si $H \neq \langle 0 \rangle$, es claro que $H = \langle m \rangle$ es infinito.

⋆

Teorema 3.9 *Todo grupo cíclico infinito es isomorfo al grupo aditivo Z y todo grupo cíclico finito de orden m es isomorfo al grupo aditivo Z_m.*

Teorema 3.10 *Toda imagen homomórfica de todo subgrupo de un grupo cíclico G es cíclico. En particular, si H es un subgrupo no trivial de $G = \langle a \rangle$ y m es el menor entero positivo tal que $a^m \in H$, entonces $H = \langle a^m \rangle$.*

Demostración

Si $f : G \to K$ es un homorfismo de grupos, entonces $Im\ f = \langle f(a) \rangle$. Para probar la segunda parte simplemente traslademos la prueba del teorema (3.8) en notación multiplicativa (esto es, reemplazamos todo $t \in Z$ por a^t). Esta prueba se trabaja siempre que G es finito.

⋆

Teorema 3.11 *Las siguientes condiciones en un grupo abeliano F son equivalentes:*

i) *F tiene una base no vacía.*

ii) *F es la suma directa de una familia de subgrupos cíclicos infinitos.*

iii) *F es (isomorfo a) una suma directa de copias del grupo aditivo Z de los enteros.*

iv) *Existe un conjunto no vacío X y una función $i : X \to F$ con la siguiente propiedad: dado un grupo abeliano G y una función $f : X \to G$, existe un único homomorfismo de grupos $\bar{f} : F \to G$ tal que $\bar{f}i = f$. En otras palabras, F es un objeto libre en la categoría de grupos abelianos.*

Demostración

i) $\Rightarrow$ ii) Si X es una base de F, entonces para cada $x \in X$, $nx = 0$ si y solo si $n = 0$. De aquí que cada subgrupo $\langle x \rangle\,(x \in X)$ es cíclico infinito (y normal dado que F es abeliano). dado que $F = \langle X \rangle$, también tenemos que $F = \left\langle \bigcup_{x\in X} \langle x \rangle \right\rangle$. Si para algún $z \in X$, $\langle z \rangle \cap \left\langle \bigcup_{x\in X} \langle x \rangle \right\rangle \neq 0$, entonces para algún $n \in Z$ diferente de cero, $nz = n_1x_1 + n_2x_2 + \cdots + n_kx_k$ con $z, x_1, x_2, \ldots, x_k$ elementos distintos de X, que contradice el hecho que X es una base. Además $\langle z \rangle \cap \left\langle \bigcup_{x\in X} \langle x \rangle \right\rangle = 0$ y de aquí $F = \sum_{x\in X} \langle x \rangle$ por la definición (3.2).

ii) $\Rightarrow$ iii) Utilizando los teoremas (3.9), (3.5) y (3.7).

iii) $\Rightarrow$ i) Supongase que $F \cong \sum Z$ y las copias de Z estan indicadas por el conjunto X. Para cada $x \in X$, sea θ_x el elemento $\{u_i\}$ de $\sum Z$, donde $u_i = 0$ para $i \neq x$, y $u_x = 1$. Verifiquemos que $\{\theta_x / x \in X\}$ es una base de $\sum Z$ y use el isomorfismo $F \cong \sum Z$ para obtener una base de F.

i) $\Rightarrow$ iv) Sea X una base de F e $i : X \to F$ la función inclusión. Supongamos que esta dada por la función $f : X \to G$. Si $u \in F$, entonces $u = n_1x_1 + \cdots + n_kx_k$ $(n_i \in Z; x_i \in X)$ dado que X genera a F. Si $u = m_1x_1 + \cdots + m_kx_k(m_i \in Z)$, entonces $\sum_{i=1}^{k}(n_i - m_i)x_i = 0$, donde $n_i = m_i$ para todo i, dado que X es una base. Consecuentemente la función $\bar{f} : F \to G$, dada por $\bar{f}(u) = \bar{f}(\sum_{i=1}^{k} n_ix_i) = n_1f(x_1)+\cdots+n_kf(x_k)$, es una función bien definida tal que $\bar{f}i = f$. Dado que G es abeliano, $\bar{f}$ es un homomorfismo. De igual forma X genera a F, algún homomorfismo $F \to G$ está completamente determinado por su acción en X. Así, si $g : F \to G$ es un homomorfismo tal que $gi = f$, entonces para algún $x \in X$ $g(x) = g(i(x)) = f(x) = \bar{f}$, de donde $g = \bar{f}$ y $\bar{f}$ es única. Además, por la definición (1.6) es un objeto libre en el conjunto X en la categoría de grupos abelianos.

iv) $\Rightarrow$ iii) Dado $i : X \to F$, construyamos la suma directa $\sum Z$ con las copias de Z indicada por X. Sea $Y = \{\theta_x / x \in X\}$ una base de $\sum Z$ como en la prueba de iii) $\Rightarrow$ i). La prueba iii) $\Rightarrow$ i) $\Rightarrow$ iv) muestra que $\sum Z$ es un objeto libre en el conjunto Y. Dado que tenemos $|X| = |Y|$, $F \cong \sum Z$ por el teorema (1.3).

$\star$

Un grupo abeliano F que satisface las condiciones del teorema (3.11) es llamado un **grupo abeliano libre** (en el conjunto X). Por definición el grupo trivial 0 es el grupo abeliano libre en el conjunto nulo ϕ.

Dado algún conjunto X, la prueba del teorema (3.11) indica como se construye un grupo abeliano libre F con base X. Simplemente sea F la suma directa $\sum Z$, con las copias de Z indicada por X.

Como en la prueba de iii) $\Rightarrow$ i), $\{\theta_x/x \in X\}$ es una base de $F = \sum Z$, y F es libre en el conjunto $\{\theta_x/x \in X\}$. Dado que la función $i : X \to F$ dada por $x \mapsto \theta_x$ es inyectiva se sigue fácilmente que F es libre en X en el sentido de la condición iv) del teorema anterior. En esta situación identificamos X con su imagen bajo i, así que $X \subset F$ y el subgrupo cíclico $\langle\theta_x\rangle = \{n\theta_x/n \in Z\} = Z\theta_x$ es escrito como $\langle\theta_x\rangle = Zx$. Por lo tanto $F = \sum_{x\in X}\langle\theta_x\rangle$ es escrito $F = \sum_{x\in X} Zx$, y un elemento típico de F tiene la forma $n_1x_1 + \cdots + n_kx_k$ $(n_i \in Z, x_i \in X)$. En particular, $X = i(X)$ es una base de F.

Teorema 3.12 *Para dos cualesquiera bases de un grupo libre abeliano F tienen la misma cardinalidad.*

Demostración

Suponga primero que F tiene una base X de cardinal finito n, así que $F \cong Z \oplus \cdots \oplus Z$ (n sumandos). Para algún subgrupo G de F se tiene que $2G = \{2u/u \in G\}$ es un subgrupo de G. De la forma que la restricción del isomorfismo $F \cong Z\oplus\cdots\oplus Z$ a $2F$ es un isomorfismo $2F \cong 2Z\oplus\cdots\oplus 2Z$, donde $F/2F \cong Z/2Z \oplus \cdots \oplus Z/2Z \cong Z_2 \oplus \cdots \oplus Z_2$ (n sumandos) por la proposición (3.2). Además $|F/2F| = 2^n$. Si Y es otra base y r algún entero tal que $|Y| \geq r$. Entonces un argumento similar muestra que $|F/2F| \geq 2^r$, donde $2^r \leq 2^n$ y $r \leq n$. De aquí tenemos que $|Y| = m \leq n$ y $|F/2F| = 2^m$. Además $2^m = 2^n$ y $|X| = n = m = |Y|$.

Si una base de F es infinita, entonces todas las bases son infinitas esto por lo demostrado en el párrafo anterior. Consecuentemente, para completar la prueba es suficiente mostrar que $|X| = |F|$, si X es algúna base infinita de F. Claramente $|X| \leq |F|$. Sea $S = \bigcup_{n\in N^*} X^n$, donde $X^n = X\times\cdots\times X$ (n factores). Para cada $s = (x_1, \ldots, x_n) \in S$ sea G_s el subgrupo $\langle x_1, \ldots, x_n\rangle$. Donde $G_s \cong Z_{y_1}\oplus\cdots\oplus Z_{y_t}$ donde $y_1, \ldots, y_t (t \leq n)$ son elementos distintos de $\{x_1, \ldots, x_n\}$. Además, $|G_s| = |Z^t| = |Z| = N_0$. Dado $F = \bigcup_{s\in S} G_s$, tenemos que $|F| = |\bigcup_{s\in S} G_s| \leq |S|N_0$. Entonces $|S| = |X|$, donde $|F| = |X|N_0 = |X|$. Además $|F| = |X|$.

$\star$

El número cardinal de algúna base X de un grupo abeliano libre F es una invariante de F; $|X|$ es llamado el **rango** de F.

EJEMPLO 1

Si F_i es un grupo libre de rango r_i, entonces $F = Fr_{i\in I}$, F_i es un grupo libre de rango $\sum_{i\in I} r_i$. En particular, si cada F_i es cíclico infinito, F tiene rango $\mid I \mid$.

