Universidad Nacional Autónoma de México

Facultad de Ciencias

Extensiones de Grupos y Cohomología.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
OSCAR RODRÍGUEZ TRUJILLO

DIRECTOR DE TESIS:
DRA. MARÍA DEL CARMEN GÓMEZ LAVEAGA

2009

Rodríguez
Trujillo
Oscar
56 66 53 95
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemático
403067510

Dra.
María del Carmen
Gómez
Laveaga

Dr.
José
Ríos
Montes

Dr.
Hugo
Alberto
Rincón
Mejía

Dr.
Octavio
Mendoza
Hernández

M. en C.
José Cruz
García
Zagal

Extensiones de Grupos y Cohomología
64 p.
2009

Extensiones de Grupos y Cohomología

Oscar Rodríguez Trujillo

Índice general

Introducción

El álgebra homológica es una rama relativamente joven de las matemáticas. Alrededor del año 1926, Poincaré ya había inventado lo que ahora conocemos como grupo fundamental. En una serie de artículos estudiaba la configuración de puntos en espacios euclidianos de dimensión alta dados por igualdades y desigualdades polinomiales, es decir, estudiaba variedades algebraicas; en dicho estudio, investigó lo que ahora llamamos campos vectoriales así como generalizaciones de campos vectoriales en las variedades algebráicas. Esto lo llevó a observar lo que conocemos como la homología de dichas variedades, él se dio cuenta de la importancia de los llamados números de Betti para abordar los problemas relativos a los campos vectoriales de una variedad; dichos números, en esencia, determinan el número de hoyos que tiene una variedad. Durante 1926 y 1927 los matemáticos Alexandroff y Hopf se encontraban en Göttingen como invitados y se interesaron en el teorema del punto fijo de Lefschetz. Estaban convencidos de que dicho teorema estaba relacionado con algo que habían estado trabajando, una generalización de la característica de Euler-Poincaré; al igual que la característica de Euler, los números de Betti usados por Poincaré eran un invariante topológico. Una mención especial merece el hecho de que, en el mismo periodo, Emmy Noether se encontraba también en Göttingen por insistencia de Hilbert. La contribución de Noether al nacimiento del álgebra homológica es de gran importancia. Ella se dió cuenta de que aquello de lo que Alexandroff, Hopf y Lefschetz estaban hablando, no debía ser pensado en términos de números, sino en términos de grupos abelianos. Así, Noether reconoció los grupos de homología, además, que los números de Betti eran invariantes numéricos de clases de isomorfismos de grupos abelianos finitamente generados.

Vietoris y Čech fueron los primeros en definir los grupos de homología sin necesidad de recurrir a poliedros o complejos simpliciales. Con tan sólo la

noción de espacio topológico, Vietoris definió los grupos de homología de tal manera que se tiene el concepto de éstos para espacios arbitrarios. Čech lo hizo de manera independiente, ambos consideraban cubiertas de un espacio por conjuntos abiertos. En 1935 se llevó a cabo un encuentro internacional en Moscú, Hopf envió a su alumno Stiefel quién se encontraba estudiando la existencia de soluciones de ecuaciones diferenciales desde el punto de vista homológico, Stiefel había llegado a la idea de lo que ahora se conoce como clases de Stiefel-Whitney. Podemos situar el origen del álgebra homológica como disciplina matemática con el estudio de la teoría homológica de grupos. Dicha teoría surgió a partir de los trabajos del matemático Witold Hurewicz en 1935 acerca de los espacios esféricos, Hurewicz observó que los grupos de homología de un espacio esférico conexo por trayectorias están completamente determinados por su grupo fundamental. La teoría de cohomología se desarrolló durante la década de 1930; fue la cohomología de De Rham la que sentaría las bases definitivas de dicha teoría. Los grupos de cohomología de dimensión baja ya habían sido estudiados antes de que la noción de grupo de cohomología fuera formulada entre 1943 y 1945. La idea de conjunto factor para abordar el problema de la extensión de grupos aparece en los trabajos de Hölder, Issai Schur, Schreier y Richard Brauer. En 1941 Hopf llegó a lo que se conoce como la fórmula de Hopf para $H_2(\pi)$, ésta resulta coincidir con la fórmula del multiplicador de Schur para un grupo finito finitamente presentado.

El propósito de este trabajo es dar una interpretación de los grupos de cohomología de dimensiones bajas, para ello trabajaremos con el anillo de grupo sobre los enteros cuya definición será precisada. Comenzamos abordando el problema de la extensión de grupos, éste consiste en clasificar dichas extensiones, en la resolución de tal problema nos encontraremos con el concepto de conjunto factor; a partir de los conjuntos factor construimos ciertos grupos que nos ayudarán a clasificar las extensiones de grupos, propiamente hablando, estos grupos se conocen como multiplicadores de Schur. Estos últimos serán los que nos proporcionen una interpretación de los grupos de cohomología de dimensiones bajas, con esto se dará una motivación más concreta para la definición general de grupos de cohomología. Finalizamos mostrando una aplicación de los grupos de cohomología a grupos cíclicos finitos.

Capítulo 1

Preliminares

En este capítulo presentamos la teoría necesaria para leer este trabajo. Hacemos un repaso de la teoría de módulos pues trabajaremos en ese contexto, seguimos con algunas nociones de categorías y funtores para poder definir los funtores de homología. A partir de los funtores de homología obtendremos nuevos funtores, explícitamente, definiremos los funtores derivados de un funtor dado. En particular, daremos los funtores derivados del funtor contravariante $\mathrm{Hom}_R(-, A)$, esto es, el funtor $Ext^n_R(-, A)$. Muchas de las pruebas de los teoremas y corolarios conocidos se omiten, a excepción de aquellos que se consideran importantes para el desarrollo de los demás capítulos.

1.1. Módulos

Podemos pensar a los módulos como la generalización de los conceptos de espacio vectorial y grupo abeliano.

Definición 1.1.1 *Sea R un anillo y sea M un grupo abeliano. M es llamado un R-módulo izquierdo si existe una función $\mu : R \times M \longrightarrow M$, llamada multiplicación por escalares, la cual se denota como $\mu(r, m) = rm$ y que cumple, para todo $r, r_1, r_2 \in R$ y todo $m, m_1, m_2 \in M$, las siguientes condiciones:*

1. $r(m_1 + m_2) = rm_1 + rm_2$,
2. $r_1(r_2m) = (r_1r_2)m$,
3. $(r_1 + r_2)m = r_1m + r_2m$,

4. $1_R m = m$.

Usualmente, un R-módulo izquierdo M se denota como ${}_R M$.

De manera análoga se da la definición de R-módulo derecho, estos se denotan como M_R. Por otro lado, si una acción de R sobre un grupo abeliano M satisface las cuatro propiedades anteriores, ésta define un homomorfismo de anillos $\rho : R \longrightarrow End(M)$, dado por $(\rho(r))(m) = rm$, es decir, la definición de R-módulo izquierdo es equivalente a dar un anillo R, un grupo abeliano M y un morfismo de anillos $\rho : R \longrightarrow End(M)$.

Ejemplos:

i) Todo anillo R puede ser considerado un módulo sobre sí mismo definiendo la multiplicación por escalares como el producto dado en R.

ii) Todo espacio vectorial V, sobre un campo k, es un k-módulo izquierdo.

iii) Todo grupo abeliano A puede ser considerado un $\mathbb{Z}$-módulo izquierdo definiendo la acción de $n \in \mathbb{Z}$ sobre los elementos de A como $na = a + a + \cdots + a$, n veces.

Definición 1.1.2 *Sean M y N dos R-módulos izquierdos. Un homomorfismo de R-módulos, también llamado R-morfismo, es una función* f:$M \longrightarrow N$ *que cumple:*

i) $f(m_1 + m_2) = f(m_1) + f(m_2)$,

ii) $f(rm) = rf(m)$.

para todo $m, m_1, m_2 \in M$ *y todo* $r \in R$. *El conjunto de todos los R-morfismos de M en N se denota como* $\mathrm{Hom}_R(M, N)$.

Un R-morfismo inyectivo se llama monomorfismo; y si f es sobreyectiva, se llama epimorfismo, así, un isomorfismo es un R-morfismo biyectivo. Recíprocamente, si f es un isomorfismo entonces es monomorfismo y epimorfismo. Si $f : M \longrightarrow N$ es un isomorfismo entonces tiene inversa, esto es, existe un R-morfismo $g : N \longrightarrow M$ tal que $gf = id_M$ y $fg = id_N$, inversamente, si f tiene inversa un R-morfismo g, entonces f es isomorfismo; si dicha inversa existe, es única y se denota como f^{-1}. Nótese que todo R-morfismo, $f : M \longrightarrow N$, es un morfismo de grupos del grupo abeliano M. Para un R-morfismo $f : M \longrightarrow N$, definimos el kernel de f como:

$$Ker(f) = \{m \in M \mid f(m) = 0\}$$

Un resultado elemental sobre morfismos de grupos nos dice que, f es monomorfismo si y sólo si $Ker(f) = \{0\}$. Es evidente que este mismo resultado aplica para R-morfismos. La imagen de M bajo f se denota como:

$$f(M) = Im(f)$$

Claramente $Ker(f)$ e $Im(f)$ son submódulos de M y N respectivamente. Ciertos tipos de R-morfismos reciben nombres particulares: por ejemplo, los R-morfismos $f : M \longrightarrow M$ son llamados endomorfismos, se denota al conjunto $\mathrm{Hom}_R(M, M) = End_R(M)$; a los isomorfismos $f : M \longrightarrow M$ se les llama automorfismos y denotamos al conjunto de automorfismos de un R-módulo izquierdo M como $Aut_R(M)$.

Si M' es un subgrupo de M y es tal que $rm' \in M'$ para todo r en R y todo m' en M', entonces M' es llamado un submódulo de M. Sea M' un submódulo de M, al grupo cociente M/M' se le puede dar una estructura de R-módulo definiendo $r(m + M') = rm + M'$; claramente tenemos un monomorfismo $M' \longrightarrow M$ y un epimorfismo $M \longrightarrow M/M'$. Si $f : M \longrightarrow N$ es inyectiva, podemos identificar a M con el submódulo $f(M)$ de N; de la misma forma, si $f : M \longrightarrow N$ es sobreyectiva, podemos identificar N con $M/Ker(f)$. De manera más general se tiene el siguiente resultado.

Teorema 1.1.3 *Sean M y N dos R-módulos izquierdos. Si $f : M \longrightarrow N$ es un R-morfismo, entonces $f(M) \cong M/Ker(f)$.* ■

En lo sucesivo, nos referiremos a los R-modulos izquierdos simplemente como R-módulos y a los R-morfismos como morfismos.

Definición 1.1.4 *Una sucesión finita o infinita de R-módulos:*

$$\cdots \longrightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \longrightarrow \cdots$$

se llama exacta en el nivel n si $Im(f_{n+1}) = Ker(f_n)$ y si es exacta en todo n entonces, se dice que la sucesión es exacta.

A una sucesión exacta del tipo:

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

se le llama sucesión exacta corta. Como consecuencia de tener una sucesión exacta, mencionamos:

i) Una sucesión $0 \longrightarrow A \xrightarrow{f} B$ es exacta si y sólo si f es un monomorfismo.

ii) Una sucesión $A \xrightarrow{f} B \longrightarrow 0$ es exacta si y sólo si f es un epimorfismo.

iii) Una sucesión $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ es exacta si y sólo si f es un isomorfismo.

Dados $f : A \longrightarrow B$, $g : B \longrightarrow D$, $p : A \longrightarrow C$ y $q : C \longrightarrow D$ morfismos de R-módulos, podemos ponerlos en un diagrama:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[q]{} & D \end{array}$$

Dicho diagrama se dice que es conmutativo si $gf = qp$; a veces se expresa esto diciendo que el diagrama conmuta. Entre los resultados que involucran diagramas de R-módulos será muy útil el siguiente.

Lema 1.1.5 *Supóngase que se tiene el siguiente diagrama conmutativo*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \xrightarrow{f} & A & \xrightarrow{g} & A'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\ 0 & \longrightarrow & B' & \xrightarrow{f'} & B & \xrightarrow{g'} & B'' & \longrightarrow & 0 \end{array}$$

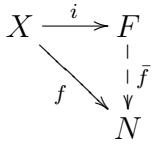
donde ambos renglones son exactos. Si cualesquiera dos de los morfismos α, α', α'' son isomorfismos, entonces el tercero también es un isomorfismo. ■

Un subconjunto X de ${}_RM$ es llamado base de ${}_RM$ si cada elemento m en ${}_RM$ puede ser expresado de manera *única* como $m{=}\sum_{x\in X} \alpha_x x$ con $\alpha_x \in R$ y $\alpha_x{=}0$ excepto para un número finito de ellos. Es fácil verificar que $X \subset M$ es una base si y sólo si: *i)* Todo elemento m de M puede ser expresado como combinación lineal finita de elementos de X, es decir, $m = \sum_{i=1}^{n} \alpha_i x$, $x \in X$, *ii)* Si se tiene $\sum_{i=1}^{n} \alpha_i x = 0$ entonces $\alpha_i{=}0$ para todo i. En general, dado un anillo arbitrario R, no podemos garantizar que todo R-módulo admita una base, aquellos que sí la admiten reciben un nombre especial.

Definición 1.1.6 *Un R-módulo M se llama libre sobre $X \subset M$ si X es una base de M.*

Usualmente, estos módulos son llamados simplemente módulos libres siempre que en el contexto esté claro qué subconjunto es la base; como ejemplo, podemos mencionar que R, considerado como módulo sobre sí mismo, es un módulo libre con base $\{1_R\}$. Los $\mathbb{Z}$-módulos libres son llamados grupos libres abelianos. A continuación se da una caracterización de los módulos libres en términos de la base y cualquier morfismo que sale de dicho módulo.

Teorema 1.1.7 *Sea F un R-módulo libre con base X. Para cualquier R-módulo N y para cualquier función $f : X \longrightarrow N$ existe un único morfismo $\bar{f} : F \longrightarrow N$ tal que $\bar{f}i = f$, donde $i : X \longrightarrow F$ es la inclusión, en un diagrama:*



es decir, $\bar{f}(x) = f(x)$ para todo $x \in X$. Se dice en este caso que $\bar{f}$ extiende a f por linealidad. ■

El resultado anterior, nos dice que el efecto de un morfismo sobre un módulo libre está completamente determinado por su efecto sobre la base. Los módulos libres nos permiten describir cualquier módulo como ilustra el siguiente resultado.

Teorema 1.1.8 *Todo R-módulo M es cociente de un R-módulo libre F.*

Demostración. Sea A_M el módulo libre con base el conjunto M. Por el Teorema 1.1.7, la identidad $1_M : M \longrightarrow M$ se extiende a un único morfismo $f : A_M \longrightarrow M$ que extiende a f, y es claro que f es epimorfismo pues 1_M es sobreyectiva. ■

Dicho resultado dice que M puede ser descrito en términos de ***generadores*** y ***relaciones***, esto es, si A es un módulo libre con base X y $f : A \longrightarrow M$ es un epimorfismo entonces X es llamado un conjunto de generadores y $Ker(f)$ es llamado el submódulo de relaciones.

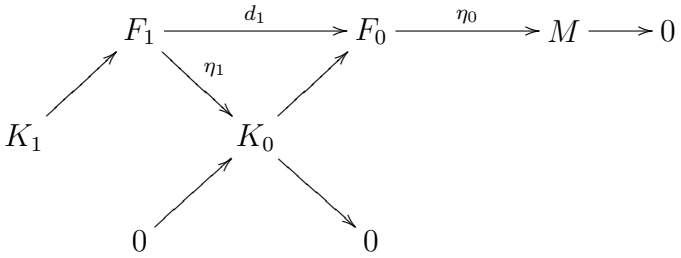
Definición 1.1.9 *Una resolución libre, de un R-módulo M, es una sucesión exacta*

$$\cdots \longrightarrow F_n \xrightarrow{d_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0$$

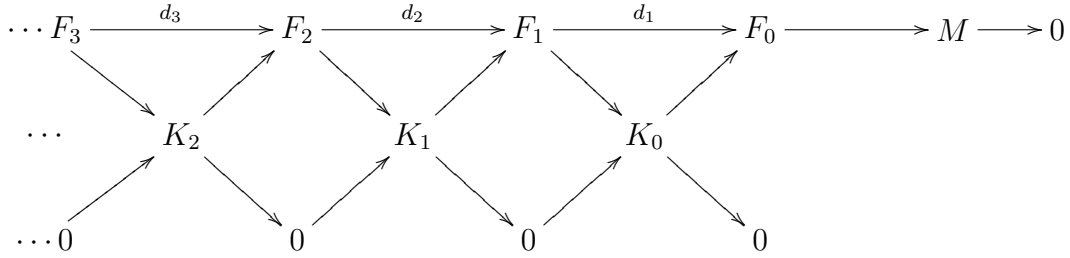
en la cual cada F_n es un R-módulo libre.