EJEMPLO 2

Sea A un conjunto y defina $G = Z^A$ e $i : A \to G$ por $i(a)(x) = 0$, si $x \neq a$ e $i(a)(a) = 1$ y si $x = a$ $\langle G, +, \bar{0}\rangle$ donde la suma es la usual entre funciones y $\bar{0}$ es la función que envía todo al 0, es un grupo abeliano. Ahora si H es un grupo abeliano, dado $f : A \to H$, defina $\bar{f} : g \to H$ por

$f(\sum_{a\in A} n_a i(a)) = \sum_{a\in A}(a)$ así $\bar{f} \circ i = f$. (G, A, i) es entonces grupo abeliano libre. Observese que si $\mid A \mid < \infty$, y $A = \{a_i\}_{i\in\{1,2,\ldots,n\}}$, bajo el isomorfismo que envía $g \in G$ al elemento cuya k-ésima entrada es $g(a_k)$, luego

$$G \approx \underbrace{Z \times Z \times \cdots \times Z}_{|A|}$$

Proposición 3.3 *Sea F_1 el grupo libre abeliano en el conjunto X_1 y F_2 el grupo libre abeliano en el conjunto X_2. Entonces $F_1 \cong F_2$ si y solo si F_1 y F_2 tienen el mismo rango (esto es, $|X_1| = |X_2|$).*

Demostración

Si $\alpha : F_1 \cong F_2$, entonces $\alpha(X_1)$ es una base de F_2 donde $|X_1| = |\alpha(X_1)| = |X_2|$ por el teorema (3.12).

$\star$

Esta proposición también es verdadera para un grupo arbitrario libre no abeliano:

Teorema 3.13 *Todo grupo abeliano G es imagen homomórfica de un grupo abeliano libre de rango $|X|$, donde X es el conjunto de generadores de G.*

Demostración

Sea F el grupo abeliano libre en el conjunto X. Entonces $F = \sum_{x\in X} Zx$ y rango $F = |X|$. Por el teorema (3.11), la función inclusión $X \to G$ induce un homomorfismo $\bar{f} : F \to G$ tal que $1x \mapsto x \in G$, donde $X \subset Im\ \bar{f}$. Dado que X genera a G tenemos que $Im\ \bar{f} = G$.

$\star$

Hemos probado un teorema que es extremadamente usado en el análisis de la estructura de generadores finitos de grupos abelianos.

Proposición 3.4 *Si $\{x_1, \ldots, x_n\}$ es una base de un grupo libre abeliano F y $a \in Z$, entonces para todo $i \neq j$ $\{x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\}$ también es una base de F.*

Demostración

Escribamos 0 como combinación lineal de elementos de la base $\{x_1, \ldots, x_{j-1}, x_j{+}ax_i, x_{j+1}, \ldots, x_n\}$ y probemos que los escalares son iguales a cero. Si $k_1x_1 + \cdots + k_j(x_j + ax_i) + \cdots + k_nx_n = 0 (k_i \in Z)$, entonces $k_1x_1 + \cdots + (k_i + k_ja)x_i + \cdots + k_jx_j + \cdots + k_nx_n = 0$, como los x_i son base por definición esto implica que $k_t = 0$ para todo t.

$\star$

Teorema 3.14 *Si F es un grupo abeliano libre de rango finito n y G es un subgrupo diferente de cero de F, entonces existe una base $\{x_1, \ldots, x_n\}$ de F, un entero r $(1 \leq r \leq n)$ y enteros positivos $d_1, \ldots, d_r$ tal que $d_1|d_2|\ldots|d_r$ y G es abeliano libre con base $\{d_1x_1, \ldots, d_rx_r\}$.*

Demostración

Si $n = 1$, entonces $F = \langle x_1 \rangle \cong Z$ y $G = \langle d_1 x_1 \rangle \cong Z(d_i \in N^*)$ por los teoremas (3.10), (3.8) y (3.9). Procediendo inductívamente, asumamos que el teorema es cierto para todos los grupos abelianos libres de rango menor que n. Sea S el conjunto de todos los enteros s tal que existe una base $\{y_1, \ldots, y_n\}$ de F y un elemento en G de la forma $sy_1 + k_2y_2 + \cdots + k_ny_n$ $(k_i \in Z)$. Note que en este caso $\{y_2, y_1, y_3, \ldots, y_n\}$ es también una base de F, donde $k_2 \in S$; similarmente $k_j \in S$ para $j = 3, 4, \ldots, n$. Dado que $G \neq 0$, tenemos que $S \neq \phi$. De aquí S contiene un menor entero positivo d_1 y para algúna base $\{y_1, \ldots, y_n\}$ de F existe un $v \in G$ tal que $v = d_1y_1 + k_2y_2 + \cdots + k_ny_n$. Por el algoritmo de la división para cada $i = 2, \ldots, n$, $k_i = d_1q_i + r_i$, con $0 \leq r_i < d_1$, donde $v = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n$. Sea $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$; por la proposición (3.4) $W = \{x_1, y_2, \ldots, y_n\}$ es base de F, la minimalidad de d_1 en S implica que $0 = r_2 = r_3 = \cdots = r_n$, así que $d_1x_1 = v \in G$.

Sea $H = \langle y_2, y_3, \ldots, y_n \rangle$. Entonces H es un grupo abeliano libre de rango $n-1$ tal que $F = \langle x_1 \rangle \oplus H$. Además vemos que $G = \langle v \rangle \oplus (G \cap H) = 0$. Si $u = t_1x_1 + t_2y_2 + \cdots + t_ny_n \in G(t_i \in Z)$, entonces por el algoritmo de la división $t_1 = d_1q_1 + r_1$ con $0 \leq r_1 < d_1$. Como $v \in G$ entonces $q_1v \in G$ y dado que $u \in G$ entonces G contiene a $u - q_1v = r_1x_1 + t_2y_2 + \cdots + t_ny_n$. La minimalidad de d_1 en S implica que $r_1 = 0$, de donde $t_2y_2 + \cdots + t_ny_n \in G \cap H$ y $u = q_1v + (t_2y_2 + \cdots + t_ny_n)$. Entonces $G = \langle v \rangle + (G \cap H)$, que prueba la suposición (definición (3.2)).

También $G \cap H = 0$, en tal caso $G = \langle d_1x_1 \rangle$ y el teorema es verdadero o $G \cap H \neq 0$. Entonces por la hipótesis inductiva existe una base $\{x_2, x_3, \ldots, x_n\}$ de H y enteros positivos $r, d_2, d_3, \ldots, d_r$ tal que $d_2|d_3| \ldots |d_r$ y $G \cap H$ es abeliano libre con base $\{d_2x_2, \ldots, d_rx_r\}$. Dado que $F = \langle x_1 \rangle \oplus H$ y $G = \langle d_1x_1 \rangle \oplus (G \cap H)$, se sigue fácilmente que $\{x_1, x_2, \ldots, x_n\}$ es una base de F y $\{d_1x_1, \ldots, d_rx_r\}$ es una base de G. Para completar el paso inductivo de la prueba necesitamos ver que $d_1|d_2$. Por el algorítmo de la división $d_2 = qd_1 + r_0$ con $0 \leq r_0 < d_1$. Dado que $\{x_2, x_1 + qx_2, x_3, \ldots, x_n\}$ es una base de F por la proposición (3.4) y $r_0x_2 + d_1(x_1 + qx_2) = d_1x_1 + d_2x_2 \in G$, la minimalidad de d_1 en S implica que $r_0 = 0$, de donde $d_1|d_2$.

$\star$

Todo subgrupo de un grupo abeliano libre de rango α (posiblemente infinito) es libre de rango a lo sumo α. La notación "$d_1|d_2| \ldots |d_r$"significa "d_1 divide a d_2, d_2 divide a d_3, etc".

Proposición 3.5 *Si G es un grupo abeliano finito generado por n elementos, entonces todo subgrupo H de G puede ser generado por m elementos con $m \leq n$.*

Demostración

Por el teorema (3.13) existe un grupo abeliano libre F de rango n y un epimorfismo $\pi : F \to G$.

$\pi^{-1}(H)$ es un subgrupo de F, y ademá, libre, de rango $m \leq n$ por el teorema (3.14). La imagen bajo π de algúna base de $\pi^{-1}(H)$ es un conjunto de a lo sumo m elementos que generan $\pi(\pi^{-1}(H)) = H$.

$\star$

La proposición es falsa si la palabra *abeliano* se omite.

4. Grupo Factor

En esta parte se estudiará como obtener una presentación para un grupo factor G/N de una presentación para G.

$$G = \langle a, b, c, \dots ; P, Q, R, \dots \rangle \tag{2}$$

En fin, para hacer esto debemos tener un subgrupo normal N dado en términos de la presentaciónn (2). Específicamente, debemos asumir que N esta definido como el subgrupo normal de G generado por las palabras $S(a, b, c, \dots), T(a, b, c, \dots), \dots$ (o, mas propiamente, por los elementos de G definidos por esas palabras).

Sabemos que un grupo puede tener muchas presentaciones, en 1908 H Tietze mostró que dada una presentación

$$\langle a, b, c, \dots ; P, Q, R, \dots \rangle \tag{3}$$

para un grupo G, puede obtenerse algúna otra presentación para G a traves de repetidas aplicaciones de las siguiente transformaciones a la presentación.