Teorema 1.1.10 *Todo R-módulo M tiene una resolución libre.*

Mostramos el proceso para construir dicha resolución. Por el Teorema 1.1.8 existe un módulo libre F_0 y un epimorfismo $\eta_0 : F_0 \longrightarrow M$ cuyo kernel denotamos por K_0. Por su parte, para K_0 existe un módulo libre F_1 y un epimorfismo $\eta_1 : F_1 \longrightarrow K_0$ con kernel K_1, esto nos da unas sucesiones exactas que ponemos en un diagrama como sigue:



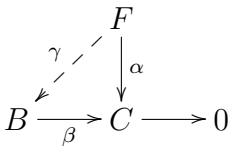
donde d_1 se define como la composición $F_1 \longrightarrow K_0 \longrightarrow F_0$. Este proceso puede repetirse inductivamente, lo cual nos dará una serie de sucesiones exactas que en un diagrama nos queda como:



donde los morfismos d_n son las composiciones $F_n \longrightarrow K_{n-1} \longrightarrow F_{n-1}$. Para cada n, $Ker(d_n) = K_n$ y $Im(d_n) = K_{n-1}$. Por lo tanto $Im(d_{n+1}) = Ker(d_n)$; y la sucesión que ésta construcción nos induce con los F_n a través de los morfismos d_n es exacta. ■

Una propiedad que cumplen los módules libres es la siguiente.

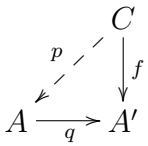
Teorema 1.1.11 *Considerese el siguiente diagrama de R-módulos*



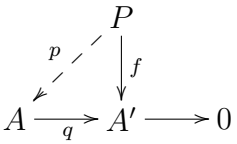
donde β es un epimorfismo. Si F es libre y $\alpha : F \longrightarrow C$ es cualquier morfismo entonces, existe $\gamma : F \longrightarrow B$ tal que el diagrama conmuta, es decir, $\beta\gamma = \alpha$.

■

Definición 1.1.12 *Decimos que un morfismo de R-módulos $f : C \longrightarrow A'$, se factoriza a través de un morfismo $q : A \longrightarrow A'$, si existe un morfismo $p : C \longrightarrow A$ tal que $qp = f$. En tal caso, tenemos el siguiente diagrama conmutativo*



Definición 1.1.13 *Un R-módulo P se dice que es proyectivo si, dado todo morfismo $f : P \longrightarrow A'$ se factoriza a través de cualquier epimorfismo $q : A \longrightarrow A'$, es decir, existe un morfismo $p : P \longrightarrow A$ tal que hace conmutar el siguiente diagrama:*



Al comparar la definición de módulos proyectivos con el Teorema 1.1.11, se sigue que todo módulo libre es proyectivo; sin embargo, el inverso no es verdadero. También, de acuerdo al Teorema 1.1.10, todo módulo tiene una resolución proyectiva.

1.2. Categorías y Funtores

La Teoría de Categorías es el lenguaje natural en el que se presenta el álgebra homológica. Presentamos los conceptos básicos que se requieren para las

siguientes secciones. De manera análoga al caso de la teoría de conjuntos, tenemos ciertos términos primitivos como "*clase*" y "*elemento*"; el término "*conjunto*" lo reservamos para aquellas clases suficientemente pequeñas para tener un cardinal.

Definición 1.2.1 *Una categoría* $\mathfrak{C}$ *consta de:*

1. *Una* ***clase*** *de objetos que denotamos como obj(*$\mathfrak{C}$*).*

2. *Para cada par de objetos* A *y* B *de* $\mathfrak{C}$ *un conjunto de* ***morfismos****,* $\mathrm{Hom}_{\mathfrak{C}}(A, B)$

3. *Dados* A*,* B *y* C *en obj(*$\mathfrak{C}$*), una* ***regla de composición***

$$\mathrm{Hom}_{\mathfrak{C}}(A, B) \times \mathrm{Hom}_{\mathfrak{C}}(B, C) \longrightarrow \mathrm{Hom}_{\mathfrak{C}}(A, C)$$

la cual se denota por $(f, g) \longmapsto gf$

Nota: Antes de continuar con la definición, introduciremos la notación que relacionará nuestra terminología y notación con ideas ya conocidas. Si f es un morfismo entre A y B, podemos considerarlo como una "función generalizada" de A en B y representarlo como $f : A \longrightarrow B$, de ésta manera, el conjunto $\mathrm{Hom}_{\mathfrak{C}}(A, B) \times \mathrm{Hom}_{\mathfrak{C}}(B, C)$ consta de parejas (f, g), donde $f : A \longrightarrow B$ y $g : B \longrightarrow C$, llamamos a A el dominio de f y a B el codominio. Siguiendo las ideas anteriores se justifica el hecho de que denotemos la regla de composición como gf. Continuamos con la definición enunciando los axiomas que debe cumplir una categoría

i) Los conjuntos $\mathrm{Hom}_{\mathfrak{C}}(A_1, B_1)$ y $\mathrm{Hom}_{\mathfrak{C}}(A_2, B_2)$ son ajenos, a menos que $A_1 = A_2$ y $B_1 = B_2$.

ii) Dados $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathfrak{C}}(B, C)$ y $h \in \mathrm{Hom}_{\mathfrak{C}}(C, D)$ la composición es asociativa, es decir:

$$h(gf) = (hg)f.$$

iii) Para cada objeto A, existe un **morfismo identidad** $1_A : A \longrightarrow A$ tal que, para cualquier $f : A \longrightarrow B$ y $g : C \longrightarrow A$, $f1_A = f$ y $1_A g = g$.

Es necesario hacer algunas observaciones sobre estos axiomas, primero, la única condición sobre $\mathrm{Hom}_{\mathfrak{C}}(A, B)$ es que sea un conjunto pudiendo ser vacío; segundo, la unicidad del morfismo identidad se sigue del mismo axioma iii), así, hay una correspondencia uno a uno $A \longmapsto 1_A$ entre obj($\mathfrak{C}$) y la clase de morfismos identidad en $\mathfrak{C}$, por lo cual, podríamos describir una categoría únicamente en términos de morfismos y composiciones. Nótese también que la composición gf tiene sentido si el codominio de f coincide con el dominio de g.

Ejemplos:

i) **Conjuntos**. Los objetos son conjuntos, los morfismos son funciones y la composición es la usual.

ii) **Grupos**. Aquí los objetos son grupos y los morfismos son homomorfismos de grupos, la composición es la usual.

iii) Consideremos la categoría de homotopía, **Htp**, donde los objetos son los espacios topológicos y los morfismos son las clases de homotopía de funciones continuas. La composición se define como $[f][g] = [fg]$; usando el hecho de que si $f \simeq f'$ y $g \simeq g'$ entonces sus composiciones son homotópicas, $fg \simeq f'g'$. Esto nos da un ejemplo de una categoría donde los morfismos no son funciones pues un morfismo es cierta clase de equivalencia de funciones.

Nuestro interés se centra en el estudio de la categoría de los R-módulos izquierdos con R un anillo fijo, ésta se denota como ${}_R\mathbf{Mod}$, en dicha categoría los objetos son los R-módulos izquierdos, los morfismos son los homomorfismos de R-módulos y la composición es la usual. Denotamos al conjunto $\mathrm{Hom}(A, B)$ en ${}_R\mathbf{Mod}$ como $\mathrm{Hom}_R(A, B)$, nótese que si $R = \mathbb{Z}$, entonces ${}_{\mathbb{Z}}\mathbf{Mod}$ es la categoría de los grupos abelianos pues los grupos abelianos son $\mathbb{Z}$-módulos y los morfismos de grupos abelianos son $\mathbb{Z}$-morfismos. Evidentemente existe la definición de categoría de R-módulos derechos la cual es completamente análoga.

Decimos que un morfismo $f : A \longrightarrow B$ en $\mathfrak{C}$ es un isomorfismo si existe un morfismo $g : B \longrightarrow A$ en $\mathfrak{C}$ tal que $gf = id_A$ y $fg = id_B$. De ésto se sigue que el morfismo g está determinado de manera única, también es invertible y se denota como f^{-1} a la que se le llama la inversa de f; como consecuencia

de lo anterior tenemos que la composición de dos morfismos invertibles es invertible. Tal como usamos los morfismos dentro de una categoría para describir relaciones entre sus objetos, no es de extrañarse que deseemos poder describir relaciones entre categorías, para ello se cuenta con el concepto de funtor.

Definición 1.2.1 *Sea $\mathfrak{C}$ y $\mathfrak{D}$ dos categorías, un funtor $T : \mathfrak{C} \longrightarrow \mathfrak{D}$ es una correspondencia que cumple:*

1) Si $A \in$ obj($\mathfrak{C}$), $T(A) \in$ obj($\mathfrak{D}$).

2) Dado $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$ entonces, $T(f) \in \mathrm{Hom}_{\mathfrak{D}}(T(A), T(B))$.

3) Dado $A \xrightarrow{f} B \xrightarrow{g} C$ en $\mathfrak{C}$, entonces $T(A) \xrightarrow{T(f)} T(B) \xrightarrow{T(g)} T(C)$ está en $\mathfrak{D}$ y $T(gf) = T(g)T(f)$.

4) $T(1_A) = 1_{T(A)}$ para todo $A \in$ obj($\mathfrak{C}$).