T1 Si las palabras $S, T, \dots$ son derivadas de $P, Q, R, \dots$, entonces agregamos $S, T, \dots$ a las relaciones definidas en (3).

T2 Si algúna de las relaciones, dígase $S, T, \dots$, listada entre las relaciones definidas $P, Q, R, \dots$, son derivables de las otras, pueden ser borradas $S, T, \dots$ de las relaciones definidas en (3).

T3 Si $K, M, \dots$ son algúnas palabras en $a, b, c, \dots$, y queremos agregar los símbolos $x, y, \dots$ a los símbolos generados en (3) y se cumplen las relaciones $x = K, y = M, \dots$ en las relaciones definidas en (3), entonces podemos reemplazarlas en 3.

T4 Si algúna de las relaciones definidas en (3) toma la forma $p = V, q = W, \dots$, donde $p, q, \dots$ son generadores en (3) y $V, W, \dots$, son palabras en los generadores mas que $p, q, \dots$, entonces borramos $p, q, \dots$ de los generadores, borramos $p = V, q = W, \dots$, de las relaciones definidas y reemplazamos $p, q, \dots$ por $p = V, q = W, \dots$, respectivamente, en las restantes relaciones definidas en (3).

T1, T2, T3 y T4 son llamadas **Transformaciones de Tietze**.

Teorema 4.1 *Dadas dos presentaciones para un grupo G,*

$$G = \langle a_1, a_2, \dots ; R_1(a_v), R_2(a_v), \dots \rangle \tag{4}$$

y

$$G = \langle b_1, b_2, \ldots ; S_1(b_\mu), S_2(b_\mu), \ldots \rangle \tag{5}$$

Entonces (5) *puede ser obtenida de* (4) *por una aplicación repetida de las transformaciones de Tietze (T1), (T2), (T3) y (T4).*

Demostración

Sea (4) una presentación de G bajo el mapeo

$$a_1 \to g_1, a_2 \to, \ldots \tag{6}$$

y sea (5) una presentación de G bajo el mapeo

$$b_1 \to h_1, b_2 \to h_2, \ldots \tag{7}$$

Mostraremos primero al cambiar (4) por las transformaciones de Tietze, así que los símbolos $b_1, b_2, \ldots$ de (5) aparecen como símbolos generados; para este propósito deseamos expresar $h_1, h_2, \ldots$ en términos de $g_1, g_2, \ldots$. Dado que $g_1, g_2, \ldots$ es un conjunto de elementos generados por G.

$$h_1 = B_1(g_1, g_2, \ldots), h_2 = B_2(g_1, g_2, \ldots), \ldots$$

Entonces por (T3), agregamos los nuevos símbolos $b_1, b_2, \ldots$ para generar los símbolos en (4), y agregamos las relaciones correspondientes

$$b_1 = B_1(g_1, g_2, \ldots), b_2 = B_2(g_1, g_2, \ldots), \ldots \tag{8}$$

obteniendo la siguiente presentación:

$$\langle a_1, a_2, \ldots, b_1, b_2, \ldots, R_1(a_v), R_2(a_v), \ldots, b_1 = B_1(a_v), b_2 = B_2(a_v), \ldots \rangle \tag{9}$$

Mas aún, G es presentado por (9) bajo el mapeo

$$a_1 \to g_1, a_2 \to g_2, \ldots, \qquad b_1 \to h_1, b_2 \to h_2, \ldots \tag{10}$$

determinado por (6) y (7).

Deseamos ahora volver a las relaciones definidas de (5) en (9). Para este propósito note que

$$S_1(b_1, b_2, \ldots), S_2(b_1, b_2, \ldots), \ldots \tag{11}$$

son relaciones bajo (10), dado que son relaciones bajo (7); de aquí,(11) pueden ser adjuntadas a las relaciones definidas en (9) por T1, obteniendo la presentación.

$$\langle a_1, a_2, \ldots, b_1, b_2, \ldots; R_1(a_v), R_2(a_v), \ldots, b_1 = B_1(a_v), b_2 = B_2(a_v), \ldots, S_1(b_\mu), S_2(b_\mu), \ldots \rangle \qquad (12)$$

la cual presenta a G bajo (10).

Deseamos ahora expresar $a_1, a_2, \ldots$ en términos de $b_1, b_2, \ldots$, así que podemos borrar $a_1, a_2, \ldots$ de (12); para este propósito se expresa $g_1, g_2, \ldots$ como palabras en $h_1, h_2, \ldots$. Dado que $h_1, h_2, \ldots$ es un conjunto de elementos generadores de G,

$$g_1 = A_1(h_1, h_2, \ldots), \qquad g_2 = A_2(h_1, h_2, \ldots), \ldots$$

De aquí, bajo la función (10)

$$a_1 = A_1(b_1, b_2, \ldots), \qquad a_2 = A_2(b_1, b_2, \ldots), \ldots \qquad (13)$$

Como relaciones en G, y de aquí se deriva de la definición de relaciones en (12). Así, por (T1) podemos agregar las relaciones (13) para las relaciones definidas en (12), obtenemos las presentación

$$\langle a_1, a_2, \ldots, b_1, b_2, \ldots; R_1(a_v), R_2(a_v), \ldots, b_1 = B_1(a_v), b_2 = B_2(a_v), \ldots, S_1(b_\mu), S_2(b_\mu), \ldots, a_1 = A_1(b_\mu), a_2 = A \qquad (14)$$

En lugar de borrar $a_1, a_2, \ldots$ como se habia planeado, observemos que (14) es simétrico; de aquí, podemos obtener (14) de (5) por las transformaciones de Tietze. Dado que el inverso de las transformaciones de Tietze es una secuencia de las transformaciones de Tietze, se tiene (5) de (14) por una secuencia de las transformaciones de Tietze. Así, (5) puede obtenerse de (4) por una aplicación repetida de las transformaciones de Tietze.

$\star$

Proposición 4.1 *Si las presentaciones* (4) *y* (5) *en el teorema* (4.1) *son finitas, entonces* (4) *puede ser cambiado en* (5) *por una secuencia finita de transformaciones de Tietze elementales.*

Demostración

Si las presentaciones (4) y (5) son finitas, entonces las relaciones (8), (11) y (13) son finitas en número y así pueden ser agregadas una a una en (4), por transformaciones de Tietze elementales, para obtener (14). Similarmente (5) puede obtenerse de (14) por un número finitos de transformaciones de Tietze elementales.

$\star$

Definición 4.1 *El subgrupo normal de un grupo generado por un conjunto de elementos, es el menor subgrupo normal que contiene esos elementos, o equivalentemente, es el subgrupo generado por el conjunto de elementos y sus conjugados.*

Podemos afirmar lo siguiente:

Teorema 4.2 *Sea G que tiene presentación (2) bajo la función:*

$$a \to g, \qquad b \to h \qquad c \to k, \dots, \tag{15}$$

y sea N el subgrupo normal de G generado por $S(g,h,k,\dots)$, $T(g,h,k,\dots)$, $\dots$. Entonces el grupo factor G/N tiene la presentación

$$\langle a, b, c, \dots ; P, Q, R, \dots, S, T. \dots \rangle \tag{16}$$

bajo la función

$$a \to gN, \qquad b \to hN \qquad c \to kN, \dots, \tag{17}$$

Demostración

Bajo la función (17), la palabra $W(a,b,c,\dots)$ lleva a $W(gN,hN,kN,\dots) = W(g,h,k,\dots)N$. Dado que G tiene presentación (2) y N es el subgrupo normal generado por $S(g,h,k,\dots)$, $T(g,h,k,\dots)$, $\dots$, el elemento de G definido por $P,Q,R,\dots,S,T,\dots$ son relaciones en G/N bajo (17) y así (17) induce un homomorfismo en G/N.

$\star$

Dado que G es generado por $g,h,k,\dots$, entonces G/N es generado por $gN,hN,kN,\dots$ y así el homomorfismo inducido por (17) es sobre.

Para mostrar que este homomorfismo es uno a uno, supongamos que $W(a,b,c,\dots)$ es mapeada en la identidad en G/N. Entonces $W(g,h,k,\dots)$ está en N. Dado que N es el subgrupo normal de G generado por $S,T,\dots$,

$$W(g,h,k,\dots) = U_1V_1U_1^{-1}\dots U_rV_rU_r^{-1} \tag{18}$$

donde U_i son elementos de G y V_i es uno de $S,S^{-1},T,T^{-1},\dots$. De aquí,

$$W(a,b,c,\dots) \sim U_1V_1U_1^{-1}\dots U_rV_rU_r^{-1} \tag{19}$$

con respecto a la presentación (2) para G. Así $W(a,b,c,\dots)$ puede ser cambiada al lado derecho de (19) por inserción y supresión de las relaciones definidas en (2) y relaciones triviales. Pero el lado derecho de (19) puede reducirse a la palabra vacía por inserción y supresión de $S,T,\dots$ y la relación trivial. Así $W(a,b,c,\dots) \sim 1$ en la presentación (16), y de aquí, el homomorfismo inducido por (17) es uno a uno de (16) a G/N.

Proposición 4.2 *Si F es el grupo libre en $a, b, c, \ldots$ y N es el subgrupo normal de F generado por $P(a, b, c, \ldots)$, $Q(a, b, c, \ldots)$, $R(a, b, c, \ldots)$, $\ldots$, entonces*

$$F/N = \langle a, b, c, \ldots ; P, Q, R, \ldots \rangle \tag{20}$$

Demostración

Se sigue inmediatamente del teorema (4.2)

$\star$

(Algunos autores definen los grupos libres sin la primera definición general que era la presentación (2); ellos toman (20) como la definición de la presentación (2)).

5. Subgrupos verbales y grupos reducidos libres

Un subgrupo normal o invariante N de un grupo G es cerrado bajo el producto de automorfismos conjugados. Un subgrupo K de G es llamado **característica**, si K es cerrado bajo todos los automorfismos de G. Un subgrupo característico es necesariamente normal, pero no lo contrario. Una propiedad siempre fuerte de un subgrupo es que su característica es *totalmente invariante*, cerrada bajo todos los endomorfismos de G (homomorfismos de G inyectivos en ellos mismos). El concepto de un "subgrupo verbal"será construido con muchos ejemplos de los subgrupos totalmente invariantes de un grupo G.

Sea $W_\mu(X_\lambda)$, donde $\mu = 1, 2, \ldots$, es el conjunto de las palabras en los símbolos X_λ, donde $\lambda = 1, 2, \ldots$. Entonces el $\{W_\mu\}$-subgrupo verbal $G(W_\mu, \ldots)$ de un grupo G es el subgrupo de G generado por todos los elementos de la forma $W_\mu(g_\lambda)$, donde g_λ es el rango sobre G.

EJEMPLO 1

$G(X^2)$ es el grupo de G generado por los cuadrados g^2 de todos los elementos g de G. El subgrupo verbal $G(X^4, X^6)$ es el mismo que $G(X^2)$. El **subgrupo conmutador** de G es el subgrupo verbal $G(X_1X_2X_1^{-1}X_2^{-1})$ generado por todos los elementos $g_1g_2g_1^{-1}g_2^{-1}$ de G. El subgrupo verbal $G(X)$, es claramente G. El subgrupo verbal $G(X_1X_2)$ es también G; para $G(X_1X_2) \subset G$ y sustituyendo g por X_1 y 1 por X_2 obtenemos todos los elementos de G. Si $\sum_n$ es el grupo simétrico en 1,2, $\ldots$, n entonces $\sum_n(X^3)$ es $\sum_n$; para $\sum_n$ es generado por un dos-cíclico y el cubo de un dos-cíclico es el mismo. Por otro lado $\sum_n(X^2)$ es A_n, el grupo alternante en 1,2,$\ldots$, n; para el cuadrado de una permutación es par, y A_n es generado por los tres-cíclicos, los cuales son cuadrados.

El subgrupo verbal $G(W_\mu, \ldots)$ es un subgrupo totalmente invariante de G. Sea α un endomorfismo de G. Entonces $\alpha(W_\mu(g_\lambda)) = W_\mu(\alpha(g_\lambda))$. De aquí, $\alpha(W_\mu(g_\lambda))$ puede ser obtenido por sustitución de $\alpha(g_\lambda)$ por X_λ en $W_\mu(X_\lambda)$, y así estar en $G(W_\mu, \ldots)$. Luego, $G(W_\mu, \ldots)$ es totalmente invariante.

No todo subgrupo totalmente invariante de un grupo G necesita ser verbal. Es decir, existe una clase importante de grupos para los que esto es cierto.

Un grupo libre reducido R de rango n con las identidades $W_\mu(X_\lambda) = 1$ es el grupo factor de el grupo libre F_n de rango n por el subgrupo verbal $F_n(W_\mu, \ldots)$. Equivalentemente, por la proposición (4.2), el grupo libre reducido R puede ser definido como el grupo:

$$\langle a_1, a_2, \ldots, a_n; W_\mu(U_\lambda(a_1, a_2, \ldots, a_n)), \ldots\rangle \tag{21}$$

donde U_λ es el rango sobre todas las palabras en $a_1, a_2, \ldots, a_n$. Note que, en general, no podemos restringir U_λ al rango solo sobre los generadores $a_1, a_2, \ldots, a_n$. A menudo denotamos R simplemente por:

$$\langle a_1, a_2, \ldots, a_n; W_\mu(X_\lambda), \ldots \rangle \tag{22}$$

Es claro, de la presentación de (21), que algún grupo G en n generadores, en los cuales las identidades $W_\mu(X_\lambda) = 1$ se mantienen, en las que $W_\mu(X_\lambda) = 1$ para algún g_λ en G, es un homomorfismo imagen de los grupos libres reducidos de rango n con las identidades $W_\mu(X_\lambda) = 1$.

Si F_n es el grupo libre en $a_1, a_2, \ldots, a_n$, entonces F_n es caracterizado por el hecho que lleva a estos generadores en algún grupo G, que puede ser extendido por un homomorfismo de F_n en G. Entonces el siguiente lema generaliza este tipo de caracterización a grupos libres reducidos.

Lema 5.1 *Sea R un grupo en el que las identidades $W_\mu(X_\lambda) = 1$ se mantienen. Entonces R es el grupo libre reducido de rango n con esas identidades si y solo si existen n generadores $a_1, a_2, \ldots, a_n$ de R tal que algún mapeo de estos generadores en un grupo G, en el cual las identidades dadas se mantengan, puede ser extendido a un homomorfismo de R en G.*

Demostración

Sea R el grupo libre reducido con la presentación (21). Entonces por la proposición (4.2), algún mapeo de $a_1, a_2, \ldots, a_n$ en un grupo G, en el cual las identidades $W_\mu(X_\lambda) = 1$ se mantengan, puede ser extendido a un homomorfismo de R en G.

De manera análoga, supongamos que las identidades $W_\mu(X_\lambda) = 1$ se mantienen en R, y R tiene n generadores $a_1, a_2, \ldots, a_n$ tal que algún mapeo de $a_1, a_2, \ldots, a_n$ en un grupo G en el cual las identidades $W_\mu(X_\lambda) = 1$ se mantienen, puede ser extendido a un homomorfismo de R en G. Sea

$$G = \langle b_1, b_2, \ldots, b_n; W_\mu(X_\lambda), \ldots \rangle \tag{23}$$

Entonces las identidades $W_\mu(X_\lambda) = 1$ se mantienen en G, y la función $a_v \to b_v$ puede ser extendida a un homomorfismo de R en G. Además, si $P(a_v)$ es una relación en R, entonces $P(b_v)$ es una relación en (23). De aquí, $P(b_v)$ es derivable de las palabras $W_\mu(U_\lambda(b_1, b_2, \ldots, b_n))$ y así $P(a_v)$ es derivable de las palabras $W_\mu(U_\lambda(a_1, a_2, \ldots, a_n))$. Entonces R tiene la presentación

$$\langle a_1, a_2, \ldots, a_n; W_\mu(U_\lambda(a_1, a_2, \ldots, a_n)), \ldots \rangle$$

y así es un grupo libre reducido de rango n con identidades $W_\mu(X_\lambda) = 1$.

⋆

Teorema 5.1 *Todo subgrupo totalmente invariante J de un grupo reducido R de rango n (y, en particular, de un grupo libre) es un subgrupo verbal $R(V_p, \ldots)$. Mas aún, podemos elegir las palabras $V_p(Y_v)$ definidas en J así que el número de símbolos Y_v usados es n.*

Demostración

Sea R que tiene representación

$$\langle a_1, a_2, \dots, a_n; W_\mu(X_\lambda(a_1, a_2, \dots, a_n)), \dots \rangle$$

y considere el conjunto de todas las palabras $V_p(Y_1, \dots, Y_n)$ tal que

$$V_p(a_1, \dots, a_n) \tag{24}$$

está en J. Mostremos que $J = R(V_p, \dots)$.

Claramente, $V_p(a_1, \dots, a_n)$ es el rango sobre todos los elementos de J, y así $J \subset R(V_p, \dots)$.

Opuestamente, consideremos algún elemento

$$V_p(U_1(a_v), \dots, U_n(a_v)) \tag{25}$$

Ahora la función $a_i \to U_i(a_v)$ puede ser extendida a un endomorfismo de R por el lema. De aquí, dado (24) está en el subgrupo totalmente invariante J, y (24) lleva a (25) bajo el endomorfismo, (25) puede estar en J. Pero el elemento en (25) generado por $R(V_p, \dots)$. Así $R(V_p, \dots) \subset J$, y así $J = R(V_p, \dots)$.

$\star$

Pero además para grupos reducidos libres está dado por el siguiente teorema, el cual es parecido a F. Levi, 1993. Pero antes de probar el teorema, necesitamos la siguiente definición:

Definición 5.1 *Si W es una palabra en $a_1, a_2 \dots, a_n$, y*

$$W = a_{v_1}^{\alpha_1}, a_{v_2}^{\alpha_2} \dots, a_{v_n}^{\alpha_n}$$

donde los α_i son enteros y $v_i = 1, 2, \dots, n$, entonces el ***exponente suma de** W **en** a_v es el entero*

$$\sigma_v(W) = \sum_{v_i = v} \alpha_i$$

EJEMPLO

Si $W = a_1^2 a_2 a_1^{-3} a_2^{-1} a_1^{-1}$ entonces $\sigma_1(W) = -2$ y $\sigma_2(W) = 0$.