Usualmente, se omiten los paréntesis al denotar la imagen de morfismos y objetos bajo un funtor. Así también, tenemos la definición de ***funtor contravariante***, en ésta, los incisos 2) y 3) de la definición anterior son reemplazados por los siguientes:

2) Si $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$, $Tf \in \mathrm{Hom}_{\mathfrak{D}}(TB, TA)$, gráficamente:

$$A \xrightarrow{f} B \quad \overset{T}{\curvearrowright} \quad TB \xrightarrow{Tf} TA$$

ésto justifica el uso del término contravariante, T invierte las flechas.

3) Si se tiene $A \xrightarrow{f} B \xrightarrow{g} C$ en $\mathfrak{C}$ entonces $TC \xrightarrow{Tg} TB \xrightarrow{Tf} TA$ en $\mathfrak{D}$ y $T(gf) = TfTg$

Para hacer la distinción entre los funtores contravariantes y los funtores que se definieron previamente, llamaremos funtores covariantes a los que preservan el sentido de las flechas.

Definición 1.2.2 *Una categoría $\mathfrak{C}$ se llama preaditiva si, para cada A y B en obj($\mathfrak{C}$), cada $\mathrm{Hom}_{\mathfrak{C}}(A, B)$ es un grupo abeliano aditivo y la composición $\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(A.C)$, $(g, f) \mapsto gf$ es $\mathbb{Z}$-bilineal.*

La categoría de R-módulos izquierdos es un ejemplo de categoría preaditiva (así como también la de módulos derechos). Si $\mathfrak{C}$ y $\mathfrak{D}$ son dos categorías preaditivas, decimos que un funtor $T : \mathfrak{C} \longrightarrow \mathfrak{D}$ es aditivo si $T(f+g) = T(f) + T(g)$ para cualquier par de morfismos de $\mathrm{Hom}_{\mathfrak{C}}(A, B)$.

Definición 1.2.3 *Sean $S, T : \mathfrak{C} \longrightarrow \mathfrak{D}$ dos funtores covariantes. Una transformación natural $\tau : S \longrightarrow T$ entre S y T es una familia de morfismos en $\mathfrak{D}$:*

$$\tau = \{\tau_A : S(A) \longrightarrow T(A)\}_{A \in obj(\mathfrak{C})}$$

que hacen conmutar el siguiente diagrama para todo $f : A \longrightarrow B$ en $\mathfrak{C}$:

$$\begin{array}{ccc} SA & \xrightarrow{\tau_A} & TA \\ {\scriptstyle Sf}\downarrow & & \downarrow{\scriptstyle Tf} \\ SB & \xrightarrow[\tau_B]{} & TB \end{array}$$

La definición de transformación natural para funtores contravariantes es análoga. Un **isomorfismo natural** (o equivalencia natural) es una transformación natural en la cual cada τ_A es un isomorfismo; en dicho caso, escribimos $S \cong T$. Si $\tau : S \longrightarrow T$ y $\sigma : T \longrightarrow U$ son dos transformaciones naturales, donde S, T y U son todos covariantes o contravariantes, podemos formar la composición $\sigma\tau : S \longrightarrow U$ definida, para cada A, como $(\sigma\tau)_A = \sigma_A\tau_A$ la cual, nuevamente, es una transformación natural.

1.3. Hom y ⊗

Regresemos la atención a la categoría ${}_R\mathbf{Mod}$. El conjunto $\mathrm{Hom}_R(A, B)$ es claramente un grupo abeliano al definir la suma de dos morfismos $f : A \longrightarrow B$ y $g : A \longrightarrow B$ como $(f+g)(a) = f(a) + g(a)$. Sin embargo, debe resaltarse el hecho de que $\mathrm{Hom}_R(A, B)$ no es, en general, un R-módulo. Dado $f : B_1 \longrightarrow B_2$ un morfismo de módulos y tomando en cuenta que la composición de dos morfismos de módulos es nuevamente morfismo, a un morfismo $g : A \longrightarrow B_1$ podemos asignarle el morfismo $fg : A \longrightarrow B_2$, lo que nos define un homomorfismo de grupos abelianos $f_* : \mathrm{Hom}_R(A, B_1) \longrightarrow \mathrm{Hom}_R(A, B_2)$, $f_*(g) = fg$. Más aún:

i) Si $f : B_1 \longrightarrow B_2$ y $f' : B_2 \longrightarrow B_3$ son R-morfismos, entonces:

$$(f'f)_* = f'_* f_* : \mathrm{Hom}_R(A, B_1) \longrightarrow \mathrm{Hom}_R(A, B_3).$$

ii) Si $id : B \longrightarrow B$ es la identidad, entonces

$$id_* : \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(A, B)$$

también es la identidad.

Lo anterior quiere decir que $\mathrm{Hom}_R(A, -)$ es un funtor (covariante) que asigna a cada módulo B un grupo abeliano $\mathrm{Hom}_R(A, B)$, y a cada morfismo de módulos $f : B_1 \longrightarrow B_2$ un morfismo de grupos abelianos:

$$f_* : \mathrm{Hom}_R(A, B_1) \longrightarrow \mathrm{Hom}_R(A, B_2).$$

Análogamente, es fácil verificar que $\mathrm{Hom}_R(-, B)$ es un funtor contravariante. Pasamos ahora a definir el producto tensorial, éste resulta ser un funtor que guarda una estrecha relación con el funtor Hom.

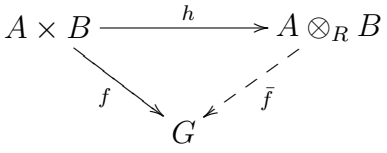
Definición 1.3.1 *Sea R un anillo asociativo con 1, A un R-módulo derecho, B un R-módulo izquierdo y G un grupo abeliano. Una función R-biaditiva (o R-balanceada) es una función $f : A \times B \longrightarrow G$ que cumple, para todo $a, a' \in A$, $b, b' \in B$ y todo $r \in R$, las siguientes condiciones:*

i) $f(a + a', b) = f(a, b) + f(a', b)$,

ii) $f(a, b + b') = f(a, b) + f(a, b')$,

iii) $f(ar, b) = f(a, rb)$.

Definición 1.3.2 *Sean A un R-módulo derecho y B un R-módulo izquierdo. El producto tensorial de A y B es un grupo abeliano, denotado como $A \otimes_R B$, y una función R-biaditiva $h : A \times B \longrightarrow A \otimes_R B$ con la siguiente propiedad universal. Para cualquier grupo abeliano G y cualquier función R-biaditiva $f : A \times B \longrightarrow G$, existe un único homomorfismo $\bar{f} : A \otimes_R B \longrightarrow G$ tal que hace conmutar el siguiente diagrama:*



Para poder hablar del producto tensorial, debemos mostrar que existe por lo que damos la idea de cómo se construye. Sea F un grupo libre abeliano con base $A \times B$, es decir, F es el grupo cuyos elementos son las combinaciones lineales con coeficientes en $\mathbb{Z}$ de parejas ordenadas (a, b). Defínase S como el subgrupo de F generado por la unión de los siguientes tres conjuntos:

i) $\{(a + a', b) - (a, b) - (a', b) \mid a, a' \in A \ y \ b \in B\}$,

ii) $\{(a, b + b') - (a, b) - (a, b') \mid a \in A \ y \ b, b' \in B\}$,

iii) $\{(ar, b) - (a, rb) \mid a \in A, b \in B \ y \ r \in R\}$.

Definimos $A \otimes_R B = F/S$. Si denotamos a la clase $(a, b) + S$ como $a \otimes b$ es fácil ver que $h : A \times B \longrightarrow A \otimes_R B$ definido por $(a, b) \mapsto a \otimes b$ es R-biaditiva y satisface la propiedad universal de la definición de producto tensorial. Es importante mencionar que, en general, un elemento de $A \otimes_R B$ es de la forma $\sum a_i \otimes b_i$ y puede que no tenga una expresion de la forma $a \otimes b$. Más aún, la expresión $\sum a_i \otimes b_i$ no es única.

Teorema 1.3.3 *Cualesquiera dos productos tensoriales de A y B son isomorfos.* ■

Teorema 1.3.4 *Sea $f : A \longrightarrow A'$ un morfismo de R-módulos derechos y $g : B \longrightarrow B'$ un morfismo de R-módulos izquierdos. Existe un único morfismo $f \otimes g : A \otimes_R B \longrightarrow A' \otimes_R B'$ tal que $(f \otimes g)(a \otimes b) = f(a) \otimes f(b)$.* ■

Teorema 1.3.5 *Sean $A \xrightarrow{f} A' \xrightarrow{f'} A''$ morfismos de R-módulos derechos y $B \xrightarrow{g} B' \xrightarrow{g'} B''$ morfismos de R-módulos izquierdos. Se tiene la composición $(g' \otimes f') \circ (g \otimes f) = g'g \otimes f'f$.* ■

Con ésto es fácil ver que el producto tensorial es un funtor.