Claramente, si $W_1 \approx W_2$, entonces $\sigma_v(W_1) = \sigma_v(W_2)$; mas aún, $\sigma_v(UV) = \sigma_v(U) + \sigma_v(V)$. De aquí, $W \to \sigma_v(W)$ es un homomorfismo de F_n, el grupo libre en $a_1, \dots, a_n$, sobre el grupo aditivo de los enteros. Tales elementos de F_n son el núcleo del homomorfismo σ_v. Esos elementos con el exponente suma cero en a_v es el mismo que el subgrupo normal de F_n están en el núcleo de todos los homomorfismo σ_v. Estos elementos con el exponente suma cero en todos los a_v; es el mismo que el subgrupo conmutador de F_n.

Teorema 5.2 *Sea $W_\mu(X_\lambda$ el conjunto de todos los elementos en el grupo libre F en $X_1, X_2, \ldots, X_n$. Entonces existe un entero no negativo d y un conjunto de palabras $V_\mu(X_\lambda$ en el subgrupo conmutador de F tal que para algún grupo G,*

$$G(W_\mu, \ldots) = G(X_1^d, V_\mu, \ldots)$$

Demostración

Sea d el máximo común divisor del conjunto de los enteros $\sigma_\lambda(W_\mu)$ donde λ y μ son el rango sobre todos los posibles valores. Sea

$$V_\mu = W_\mu X_1^{-\beta_1}, \ldots, X_n^{-\beta_n} \tag{26}$$

donde $\beta_\lambda = \sigma_\lambda(W_\mu)$.

Claramente $\sigma_\lambda(V_\mu) = \sigma_\lambda(W_\mu) - \beta_\lambda = 0$. De aquí V_μ es el subgrupo conmutador de F, el grupo libre en X_λ.

Mostraremos ahora que si G es algún subgrupo entonces $G(W_\mu, \ldots) = G(X_1^d, V_\mu, \ldots)$.

Para ellos dado que $d|\beta_\lambda$, claramente si g_λ está en G, entonces $g_\lambda^{\beta_\lambda}$ está en $G(X_1^d, V_\mu, \ldots)$. De aquí,

$$W_\mu(g_\lambda) = V_\mu(g_\lambda g_n^{\beta_\lambda} \ldots g_1^{\beta_\lambda}$$

está en $G(X_1^d, V_\mu, \ldots)$, y así $G(W_\mu, \ldots) \subset G(X_1^d, V_\mu, \ldots)$.

Dicho de otra manera, en $W_\mu(X_\lambda)$ sustituyamos g por X_v y 1 por X_λ, $\lambda \neq v$; entonces resulta el elemento g^{β_v}. Dado que g^{β_v} está en $G(W_\mu, \ldots)$ para todo β_v, se sigue que g^d está en $G(W_\mu, \ldots)$. Pero entonces de (26), $V_\mu(g_\lambda$ puede estar en $G(W_\mu, \ldots)$. De aquí $G(X_1^d, V_\mu, \ldots) \subset G(W_\mu, \ldots)$, y así los dos subgrupos verbales serán iguales.

$\star$

Proposición 5.1 *Todo grupo libre reducido de rango n tiene una presentación*

$$\langle a_1, \ldots, a_n; X_1^d, W_\mu(X_\lambda), \ldots \rangle \tag{27}$$

donde d es un entero no negativo, $\lambda = 1, \ldots, n$ y W_μ está en el subgrupo conmutador de F, el grupo libre en $X_1, \ldots, X_n$.

Demostración

La prueba es inmediata de los teoremas (5.1) y (5.2)

$\star$

Proposición 5.2 *Solo los subgrupos verbales de un grupo abeliano G son los* ***subgrupos potencia*** *$G(X_1^d)$*

Demostración

Algún elemento de un subgrupo conmutador de un grupo abeliano es la identidad. De aquí, $G(X_1^d, V_\mu, \ldots)$ se reduce a $G(X_1^d)$.

$\star$

Usando el teorema (5.2), podemos clasificar todos los grupos abelianos libres reducidos.

El grupo abeliano libre A_n de rango n (n posiblemente finito) es el grupo libre reducido

$$\langle a_1, \ldots, a_n; X_1 X_2 X_1^{-1} X_2^{-1} \rangle \tag{28}$$

Este es el grupo cociente de el grupo libre F_n por su subgrupo conmutador.

El grupo A_n es isomorfo al grupo aditivo de todos los vectores

$$(\alpha_1, \ldots, \alpha_n)$$

con componentes del anillo de enteros (y todos finitos y algúnas componentes igual a cero) bajo la función

$$W(a_1, \ldots, a_n) \to (\sigma_1(W), \ldots, \sigma_n(W))$$

El grupo abeliano libre $A_{n,d}$ de rango n y exponente d (donde n es posiblemente finito y d es un entero mayor que 1) es el grupo libre reducido

$$\langle a_1, \ldots, a_n; X_1^d X_1 X_2 X_1^{-1} X_2^{-1} \rangle$$

El grupo $A_{n,d}$ es isomorfo al grupo aditivo de todos los vectores

$$(\alpha_1, \ldots, \alpha_n)$$

Con coordenadas del anillo de enteros módulo d (y todos finitos y algúnos iguales a cero) bajo la función

$$W(a_1, \ldots, a_n) \to (\alpha_1, \ldots, \alpha_n)$$

donde $\alpha_v = \sigma_v(W) \bmod d$.

Es fácil ver de esta representación de $A_{n,d}$ que su orden es d^n si n es finito, y n si n es infinito; mas aún, d es el máximo orden de algún elemento. De aquí, si $A_{n,d}$ es isomorfo a $A_{m,c}$, entonces $d = c$ y $n = m$.

Claramente, el número más pequeño de generadores de $A_{n,d}$ es n. Pero, si $A_{n,d}$ tiene p generadores, este es isomorfo a la imagen de $A_{p,d}$ (dado $X_1^d = 1$ y $X_1 X_2 X_1^{-1} X_2^{-1} = 1$ son identidades que se mantienen en $A_{n,d}$); de aquí, el orden de $A_{n,d}$ puede ser menor o igual al orden de $A_{p,d}$. Esto implica $n \leq p$.

Esto remarca el hecho que n es el menor número de generadores para algún grupo libre reducido de rango n.

Teorema 5.3 *Un grupo libre reducido R de rango n ($R \neq 1$) no puede ser generado por menos que n elementos. De aquí, los grupos libres reducidos, y, en particular, los grupos libres y grupos libres abelianos, de diferentes rangos no pueden ser isomórficos.*

Demostración

Por la proposición (5.1) podemos asumir que

$$R = \langle a_1, \ldots, a_n; X_1^d, W_\mu(X_\lambda), \ldots \rangle$$

donde d es mayor que 1 o $d = 0$ (dado que $R \neq 1$), y W_μ es el subgrupo conmutador de F, el grupo libre en X_λ. Si p es algún divisor de d, p mayor que 1, entonces

$$A_{n,d} = \langle a_1, \dots, a_n; X_1^p X_1 X_2 X_1^{-1} X_2^{-1} \rangle$$

es isomorfo a la imagen de R; claramente las identidades $X_1^d = 1$ y $W_\mu(X_\lambda) = 1$ se mantienen en $A_{n,p}$. De aquí, si R tiene menos de n generadores, entonces es $A_{n,p}$; pero $A_{n,p}$ no puede tener menos de n generadores. Así R no puede tener menos de n generadores.

$\star$

El teorema (5.3) resuelve el problema del isomorfismo para dos grupos libres, tanto como para dos grupos libres abelianos presentados como tales. Mas aún, el concepto de subgrupo verbal puede ser usado como un parámetro para probar isomorfismo.

Teorema 5.4 *Sea $\{W_\mu(X_\lambda)\}$ el conjunto de palabras. Entonces si dos grupos G_1 y G_2 son isomórficos, los grupos Γ_1 y Γ_2, donde*

$$\Gamma_i = G_i / G_i(W_\mu, \dots)$$

son también isomórficos.

Demostración

Bajo un isomorfismo de G_1 sobre G_2, $G_1(W_\mu, \dots)$ lleva sobre $G_2(W_\mu, \dots)$. Mas aún las clases de Γ_1 llevan isomorficamente sobre las clases de Γ_2.

$\star$

En vista de la infinita variedad de subgrupos verbales, puede verse que el teorema (5.4) posee un número infinito de pruebas utilizadas para isomorfismos. Sin embargo todos los teoremas (5.4) son reducidos al isomorfismo de G_1 y G_2 para el de Γ_1 y Γ_2. Si Γ_1 y Γ_2 son grupos abelianos generados finitamente, o son grupos abelianos finitos generados sobre un (ideal principal) operadores de anillos, entonces el isomorfismo de Γ_1 y Γ_2 puede ser resuelto. Si Γ_1 y Γ_2 son generados finitamente y las palabras W_μ son *conmutadores simples*, entonces el isomorfismo de Γ_1 y Γ_2 puede ser resuelto. En general, no existen pruebas para resolver si Γ_1 y Γ_2 son isomórficos.

El estudio de los grupos libres reducidos con la identidad $X^d = 1$, dejan algo de problemas difíciles (excepto para algún valor especial de d), la mayoría de los cuales estan todavía sin resolver.

La *variedad de grupos* correspondientes a las identidades $\{W_\mu(X_\lambda) = 1\}$ es justamente el conjunto de grupos en el cual las identidades $W_\mu(X_\lambda) = 1$ se mantienen.

Los términos *endomorfismo* y *totalmente invariante* fueron introducidos por F. Levi, 1933. La mayoría de resultados de este sección son junto a B. H. Neumann, 1937.

6. Presentación de Subgrupos (El método de Reidemeister-Schreier)

Sea G un grupo con presentación

$$G = \langle a_1, \ldots, a_n; R_\mu(a_v), \ldots \rangle \tag{29}$$

Ya vimos como se presenta un grupo factor G/N de G; ahora veremos como se presenta un subgrupo H de G.

Para presentar el grupo factor G/N requerimos palabras en el a_v, las cuales generan el subgrupo normal N; para presentar el subgrupo H requerimos que las palabras en el a_v, las cuales generan el subgrupo H. Pero además estos son generadores para H, requerimos de un proceso para reescribir una palabra en el a_v el cual define un elemento de H, como una palabra en los generadores de H.

Específicamente, sea G presentado como en (29), y sea H el subgrupo de G generador por las palabras $J_i(a_v), \ldots$ entonces por un *proceso de reescritura* para H (con respecto a los generadores $J_i(a_v)$) es una función.

$$\tau : U(a_v) \to V(s_i) \tag{30}$$

de palabras $U(a_v)$ la cual define elementos de H, en palabras en símbolos s_i, tal que las palabras

$$U(a_v), \qquad V(J_i(a_v))$$

define el mismo elemento de H. (El símbolo s_i sera el símbolo generador usado para $J_i(a_v)$ en la presentación de H).

EJEMPLO 1

Sea G el grupo libre en a y b, y sea H el subgrupo normal de G generador por b. Entonces H es generado por b y sus conjugados por potencias de a, para $a^k b a^{-k}$, donde k es algún entero. Sea

$$J_k(a,b) = a^k b a^{-k}$$

Una palabra $W(a,b)$ define un elemento de H si y solo si el exponente suma de W en a es cero. Además, si

$$U(a,b) = a^{\alpha_1} b^{\beta_1} a^{\alpha_2} b^{\beta_2} \dots a^{\alpha_r} b^{\beta_r} \tag{31}$$

tiene exponente suma cero en a, entonces $U(a,b)$ y

$$(a^{\alpha_1} b a^{-\alpha_1})^{\beta_1} (a^{\alpha_1+\alpha_2} b a^{-\alpha_1-\alpha_2})^{\beta_2} \dots (a^{\alpha_1+\alpha_2+\cdots+\alpha_r} b a^{-\alpha_1-\alpha_2-\cdots-\alpha_r})^{\beta_r}$$

define el mismo elemento de H. De aquí, la función τ que envia la palabra en (31) en

$$s_{\alpha_1}^{\beta_1} s_{\alpha_1+\alpha_2}^{\beta_2} \dots s_{\alpha_1+\alpha_2+\cdots+\alpha_r}^{\beta_r} \tag{32}$$

es un proceso de reescritura para H.

Deseamos ahora para presentar un subgrupo H de un grupo G dado por (29), usando los símbolos generadores s_i para generar elementos $J_i(a_v)$.

Teorema 6.1 *Sea H un subgrupo de un grupo G presentado en (29). Si $J_i(a_v)$ son generadores para H y la función τ es un proceso de reescritura para H (con respecto a los generadores $J_i(a_v)$), entonces un presentación para H bajo la función $s_i \to J_i(a_v)$ se obtiene por el uso de los símbolos s_i como símbolos generadores y usando las siguientes ecuaciones como relaciones definidas:*

$$s_i = \tau(J_i(a_v)) \tag{33}$$

$$\tau(U) = \tau(U^*) \tag{34}$$

donde $U(a_v)$ y $U^*(a_v)$ son palabras libremente iguales las cuales definen elementos de H.

$$\tau(U_1 U_2) = \tau(U_1)\tau(U_2) \tag{35}$$

donde $U_1(a_v)$ y $U_2(a_v)$ definen elementos de H; y

$$\tau(WR_\mu W^{-1}) = 1 \tag{36}$$

donde $R_\mu(a_v)$ es una relación definida en (29) y W es alguna palabra en a_v

Demostración

Primero mostraremos que (33), (34), (35) y (36) son relaciones. Pero, si $U(a_v)$ define un elemento de H, y

$$\tau(U(a_v)) = V(s_i)$$

entonces $U(a_v)$ y $V(J_i(a_v))$ definen el mismo elemento de H, por definición del proceso de reescritura. De aquí, bajo la función $s_i \to J_i(a_v)$, las ecuaciones (33), (34), (35) y (36) son relaciones.

Para mostrar que (33), (34), (35) y (36) definen relaciones, debemos mostrar que algúna relación

$$s_{i_1}^{\epsilon_1} \dots s_{i_r}^{\epsilon_r} \qquad (\epsilon_{i_j} = \pm 1) \tag{37}$$

puede ser reducida a la palabra vacía utilizando las relaciones (33), (34), (35) y (36). Es conveniente primero derivar algunas relaciones de (33), (34), (35) y (36); el término *derivar* significa obtener con respecto a (33), (34), (35) y (36).

En (35), si reemplazamos U_1 y U_2 por la palabra vacía 1, obtenemos $\tau(1) = \tau(1)\tau(1)$ o equivalentemente $\tau(1) = 1$. Ahora en (35) reemplacemos U_2 por U_1^{-1}, y usemos (34) para obtener $\tau(U_1)\tau(U_1^{-1}) = 1$, o equivalentemente

$$\tau(U_1^{-1}) = \tau(U_1)^{-1} \tag{38}$$

De aquí, de (35) y (38) podemos obtener

$$\tau(U_1^{\epsilon_1} \dots U_p^{\epsilon_p}) = \tau(U_1)^{\epsilon_1} \dots \tau(U_p)^{\epsilon_p} \tag{39}$$

Ahora demostraremos que podemos obtener la ecuacion (37). Usando (33), (37) puede ser reemplazado por

$$\tau(J_{i_1}(a_v))^{\epsilon_1}\ldots\tau(J_{i_r}(a_v))^{\epsilon_r}$$

la cual por (39) puede ser reemplazada por

$$\tau(J_{i_1}^{\epsilon_1}\ldots J_{i_r}^{\epsilon_r}) \tag{40}$$

Ahora, dado (37) es una relación bajo $s_i \to J_i(a_v)$.

$$J_{i_1}(a_v)^{\epsilon_1}\ldots J_{i_r}(a_v)^{\epsilon_r} \tag{41}$$

define la identidad en H, y de aquí, tambien en G. Dado que G tiene la representación (29), se sigue de la proposición (4.2) que (41) es igualmente libre a un producto

$$(W_1R_{\mu_1}W_1^{-1})^{\eta_1}\ldots(W_tR_{\mu_t}W_t^{-1})^{\eta_t} \tag{42}$$

donde $\eta_j = \pm 1$ y R_{μ_j} es una relación definido en (29). De aquí, usando (34), (40) puede ser reemplazado por

$$\tau((W_1R_{\mu_1}W_1^{-1})^{\eta_1}\ldots(W_tR_{\mu_t}W_t^{-1})^{\eta_t}) \tag{43}$$

Usando (39), (43) puede ser reemplazado por

$$\tau(W_1R_{\mu_1}W_1^{-1})^{\eta_1}\ldots\tau(W_tR_{\mu_t}W_t^{-1})^{\eta_t}) \tag{44}$$

Pero entonces las relaciones en (36) nos permiten reducir (44) a la palabra vacía.

$\star$

La presentación para H obtenida en el teorema (6.1) es muy engorrosa.

Por una elección de manera cuerda de generadores y el proceso de reescritura, la presentación puede ser grandemente simplificada. Una eleccion tal que puede ser usado una *función clase derecha* para G mod H, obtenemos ambos generadores y un proceso de reescritura.

Si G tiene la presentación (29), entonces *la función representante clase derecha para G (en los generadores a_v) modulo un subgrupo de H*, es una función de palabras en a_v,

$$W(a_v) \to \overline{W}(a_v)$$

donde $\overline{W}(a_v)$ forma una clase derecha de sistemas representantes de G mod H, los cuales contienen la palabra vacía, y donde $\overline{W}(a_v)$ es la representante de la clase de $W(a_v)$.

Teorema 6.2 *Si $W \to \overline{W}$ es una función clase derecha para G mod H, entonces H es generado por las palabras*

$$Ka_v\overline{Ka_v}^{-1} \tag{45}$$

donde K es un representante arbitrario y a_v es un generador para G.

Demostración

Para mostrar que las palabras en (45) son generadores para H, es coveniente usar la siguiente propiedad que es fácil de verificar de una función representante clase derecha:

1. $\overline{W} = 1$ si y solo si W define un elemento de H
2. W es libremente igual a V implica que $\overline{W} = \overline{V}$
3. $\overline{\overline{W}} = \overline{W}$
4. $\overline{WV} = \overline{\overline{W}V}$

   La palabra $Ka_v\overline{Ka_v}^{-1}$ claramente define un elemento de H; para Ka_v y $\overline{Ka_v}$ determina la misma clase derecha de H.