Corolario 1.3.6 *Sea A un R-módulo derecho. Entonces, la correspondencia $A \otimes - :_R \mathbf{Mod} \longrightarrow \mathbf{Ab}$ que a cada $B \in {}_R\mathbf{Mod}$ le asigna $A \otimes_R B$ y a cada $f \in \mathrm{Hom}_R(B, B')$ le asigna $A \otimes (f) = 1_A \otimes_R f : A \otimes_R B \longrightarrow A \otimes_R B'$, es un funtor aditivo.*

Demostración. Denotemos a $A \otimes -$ por $\mathbf{F}$. Tenemos que $\mathbf{F}$ manda la identidad en la identidad pues $\mathbf{F}(1_B) = 1_A \otimes 1_B$ es la identidad en $A \otimes_R B$ ya que deja fijo a los generadores. Si $g : B \longrightarrow B'$ y $g' : B' \longrightarrow B''$son morfismos entre R-módulos izquierdos, por el Teorema 1.3.5 se tiene que:

$$\mathbf{F}(g'g) = 1_A \otimes g'g = (1_A \otimes g')(1_A \otimes g) = \mathbf{F}(g')\mathbf{F}(g)$$

por tanto $\mathbf{F}$ es un funtor. Para probar que $\mathbf{F}$ es aditivo nótese que si $g, h : B \longrightarrow B'$ entonces:

$$\mathbf{F}(g+h) = 1_A \otimes (g+h) = 1_A \otimes g + 1_A \otimes h = \mathbf{F}(g) + \mathbf{F}(h)$$

■

De manera análoga, si B un R-módulo izquierdo entonces se tiene un funtor aditivo $- \otimes B : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$. En general $A \otimes_R B$ es un grupo abeliano, pidiendo una condición extra sobre A o sobre B obtenemos que el producto tensorial es un R-módulo.

Definición 1.3.7 *Sean R y S anillos. Dado un grupo abeliano B decimos que es un $R-S$-bimódulo, denotado como ${}_RB_S$, si es tanto un R-módulo izquierdo como un S-módulo derecho y las acciones de R y S están relacionadas de la siguiente manera, para todo $r \in R$, $b \in B$ y $s \in S$ se tiene que*

$$r(bs) = (rb)s.$$

Como ejemplo de un bimódulo podemos mencionar que R es un $R-R$-bimódulo. También, si R es conmutativo, a todo R-módulo izquierdo puede dársele estructura de R-módulo derecho definiendo la acción de R sobre B por la derecha como $br = rb$, en dicho caso B es un $R-R$-bimódulo.

Teorema 1.3.8 *Si A es un R-módulo derecho y B es un $R-S$-bimódulo, entonces $A \otimes_R B$ es un S-módulo derecho, donde la acción de S está dada por:*

$$(a \otimes b)s = a \otimes (bs)$$

Análogamente, cuando tenemos ${}_SA_R$ y ${}_RB$, $A \otimes_R B$ es un S-módulo izquierdo y la acción de S por la izquierda es:

$$s(a \otimes b) = (sa) \otimes b$$

■

Lo anterior tiene un efecto sobre los funtores del Teorema 1.3.6.

Corolario 1.3.9 *Dado un bimódulo ${}_RB_S$, se tiene un funtor aditivo $-\otimes_R B : \mathbf{Mod}_R \longrightarrow \mathbf{Mod}_S$. Similarmente, dado un bimódulo ${}_RA_S$, se tiene un funtor aditivo $A \otimes_R - :\ {}_S\mathbf{Mod} \longrightarrow\ {}_R\mathbf{Mod}$.*

■

El siguiente corolario es consecuencia del Teorema 1.3.8.

Corolario 1.3.10 *Si R es conmutativo y A, B son R-módulos, entonces $A \otimes_R B$ es un R-módulo con $r(a \otimes b) = a \otimes (rb) = (ra) \otimes b$.*

■

Se tienen situaciones análogas para el funtor Hom.

Teorema 1.3.11 *Sean R y S anillos.*

i) Dados ${}_RA_S$ y ${}_RB$. $\mathrm{Hom}_R(A, B)$ es un S-módulo izquierdo, donde la acción de S está dada por $(sf)(a) = f(as)$. Se tiene un funtor aditivo $\mathrm{Hom}_R(A, -) :{}_R\mathbf{Mod} \longrightarrow{}_S\mathbf{Mod}$.

ii) Dados ${}_RA_S$ y B_S. $\mathrm{Hom}_S(A, B)$ es un R-módulo derecho, donde la acción de R está dada por $(fr)(a) = f(ra)$. Se tiene un funtor aditivo $\mathrm{Hom}(A, -)_S : \mathbf{Mod}_S \longrightarrow \mathbf{Mod}_R$.

iii) Dados ${}_SB_R$ y A_R. $\mathrm{Hom}_R(A, B)$ es un S-módulo izquierdo, donde la acción de S está dada por $(sf)(a) = s(f(a))$. Se tiene un funtor aditivo $\mathrm{Hom}(-, B)_R : \mathbf{Mod}_R \longrightarrow{}_S\mathbf{Mod}$.

iv) Dados ${}_SB_R$ y ${}_SA$. $\mathrm{Hom}_S(A, B)$ es un R-módulo derecho, donde la acción de R está dada por $(fr)(a) = (f(a))r$. Se tiene un funtor aditivo $\mathrm{Hom}(A, -)_R :{}_S\mathbf{Mod} \longrightarrow \mathbf{Mod}_R$.

■

Teorema 1.3.12 *Sea R un anillo y B un R-módulo izquierdo. Entonces, el mapeo $f : R \otimes_R B \longrightarrow B$ dado por $f(r \otimes b) = rb$ está bien definido y es un isomorfismo de R-módulos.*

Demostración. Dado que R es un $R-R$-bimódulo entonces, $R \otimes_R B$ es un R-módulo izquierdo; por lo tanto, la función $f : R \times B \longrightarrow B$ dada por $f(r,b) = rb$ es una función R-biaditiva. De acuerdo a la definición de producto tensorial, existe $\varphi : R \otimes_R B \longrightarrow B$ tal que $\varphi(r \otimes b) = rb$. Para ver que φ es un isomorfismo nótese que su inversa está dada por $\theta : B \longrightarrow R \otimes_R B$ definida como $\theta(b) = 1_R \otimes b$. ■
Para A y $A \otimes_R R$ como R-módulos derechos se tiene que $A \otimes_R R \cong A$. Nos interesa saber cuál es el efecto que tienen, sobre las sucesiones exactas, los funtores que hemos descrito.

Definición 1.3.13 *Un funtor covariante aditivo* $\mathbf{F} : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ *se llama exacto izquierdo si para cualquier sucesión exacta corta*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \ ,$$

al aplicarle $\mathbf{F}$*, se tiene que*

$$0 \longrightarrow \mathbf{F}A \xrightarrow{\mathbf{F}\alpha} \mathbf{F}B \xrightarrow{\mathbf{F}\beta} \mathbf{F}C$$

es exacta. Similarmente, un funtor covariante aditivo $\mathbf{G} :_R \mathbf{Mod} \longrightarrow \mathbf{Ab}$ *es exacto derecho si para cualquier sucesión exacta corta*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \ ,$$

al aplicarle $\mathbf{G}$*, la sucesión obtenida*

$$\mathbf{G}A \xrightarrow{\mathbf{G}\alpha} \mathbf{G}B \xrightarrow{\mathbf{G}\beta} \mathbf{G}C \longrightarrow 0$$

es exacta.

Si $\mathbf{F}$ es exacto izquierdo entonces $\mathbf{F}\alpha : \mathbf{F}A \longrightarrow \mathbf{F}B$ es monomorfismo y $Im(\mathbf{F}\alpha) = Ker(\mathbf{F}\beta)$ por lo que $\mathbf{F}$ preserva monomorfismos. Análogamente, si $\mathbf{F}$ es exacto derecho entonces $\mathbf{F}$ preserva epimorfismos. Para funtores contravariantes, las definiciones de exacto izquierdo y derecho quedan como sigue.

Definición 1.3.14 *Un funtor contravariante aditivo* $\mathbf{F} : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$*, es exacto izquierdo si dada una sucesión exacta corta*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \ ,$$

al aplicarle $\boldsymbol{F}$*, la sucesión obtenida*

$$0 \longrightarrow \mathbf{F}C \xrightarrow{\mathbf{F}\beta} \mathbf{F}B \xrightarrow{\mathbf{F}\alpha} \mathbf{F}A\ ,$$

también es exacta. Un funtor contravariante aditivo $\mathbf{G} :_R \mathbf{Mod} \longrightarrow \mathbf{Ab}$*, es exacto derecho si dada una sucesión exacta corta*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C\ ,$$

al aplicarle G*, la sucesión que se obtiene*

$$\mathbf{G}C \xrightarrow{\mathbf{G}\beta} \mathbf{G}B \xrightarrow{\mathbf{G}\alpha} \mathbf{G}A \longrightarrow 0\ ,$$

resulta ser exacta.