   Ahora mostraremos que todo elemento de H puede ser expresado como un producto de palabras en (45) y sus inversos.

   Primero observese que la palabra

$$Ka_v^{-1}\overline{Ka_v^{-1}}^{-1} \tag{46}$$

   es el inverso de una palabra en (45), para un K dado que es representante, se sigue que

$$\overline{\overline{Ka_v^{-1}}a_v} = \overline{Ka_v^{-1}a_v} = \overline{K} = K$$

usando 4,2 y 3. De aquí, (46) es el inverso de la palabra $Ma_v\overline{Ma_v}^{-1}$ donde $M = \overline{Ka_v^{-1}}$, el cual es incluido en (45).

Supongamos ahora que

$$U = a_{v_1}^{\epsilon_1} a_{v_2}^{\epsilon_2} \dots a_{v_r}^{\epsilon_r} \qquad (\epsilon_i = \pm 1) \tag{47}$$

define un elemento de H; debemos expresar U en términos de las palabras en (45) y (46). Por eso insertaremos antes y después de cada $a_{v_j}^{\epsilon_j}$ en U, las palabras $\overline{W_j}$ y $\overline{W_j a_{v_j}^{\epsilon_j}}^{-1}$, respectivamente, y tratando de elegir el W_j así para nuestro nuevo producto,

$$\overline{W}_1 a_{v_1}^{\epsilon_1} \overline{W_1 a_{v_1}^{\epsilon_1}}^{-1} \overline{W}_2 a_{v_2}^{\epsilon_2} \overline{W_2 a_{v_2}^{\epsilon_2}}^{-1} \dots \overline{W}_r a_{v_r}^{\epsilon_r} \overline{W_r a_{v_r}^{\epsilon_r}}^{-1} \tag{48}$$

define el mismo elemento de H como en (47). Ahora, (48) ciertamente definiremos el mismo elemento de H como en (47) lo hicimos, si elegimos

$$W_1 = 1, W_2 = W_1 a_{v_1}^{\epsilon_1}, W_3 = W_2 a_{v_2}^{\epsilon_2}, \dots, W_r = W_{r-1} = a_{v_{r-1}}^{\epsilon_{r-1}}$$

Si elegimos

$$W_1 = 1, W_2 = W_1 a_{v_1}^{\epsilon_1}, W_3 = W_2 a_{v_2}^{\epsilon_2}, \dots, W_r = W_{r-1} = a_{v_{r-1}}^{\epsilon_{r-1}}$$

(W_j es llamado el $j-1$-esimo segmento inicial de U); si para W_j así se eligen, entonce (48) es libremente igual a

$$\overline{W}_1 U \overline{W_r a_{v_r}^{\epsilon_r}}^{-1} = \overline{1} U \overline{U}^{-1} = 1U1^{-1} = U$$

($\overline{U} = 1$, dado que U es un elemento de H).

Mas aún, usando 4, es claro que

$$\overline{W}_j a_{v_j} \overline{W_j a_{v_j}}^{-1} \tag{49}$$

es una de las palabras en (45), y

$$\overline{W}_j a_{v_j}^{-1} \overline{W_j a_{v_j}^{-1}}^{-1} \tag{50}$$

la cual es una de las palabras en (45).

De aquí, toda palabra $U(a_v)$ la cual define un elemento de H es un producto (48) de palabras en (45) y sus inversos. Así las palabras en (45) generan H.

$\star$

Proposición 6.1 *Si G es finitamente generado y H es un subgrupo de índice finito, entonces H es finitamente generado.*

Demostración

Además, si G tiene n generadores y H tiene índice j, entonces los generadores (45) para H son nj en número (despues, debemos obtener un mejor límite para el número de generadores necesarios para H). De aquí, H es finitamente generado.

$\star$

Proposición 6.2 *Sea $W \to \overline{W}$ sera una función representante clase derecha para G mod H. Introduce el símbolo generado.*

$$s_{K,a_v}$$

para los elementos de H definidos por la palabra

$$K a_v \overline{K a_v}^{-1}$$

donde K es una clase representante derecha arbitraria y a_v es un generador en (29).

Definamos la función τ de palabras en U en (47)*, la cual define un elemento de H, por*

$$\tau(U) = s^{\epsilon_1}_{K_1,a_{v_1}} s^{\epsilon_2}_{K_2,a_{v_2}} \dots s^{\epsilon_r}_{K_r,a_{v_r}} \tag{51}$$

donde K_j es el representante del segmento inicial de U precediendo a_{v_j} si $\epsilon_j = 1$ y K_j es el representante del segmento inicial de U e incluye a $a^{-1}_{v_j}$ si $\epsilon_j = -1$. Entonces τ es un proceso de reescritura para H.

Demostración

Para mostrar que τ es un proceso de reescritura, debemos mostrar que si $s^{\epsilon_j}_{K_j,a_{v_j}}$ es reemplazado por $K_j a_{v_j} \overline{K_j a_{v_j}}^{-1}$ en (51) entonces una palabra en a_v resulta que define el mismo elemento de H como $U(a_v)$.

Si W_j es el segmento inicial de U el cual precede a $a^{\epsilon_j}_{v_j}$, entonces por construccion de K_j,

$$K_j = \overline{W_j}, \qquad \text{si } \epsilon_j = 1$$

y

$$K_j = \overline{W_j a^{-1}_{v_j}}, \qquad \text{si } \epsilon_j = -1$$

De aquí, en algún momento, $s^{\epsilon_j}_{K_j,a_{v_j}}$ es reemplazado por

$$\overline{W_j} a^{\epsilon_j}_{v_j} \overline{W_j a^{\epsilon_j}_{v_j}}^{-1}$$

Pero entonces (51) se convierte en (48), y así definimos el mismo elemento como $U(a_v)$.

Así τ es un proceso de reescritura.

⋆

Un proceso de reescritura τ se obtiene de una función representante clase derecha, como en la última proposición, es llamado un **proceso de reescritura de Reidemeister**.

Para ilustrar el metodo de reescritura en un proceso de Reidemeister, supongamos $a_1^2a_2^{-1}a_3$ define un elemento de H. Entonces

$$\tau(a_1a_1a_2^{-1}a_3) = s_{\overline{1}a_1}s_{\overline{a_1}a_1}s^{-1}_{\overline{a_1^2a_2^{-1}a_2}}s_{\overline{a_2^2a_2^{-1}a_3}}$$

Notese que los calculos de $\tau(U)$ puede sacarse por el reemplazo de un símbolo a_v^ϵ de U por el s-símbolo apropiado s^ϵ_{K,a_v}.

Usando el proceso de reescritura de Reidemeister τ en el teorema (6.1) simplifica grandemente la representación para H: las relaciones definidas (34) y (35) puede ser eleminado, y (36) puede ser restringido.

Teorema 6.3 *(Reidemeister). Sea τ el proceso de reescritura de Reidemeister dado por* (51) *para un subgrupo H de un grupo G. Si G tiene representación* (29)*, entonces H tiene la siguiente representación*

$$\langle s_{K,a_v}, \ldots; s_{K,a_v} = \tau(Ka_v\overline{Ka_v}^{-1}), \ldots, \tau(KR_\mu K^{-1}), \ldots\rangle \tag{52}$$

bajo la función $s_{K,a_v} \to Ka_v\overline{Ka_v}^{-1}$, donde K es un representante arbitrario (usado en la función clase derecha determinada por τ), a_v es un generador arbitrario y R_μ es una relación definido arbitrariamente en (29).

Demostración

Es suficiente para demostrar las relaciones (34), (35) y (36) puede ser derivada de las relaciones definidas en (52); entonces usando una transformación Tietze podemos borrar las relaciones redundantes definidas.

Para obtener (34), (35) y (36) es conveniente tener las siguientes propiedades de un proceso de reescritura de Reidemeister:

5. Si U y U^* son palabras libremente iguales (en el a_v) el cual define elementos de H entonces $\tau(U)$ y $\tau(U^*)$ son palabras libremente iguales (en el s-símbolo)

6. Si U_1 y U_2 definen elementos de H entonces $\tau(U_1U_2)$ y $\tau(U_1)\tau(U_2)$ son palabras idénticas (en los s-símbolos).

Claramente, para mostrar 5, es suficiente verificar que $\tau(Va_v^\epsilon a_v^{-\epsilon}W)$ es libremente igual a $\tau(VW)$, donde $\epsilon = \pm 1$. Ahora, calculando τ de una palabra podemos hacerlo reemplazando cada a-símbolo por el apropiado s-símbolo dependiendo solo de los a-símbolos y el segmento representante precediendo el a-símbolo, el s-símbolo reemplaza los a-símbolo de V y W calculando $\tau(VW)$ y $\tau(Va_v^\epsilon a_v^{-\epsilon}W)$, serán el mismo. De aquí, necesitamos considerar solo los s-símbolos los cuales reeplazan a_v^ϵ y $a_v^{-\epsilon}$. Estos son

$$s_{\bar{V},a_v} \qquad \text{y} \qquad s^{-1}_{\overline{V_{a_v a_v^{-1}}},a_v} = s^{-1}_{\overline{V},a_v}$$

Si $\epsilon = 1$, y

$$s^{-1}_{\overline{V_{a_v^{-1}},a_v}} \qquad \text{y} \qquad s_{\overline{V_{a_v^{-1}},a_v}}$$

Si $\epsilon = -1$. Esto prueba 5.