Definición 1.3.15 *Un funtor* $\mathbf{F} :_R \mathbf{Mod} \longrightarrow \mathbf{Ab}$ *es exacto si es exacto derecho y exacto izquierdo.*

Estableceremos ahora las propiedades de exactitud de Hom y $\otimes$.

Teorema 1.3.16 *Para todo módulo* M*,* $\mathrm{Hom}(M, -)$ *es un funtor exacto izquierdo y* $\mathrm{Hom}(-, M)$ *es un funtor (contravariante) exacto izquierdo.*

Demostración. Probaremos que $F = \mathrm{Hom}(M, -)$ es exacto izquierdo. La demostración de que $\mathrm{Hom}(-, M)$ es exacto izquierdo es análoga. Consideremos la siguiente sucesión exacta corta:

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

queremos probar la exactitud de:

$$0 \longrightarrow \mathrm{Hom}(M, A) \xrightarrow{F\alpha} \mathrm{Hom}(M, B) \xrightarrow{F\beta} \mathrm{Hom}(M, C)$$

Debemos probar que F preserva monomorfismos y que $Im(F\alpha) = Ker(F\beta$. Observemos que si $F\alpha(f) = 0$ entonces $\alpha f(a) = 0$ para todo $a \in A$. Puesto que α es monomorfismo lo anterior implica que $f(a) = 0$ para todo $a \in A$, por tanto, f es el morfismo cero. Falta probar que $Im(F\alpha) = Ker(F\beta$. Si $g \in Im(F\alpha)$ entonces $g = \alpha f$ para algún $f \in \mathrm{Hom}(M, A)$, de esto se sigue que $F\beta(g) = \beta g = \beta\alpha f = 0$ pues $\beta\alpha = 0$, así, $g \in Ker(F\beta)$ por lo que $Im(F\alpha) \subset Ker(F\beta)$. Ahora, si $g \in \mathrm{Hom}(M, B)$ pertenece al núcleo de $F\beta$ entonces $F\beta(g) = \beta g = 0$. Queremos probar que $g = \alpha f$ para algún $f \in \mathrm{Hom}(M, A)$. Para todo $m \in M$, $\beta(g(m)) = 0$ por lo que $g(m) \in Ker(\beta) = Im(\alpha)$; existe un único $a \in A$ tal que $\alpha(a) = g(m)$ pues α es monomorfismo. Tomando $f : M \longrightarrow A$ definido por $f(m) = a = \alpha^{-1}g(m)$ se tiene que $\alpha f = g$, por lo tanto $Ker(F\beta) \subset Im(F\alpha)$. ■

Teorema 1.3.17 *Los funtores $M \otimes_R -$ y $- \otimes_R N$ son exactos derechos.*

Demostración. Consideremos la siguiente sucesión exacta de R-módulos.

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

Debemos probar la exactitud de la sucesión inducida:

$$M \otimes_R A \xrightarrow{1\otimes\alpha} M \otimes_R B \xrightarrow{1\otimes\beta} M \otimes_R C \longrightarrow 0$$

Primero veamos que $1 \otimes \beta$ es un epimorfismo. Dado que β es un epimorfismo, tomando $\sum m_i \otimes c_i \in M \otimes C$, existe $b_i \in B$ tal que $\beta(b_i) = c_i$ para todo i, con esto tenemos que:

$$1 \otimes \beta(\sum m_i \otimes b_i) = \sum m_i \otimes \beta b_i = \sum m_i \otimes c_i$$

Sólo resta demostrar que $Ker((1 \otimes \beta)) = Im(1 \otimes \alpha)$. Para probar la inclusión $Im(1 \otimes \alpha) \subset Ker((1 \otimes \beta))$ es suficiente observar que $(1 \otimes \beta) \circ (1 \otimes \alpha) = 1 \otimes (\beta\alpha) = 1 \otimes 0 = 0$. Por último, denotemos $E = Im(1 \otimes \alpha)$, como ya vimos que $E \subset Ker((1 \otimes \beta))$, el morfismo $1 \otimes \beta$ induce un morfismo

$$\begin{gathered}\hat{\beta} : (M \otimes_R B)/E \longrightarrow M \otimes C \\ m \otimes b + E \mapsto m \otimes \beta b\end{gathered}$$

con $m \in M$ y $b \in B$. Tomando la proyección $\pi : M \otimes B \longrightarrow (M \otimes B)/E$, es fácil ver que $\hat{\beta}\pi = 1 \otimes \beta$, más aún, $\hat{\beta}$ es un isomorfismo. En efecto, la función $f : M \times C \longrightarrow (M \otimes C)/E$ dada por $f(m, c) = m \otimes b + E$, donde $c = \beta(b)$, está bien definida (b existe porque β es epimorfismo) pues, si $\beta(b') = c$ entonces $\beta(b - b') = 0$ y $b - b' \in Ker(\beta) = Im(\alpha)$ por lo que existe $a \in A$ tal que $\alpha(a) = b - b'$. Por lo tanto, $a \otimes (b - b') = a \otimes \alpha(a) \in Im(1 \otimes \alpha) = E$. Claramente f es R-biaditiva y, por la definición de producto tensorial, induce un único morfismo $\hat{f} : M \otimes C \longrightarrow (M \otimes B)/E$ con $\hat{f}(m \otimes c) = m \otimes b + E$. Claramente $\hat{f}$ es inversa de $\hat{\beta}$, con esto tenemos que:

$$Ker((1 \otimes \beta)) = Ker(\hat{\beta}\pi) = Ker(\pi) = E = Im(1 \otimes \alpha)$$

■

Por último, exhibimos la relación que guardan entre sí los funtores Hom y $\otimes$, éstos forman lo que se conoce como par adjunto de funtores.

Definición 1.3.18 *Sean* $\mathbf{F} : \mathfrak{C} \longrightarrow \mathfrak{D}$ *y* $\mathbf{G} : \mathfrak{D} \longrightarrow \mathfrak{C}$ *dos funtores. Decimos que la pareja ordenada* $(\mathbf{F}, \mathbf{G})$ *es un par adjunto de funtores si, para cada* $C \in obj(\mathfrak{C})$ *y cada* $D \in obj(\mathfrak{D})$ *existe un isomorfismo natural*

$$\tau_{C,D} : \mathrm{Hom}_{\mathfrak{D}}(\mathbf{F}C, D) \longrightarrow \mathrm{Hom}_{\mathfrak{C}}(C, \mathbf{G}D).$$

Más explícitamente, para todo $f : C' \longrightarrow C$ en $\mathfrak{C}$ y para todo $h : D \longrightarrow D'$ en $\mathfrak{D}$, se tienen los siguientes diagramas conmutativos:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathfrak{D}}(\mathbf{F}C, D) & \xrightarrow{\tau_{C,D}} & \mathrm{Hom}_{\mathfrak{C}}(C, \mathbf{G}D) \\ \downarrow{\scriptstyle (\mathbf{F}f)^*} & & \downarrow{\scriptstyle f^*} \\ \mathrm{Hom}_{\mathfrak{D}}(\mathbf{F}C', D) & \xrightarrow{\tau_{C',D}} & \mathrm{Hom}_{\mathfrak{C}}(C', \mathbf{G}D), \end{array}$$

$$\begin{array}{ccc} \mathrm{Hom}_{\mathfrak{D}}(\mathbf{F}C, D) & \xrightarrow{\tau_{C,D}} & \mathrm{Hom}_{\mathfrak{C}}(C, \mathbf{G}D) \\ \downarrow{\scriptstyle h_*} & & \downarrow{\scriptstyle (\mathbf{G}h)_*} \\ \mathrm{Hom}_{\mathfrak{D}}(\mathbf{F}C, D') & \xrightarrow{\tau_{C,D'}} & \mathrm{Hom}_{\mathfrak{C}}(C, \mathbf{G}D'). \end{array}$$

El Teorema 1.3.8 dice que si se tiene A_R y ${}_RB_S$ entonces $A \otimes_R B$ es un S-módulo derecho. El Teorema 1.3.11, inciso *ii*), dice que si tenemos C_S y ${}_RB_S$ entonces $\mathrm{Hom}_S(B, C)$ es un R-módulo derecho por lo cual tiene sentido tomar $\mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$.

Teorema 1.3.19 *Sean* R *y* S *anillos. Considérense* A_R, ${}_RB_S$ *y* C_S. *Tenemos el siguiente isomorfismo natural:*

$$\tau_{\mathbf{A},\mathbf{B},\mathbf{C}} : \mathrm{Hom}_S(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

Explícitamente, para cada $f : A \otimes_R B \longrightarrow C$, $a \in A$ *y* $b \in B$:

$$\tau_{\mathbf{A},\mathbf{B},\mathbf{C}}(f) = \tau_a(f)$$

donde $\tau_a(f)(b) = f(a \otimes b)$.
Si se tienen ${}_RA$, ${}_SB_R$ *y* ${}_SC$, *existe un isomorfismo natural:*

$$\tau : \mathrm{Hom}_S(B \otimes_R A, C) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)).$$

■

Más aún, fijando cualesquiera dos de entre A, B y C, se tienen los siguientes isomorfismos naturales. Fijando B y C:

$$\mathrm{Hom}_S(- \otimes_R B, C) \cong \mathrm{Hom}_R(-, \mathrm{Hom}_S(B, C)).$$

Fijando A y C:

$$\mathrm{Hom}_S(A \otimes_R -, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(-, C)).$$

Fijando A y B:

$$\mathrm{Hom}_S(A \otimes_R B, -) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, -)).$$

Por ejemplo, fijando B y C, si $f \in \mathrm{Hom_R}(A, A')$, tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathrm{Hom}_S(A' \otimes_R B, C) & \xrightarrow{\tau_{A',B,C}} & \mathrm{Hom}_R(A', \mathrm{Hom}_S(B, C)) \\ \downarrow{\scriptstyle (f \otimes 1_B)^*} & & \downarrow{\scriptstyle f^*} \\ \mathrm{Hom}_S(A \otimes_R B, C) & \xrightarrow{\tau_{A,B,C}} & \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)). \end{array}$$

1.4. Funtores de Homología

En esta sección todos los funtores considerados son aditivos.

Definición 1.4.1 *Un complejo de cadena (o simplemente complejo)* $\mathbf{A}$ *es una sucesión de módulos y morfismos:*

$$\mathbf{A} : \cdots \longrightarrow A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \longrightarrow \cdots$$

con $n \in \mathbb{Z}$*, donde los morfismos cumplen* $d_n d_{n+1} = 0$ *para todo* n*. Nótese que la condición* $d_n d_{n+1} = 0$ *es equivalente a pedir que* $Im(d_{n+1}) \subset Ker(d_n)$*. Siempre que sea necesario exhibir explícitamente los morfismos de un complejo, escribiremos* $(\mathbf{A}, \mathbf{d})$ *donde* $\mathbf{d} = \{d_n : n \in \mathbb{Z}\}$*.*

Toda sucesión exacta es un complejo, la condición de exactitud nos dice que $Im(d_{n+1}) = Ker(d_n)$ que en particular dice que $Im(d_{n+1}) \subset Ker(d_n)$ para todo n. Si $\mathbf{A}$ es un complejo y F es un funtor entonces:

$$\mathbf{F}(\mathbf{A}) : \cdots \longrightarrow F(A_{n+1}) \xrightarrow{Fd_{n+1}} F(A_n) \xrightarrow{Fd_n} F(A_{n-1}) \longrightarrow \cdots$$

es un complejo. En el caso particular de las sucesiones exactas, $F(\mathbf{A})$ es un complejo que no necesariamente es exacto.

Definición 1.4.2 *Sean* $\boldsymbol{A}$ *y* $\boldsymbol{A'}$ *son dos complejos. Un morfismo de cadenas* $\mathbf{f} : \mathbf{A} \longrightarrow \mathbf{A}'$ *es una sucesión de morfismos* $f_n : A_n \longrightarrow A'_n$*, con* $n \in \mathbb{Z}$*, tales que hacen conmutar el siguiente diagrama.*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & A_{n+1} & \xrightarrow{d_{n+1}} & A_n & \xrightarrow{d_n} & A_{n-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \cdots & \longrightarrow & A'_{n+1} & \xrightarrow{d'_{n+1}} & A'_n & \xrightarrow{d'_n} & A'_{n-1} & \longrightarrow & \cdots \end{array}$$

Dos complejos $\boldsymbol{A}$ y $\boldsymbol{A'}$ son isomorfos si existe un morfismo de cadenas $\mathbf{f} : \mathbf{A} \longrightarrow \mathbf{A}'$ en el que cada f_n es un isomorfismo.

Definición 1.4.3 *Un complejo* $(\boldsymbol{A'},\boldsymbol{d'})$ *es un subcomplejo de* $(\boldsymbol{A},\boldsymbol{d})$ *si cada* A'_n *es un submódulo de* A_n *y* $d'_n = d_n \mid_{A'_n}$ *para todo* n*. En dicho caso, tenemos un complejo cociente:*

$$\mathbf{A}/\mathbf{A}' : \cdots \longrightarrow A_n/A'_n \xrightarrow{\bar{d_n}} A_{n-1}/A'_{n-1} \longrightarrow \cdots$$

donde $\bar{d_n}(a_n + A'_n) = d_n(a_n) + A'_{n-1}$*.*

Definición 1.4.4 *Defínase* ***Comp*** *como la clase de todos los complejos de cadena, ésta junto con los morfismos de cadena forman una categoría. Si* $\mathbf{A}$*,* $\mathbf{B}$ *y* $\mathbf{C}$ *son complejos y* $\mathbf{f} : \mathbf{A} \longrightarrow \mathbf{B}$*,* $\mathbf{g} : \mathbf{B} \longrightarrow \mathbf{C}$ *son morfismos de cadena, la composición* $\mathbf{g} \circ \mathbf{f} : \mathbf{A} \longrightarrow \mathbf{C}$ *está dada por la composición* $g_n \circ f_n : A_n \longrightarrow C_n$*, para todo* n*. Y no es difícil ver que* ***Comp*** *es una categoría preaditiva.*

Definición 1.4.5 *Sea* $(\mathbf{A}, \mathbf{d})$ *un complejo. Definimos su* n*-ésimo módulo de homología,* $H_n(\mathbf{A})$*, como:*

$$H_n(\mathbf{A}) = Ker(d_n)/Im(d_{n+1}).$$

El cociente tiene sentido pues, dado que $\mathbf{A}$ es un complejo, se tiene que $d_n d_{n+1} = 0$ lo cual implica que $Im(d_{n+1}) \subset Ker(d_n)$. Los elementos de $Ker(d_n)$ se llaman n-ciclos y los elementos de $Im(d_{n+1})$ se llaman n-fronteras. Usaremos la siguiente notación:

$$\begin{aligned} Ker(d_n) &= Z_n(\mathbf{A}) \\ Im(d_{n+1}) &= B_n(\mathbf{A}) \end{aligned}$$

con esto tenemos que $H_n(\mathbf{A}) = Z_n(\mathbf{A})/B_n(\mathbf{A})$.

Definición 1.4.6 *Sea* $\mathbf{f} : \mathbf{A} \longrightarrow \mathbf{A}'$ *es un morfismo de cadenas. Para cada* n *definimos:*

$$H_n(\mathbf{f}) : H_n(\mathbf{A}) \longrightarrow H_n(\mathbf{A}')$$
$$z_n + B_n(\mathbf{A}) \mapsto f_n(z_n) + B_n(\mathbf{A}')$$

$H_n(\mathbf{f})$ *se llama morfismo inducido por* $\mathbf{f}$*, se denota por* f_{*n} *aunque usualmente se omite el subíndice* n*.*

Un complejo $\mathbf{C}$ es una sucesión exacta sí y sólo sí $H_n(\mathbf{C}) = 0$ para toda n. Así, H_n mide qué tan lejos está un complejo de ser una sucesión exacta. Una sucesión exacta es llamada complejo acíclico.

Teorema 1.4.7 *Para cada* n*,* $H_n : \mathbf{Comp} \longrightarrow {}_R\mathbf{Mod}$ *es un funtor aditivo.*

■

Teorema 1.4.8 *Si* $(\mathbf{C}, \mathbf{d})$ *y* $(\mathbf{C}', \mathbf{d}')$ *son dos complejos isomorfos, entonces* $H_n(\mathbf{C}) \cong H_n(\mathbf{C}')$ *para todo* n*.* ■

Ahora introducimos un concepto que originalmente surge en la topología algebráica.