Para demostrar 6, notese que los s-símbolos reemplazan los a-símbolos de U_1 calculando $\tau(U_1U_2)$, son precisamente los s-símbolos de $\tau(U_1)$. Mas aún, dado que U_1 esta en H, $\overline{U_1W} = \overline{W}$ para algúna palabra $W(a_v)$. De aquí, los s-símbolos reemplazan a los a-símbolos de U_2 calculando $\tau(U_1U_2)$ son precisamente los s-símbolos de $\tau(U_2)$.

Es claro de las propiedades 5 y 6 que las relaciones (34) y (35) pueden ser obtenidas de las relaciones triviales.

Para simplificar las relaciones en (36), notese que alguna palabra W es libremente igual a la palabra UK, donde K esta en $\overline{W}$ y U esta en WK^{-1} el cual define un elemento de H. Así

$$\begin{aligned}
\tau(WR_\mu W^{-1}) &\approx \tau(UKR_\mu K^{-1}U^{-1}) && (53)\\
&= \tau(U)\tau(KR_\mu K^{-1})\tau(U^{-1}) && (54)\\
& && (55)
\end{aligned}$$

Dado que (34) y (35) se mantienen, $\tau(U^{-1}) = \tau(U)^{-1}$ se mantiene, y así la relación $\tau(WR_\mu W^{-1})$ es derivable de la relación

$$\tau(U)\tau(KR_\mu K^{-1})\tau(U^{-1})$$

y de aquí, de la relación

$$\tau(KR_\mu K^{-1})$$

Así (52) presenta H.

⋆

Proposición 6.3 *Si G es finitamente presentado y H es de índice finito en G, entonces H es finitamente presentado.*

Demostración

Esta es una consecuencia inmediata del teorema (6.3).

⋆

Para simplificar la presentación (52) aún mas, debemos restringir nosotros mismos a una clase especial de funciones de clase derecha.

Una función clase derecha Schreier es una para la cual algún segmento inicial de un representante es otra vez un representante. El sistema de representantes es llamado un **sistema de Schreier**. Un proceso de reescritura Reidemeister usando un sistema de Schreier es llamado un **proceso de reescritura de Reidemeister-Schreier**.

Como una ilustración de un sistema de Schreier, sea G el grupo libre sobre a y b, y sea H el subgrupo normal de G generado por a^2, b^2 , y $aba^{-1}b^{-1}$. Entonces G/H tiene cuatro clases. El sistema representante 1,a, b, ab es Schreier, como lo es el sistema representante $1, a, b, ab^{-1}$. El sistema representante $1, a, b, ab^{-1}$ no es Schreier; para, el segmento inicial a^{-1} de $a^{-1}b^{-1}$ no es representante.

Lema 6.1 *Sea G que tiene representación* (29) *y sea H un subgrupo de G. Entonces existe algún sistema Schreier de representantes para G mod H.*

Demostración

Llamaremos **longitud de una clase de** G mod H al tamaño de la palabra más corta en ella, y definiremos nuesto representante Schreier inductivamente, usando la longitud de una clase.

Eligiendo la palabra vacía como la representante de H, la clase de longitud cero. Si S_1 es una clase de tamaño 1, elegimos algúna palabra de longitud 1 en S_1 como su representante. Si S_2 tiene longitud 2, seleccionamos una palabra b_1b_2 de longitud 2 en S_2 (b_1 y b_2 son generadores en (29) o sus inversos). Ahora $\overline{b_1}b_2$ esta en S_2 por 4, y dado que $\overline{b_1}$ tiene tamaño a lo sumo 1, $\overline{b_1}b_2$ debe tener longitud 2. Elegimos $\overline{b_1}b_2$ como el representante de S_2. En general, asumiendo que tenemos que elegir representantes para todas las clases de longitud menor que r, si S_r es una clase de longitud r y $b_1 \dots b_{r-1}b_r$ es una palabra en S_r, elegimos $\overline{b_1 \dots b_{r-1}b_r}$ (la cual tiene longitud r) como la representante de S_r. Claramente, por construcción, si el último símbolo es borrado de la representante, otro representante es obtenido. De aquí, algún segmento inicial de un representante es un representante, y tenemos construido un sistema Schreier para G mod H.

$\star$

Nótese que en la prueba de el lema construimos un sistema Schreier minimal, un sistema Schreier en el cual cada representante tiene longitud no excedente al tamaño de alguna palabra que los represente. No todo sistema Schreier es minimal.

Usando un proceso de reescritura Reidemeister-Schreier las relaciones (33) es una presentación para H puede ser grandemente simplificado.

Teorema 6.4 *(Schreier). Sea G representado como en* (29) *y sea H un subgrupo de G. Si τ es un proceso de reescritura Reidemeister-Schreier, entonces H puede ser presentado como*

$$\langle s_{K,a_v}, \dots ; s_{M,a_\lambda}, \dots, \tau(KR_\mu K^{-1}), \dots \rangle \tag{56}$$

donde K es un representativo Schreier arbitrario, a_v es un generador arbitrario y R_μ es una relación definida arbitrariamente en (29)*, y M es un representante Schreier y a_λ un generador tal que*

$$Ma_\lambda \approx \overline{Ma_\lambda} \tag{57}$$

Demostración

Si $Ma_\lambda \approx \overline{Ma_\lambda}$ entonces $Ma_\lambda\overline{Ma_\lambda}^{-1} \approx 1$. De aquí, por 5, $\tau(Ma_\lambda\overline{Ma_\lambda}^{-1}) \approx \tau(1) = 1$. Así la relación

$$s_{M,a_\lambda} = \tau(Ma_\lambda\overline{Ma_\lambda}^{-1})$$

es derivable de la relación

$$s_{M,a_\lambda} \tag{58}$$

y opuestamente.

Mas aún, usando la propiedad Schreier de los sistemas representativos, debemos mostrar que

$$\tau(Ka_v\overline{Ka_v}^{-1})$$

puede ser reducido a s_{K,a_v} borrando los s-símbolos de tipo (58) para el cual (57) se mantiene. Para, algún s-símbolo reemplazando un a-símbolo de K calculando $\tau(Ka_v\overline{Ka_v}^{-1})$ tendrémos la forma

$$s_{N,a_p}$$

o

$$s^{-1}_{Na_p^{-1},a_p}$$

donde N es el segmento inicial de K precediendo el a-símbolo reemplazado. En el primer caso, Na_p es un segmento inicial de K, y así

$$\overline{Na_p} = Na_p$$

en el segundo caso, N es un segmento inicial de K, y así

$$\overline{Na_p^{-1}a_p} = \overline{N} = N \approx Na_p^{-1}a_p$$

Así, para algún s-símbolo s_{M,a_λ} enteramente de K, tenemos $\overline{Ma_\lambda} \approx Ma_\lambda$. Usando que $\tau(U^{-1})$ es la misma palabra en el s-símbolo como $\tau(U)^{-1}$, podemos mostrar que un s-símbolo s_{M,a_λ} reemplazando un a-símbolo de $\overline{Ka_v}^{-1}$ calculando $\tau(Ka_v)\overline{Ka_v}^{-1}$, satisfacera $\overline{Ma_\lambda} \approx Ma_\lambda$.

De aquí, ante la definición de relaciones (58), la relación en (33)

$$s_{K,a_v} = \tau(Ka_v\overline{Ka_v}^{-1})$$

es derivable de la relación

$$s_{K,a_v} = s_{K,a_v}$$

la cual puede ser claramente borrada.

⋆

Teorema 6.5 *(Nielsen-Schreier). Un subgrupo de un grupo libre es libre*

Demostración

Si G es un grupo libre, puede ser presentado con un conjunto vacío de relaciones definidas. De aquí, la definición de relaciones en (56) es justamente cierta de generadores de subgrupos. Usando una trasformación Tietze para borrar los generadores que aparecen como definición de relaciones, junto con la correspondiente definición de relaciones, resultando presentaciones que tienen un conjunto vacío de definición de relaciones. De aquí, el subgrupo es libre.

⋆

Conclusiones

La teoría utilizada durante todo el documento ha sido desglosada para que pueda ser utlizada como documento guía en una materia electiva, ya que los resultados son importantes, porque amplian las fronteras del Álgebra Moderna en la Escuela de Matemática en una rama que se ha quedado corta, esperando que con este documento se despierte el interés de estudiantes y docentes.

Además los resultados para grupos libres, tiene similitud con ciertas propiedades vistas para grupos y anillos, lo que facilita la visión de los nuevos resultados para esta teoría y amplía el área.

Bibliografía

- "Combinatorial Group Theory : Presentations of Groups in Terms of Generators and Relations", Magnus
  Wilhelm, Karrass Abraham, Solitar Donald, Dover Books on Advanced Mathematics,1976.
- "The Theory of Groups",A.G.; Hirsch, K.A. Kurosh, Chelsea Publishing Company,1960.
- "Graduate Texts in Mathematics", Hungerford, Thomas W. ,Springer Verlag, Secaucus, New Jersey, U.S.A.,1987.