Definición 1.4.9 *Sean* $\mathbf{f}, \mathbf{g} : (\mathbf{A}, \mathbf{d}) \longrightarrow (\mathbf{A}', \mathbf{d}')$ *dos morfismos de cadenas. Decimos que* $\mathbf{f}$ *y* $\mathbf{g}$ *son homotópicas si, para todo* n*, existe una familia de morfismos* $s_n : A_n \longrightarrow A'_{n+1}$ *tales que* $f_n - g_n = d'_{n+1}s_n + s_{n-1}d_n$*. Los morfismos* s_n *forman una homotopía entre* f *y* g*. Denotamos la relación de homotopía entre* f *y* g *como* $f \simeq g$*.*

Definición 1.4.10 *Un morfismo de cadenas* $\mathbf{f} : (\mathbf{A}, \mathbf{d}) \longrightarrow (\mathbf{A}', \mathbf{d}')$ *es nulhomotópico si* f *es homotópico al morfismo cero, esto es, si para todo* n *existe una familia de morfismos* $s_n : A_n \longrightarrow A'_{n+1}$ *tales que* $f_n = f_n - 0 = d'_{n+1}s_n + s_{n-1}d_n$

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A_{n+1} & \xrightarrow{d_{n+1}} & A_n & \xrightarrow{d_n} & A_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & \swarrow{\scriptstyle s_n} & \downarrow{\scriptstyle f_n} & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & A'_{n+1} & \xrightarrow[d'_{n+1}]{} & A'_n & \xrightarrow[d'_n]{} & A'_{n-1} & \longrightarrow & \cdots
\end{array}$$

Teorema 1.4.11 *Si* $f, g : \mathbf{A} \longrightarrow \mathbf{A}'$ *son morfismos de cadena homotópicos entonces* $f_* = g_* : H_n(\mathbf{A}) \longrightarrow H_n(\mathbf{A}')$ *para todo* n*.*

■

Definición 1.4.12 *Un complejo* $(\mathbf{C},\mathbf{d})$ *se dice que tiene una homotopía de contracción si* 1_C *es nulhomotópica. En éste caso, decimos que el complejo* $\mathbf{C}$ *es contraible.*

Teorema 1.4.13 *Un complejo* $(\mathbf{C},\mathbf{d})$ *que tenga una homotopía de contracción es aciclico, es decir, es una sucesión exacta.*

Demostración. Dado que $(\mathbf{C},\mathbf{d})$ tiene una homotopía de contracción entonces $1_C \simeq 0$. Por el Teorema 1.4.11, $1_{*C} = 0_*$ por lo cual $H_n(\mathbf{C}) = 0$ para todo n, en otras palabras, $Ker(d_n) = Im(d_{n+1})$ para todo n; por lo que la sucesión es exacta. ■

1.5. Funtores derivados y $Ext_R^n(-,A)$

Dado un funtor T entre dos categorías de módulos, construimos una sucesión de nuevos funtores llamados funtores derivados.

Definición 1.5.1 *Sea* $\mathbf{C}$ *un complejo de la forma:*

$$\mathbf{C} : \cdots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow M \longrightarrow 0$$

Llamamos complejo trunco al complejo que se obtiene al quitar M *de la sucesión anterior:*

$$\mathbf{C}_M : \cdots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow 0\ ,$$

y se denota por $\mathbf{C}_M$.

Teorema 1.5.2 *(Teorema de Comparación). Considerese el diagrama*

$$\begin{array}{ccccccccc}
\cdots P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
\vdots & & \vdots & & \vdots & & \downarrow f & & \\
\cdots P_2' & \xrightarrow{d_2'} & P_1' & \xrightarrow{d_1'} & P_0' & \xrightarrow{\varepsilon} & M' & \longrightarrow & 0
\end{array}$$

donde cada C_n *en la sucesión superior es proyectivo y la fila inferior es exacta. Entonces existe un morfismo de cadenas* $\bar{f} : \mathbf{P}_M \longrightarrow \mathbf{P'}_{M'}$ *que hace conmutar el diagrama. Más aún, si* $\bar{f}' : \mathbf{P}_M \longrightarrow \mathbf{P'}_{M'}$ *es otro morfismo que hace conmutar el diagrama, entonces* $\bar{f} \simeq \bar{f}'$. ■

Al morfismo $\bar{f} : \mathbf{P}_M \longrightarrow \mathbf{P'}_{M'}$ del teorema anterior se le conoce como el levantamiento homotópico de $f : M \longrightarrow M'$. Ahora definimos los funtores derivados derechos R^nT de un funtor aditivo T contravariante. Escogemos T contravariante pues trabajaremos con el funtor $\mathrm{Hom}_R(-, A)$ el cual es contravariante. Para cada R-módulo A, damos una resolución proyectiva de A y consideramos $\mathbf{P}_A$ su complejo trunco; aplicamos T y tomamos su homología $H^n = Ker(Td_{n+1})/Im(Td_n)$, $H^n(T(\mathbf{P}_A))$, esto último tiene sentido pues dado que T es contravariante, de la sucesión:

$$\mathbf{P}_A : \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow 0$$

al aplicarle T obtenemos la sucesión:

$$\cdots \longleftarrow TP_2 \xleftarrow{Td_2} TP_1 \xleftarrow{Td_1} TP_0$$

en dicho caso a los morfismos Td_i se les denota como d_i^*.

Definición 1.5.3 *Para cada R-módulo A, definimos los funtores derivados derechos de T:*

$$R^nT = H^n(T(\mathbf{P}_A)) = Ker(Td_{n+1})/Im(Td_n).$$

Si $f : A \longrightarrow B$ es un morfismo de R-módulos, por el Teorema de Comparación, existe el levantamiento homotópico $\bar{f} : \mathbf{P}_A \longrightarrow \mathbf{P}_B$. Definimos:

$$R^nT(f) : R^nT(A) \longrightarrow R^nT(B)$$
$$R^nT(f) = H^n(T\bar{f})$$

es decir, si $z_n \in Ker(Td_{n+1})$, se tiene que:

$$[R^nT(f)](z_n + Im(Td_n)) = (T\bar{f})(z_n) + Im(Td'_{n+1})$$

Teorema 1.5.4 *Dado un funtor contravariante T, R^nT es un funtor aditivo para todo n.* ■

La definición de funtor derivado está dada en términos de una resolución proyectiva de A, para que esté bien definido no debe depender de la resolución elegida. Supongamos que damos otra resolución proyectiva de A. Sea $\tilde{\mathbf{P}}_A$ al complejo trunco asociado a dicha resolución y denotemos como $\tilde{R}^nT$ a los funtores derivados derechos obtenidos.

Teorema 1.5.5 *Si T es un funtor aditivo contravariante entonces, para cada n, hay una equivalencia natural $R^nT \cong \tilde{R}^nT$. En particular, para todo A, $R^nT(A) \cong \tilde{R}^nT(A)$.* ■

En otras palabras, la definición de R^nT es independiente de la resolución proyectiva de A.

Definición 1.5.6 *Si $T = \mathrm{Hom}_R(-,B)$ definimos $Ext^n_R(-,B) = R^nT$. En particular, si $\boldsymbol{P}$ es una resolución proyectiva de A:*

$$Ext^n_R(A,B) = H^n(\mathrm{Hom}_R(\mathbf{P}_A, B)) = Ker(d^*_{n+1})/Im(d^*_n).$$

Corolario 1.5.7 *El módulo $Ext^n_R(A,B)$ es independiente de la elección de la resolución proyectiva de A.* ■

Teorema 1.5.8 *Si B es un R-módulo izquierdo, el funtor $\mathrm{Hom}_R(-,B)$ es naturalmente equivalente a $Ext^0_R(-,B)$. Por lo tanto, para todo R-módulo izquierdo A, existe un isomorfismo $\mathrm{Hom}_R(A,B) \cong Ext^0_R(A,B)$*

Demostración. Sea A un R-módulo y $\mathbf{P} : \cdots \longrightarrow P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \longrightarrow 0$ una resolución proyectiva de A. Por definición $Ext^n_R(A,B) = Ker(d^*_{n+1})/Im(d^*_n)$, para $n = 0$, $Ext^0_R(A,B) = Ker(d^*_1)$. Por otro lado, al aplicarle $\mathrm{Hom}_R(-,B)$ a $\mathbf{P}$ obtenemos:

$$\mathrm{Hom}_R(P_1,B) \xleftarrow{d^*_1} \mathrm{Hom}_R(P_0,B) \xleftarrow{\varepsilon^*} \mathrm{Hom}_R(A,B) \longleftarrow 0 \quad (*)$$

dado que $\mathrm{Hom}_R(-,B)$ es exacto izquierdo, la sucesión $(*)$ es exacta; por lo tanto $Ker(d^*_1) = Im(\varepsilon^*)$. Lo anterior nos da un isomorfismo:

$$Ext^0_R = Ker(d^*_1 = Im(\varepsilon^*) \cong \mathrm{Hom}_R(A,B)/Ker(\varepsilon^*) = \mathrm{Hom}_R(A,B)$$

para cada R-módulo B, los morfismos ε^* constituyen una equivalencia natural de funtores. ■

Proposición 1.5.9 *Sean R y S anillos y tomemos ${}_SA$, ${}_RB_S$ y ${}_RC$ con B proyectivo sobre R. Se tiene el siguiente isomorfismo:*

$$Ext^n_R(B \otimes_S A, C) \cong Ext^n_S(A, \mathrm{Hom}_R(B,C)).$$

Demostración. Tomemos ${}_SA$, ${}_RB_S$ y ${}_RC$ con B proyectivo sobre R, con esto, $B \otimes_R A$ es un S-módulo y $\mathrm{Hom}_S(A, B)$ es un R-módulo. Sean **P** y **P'** resoluciones S-proyectivas de $B \otimes_R A$ y A respectivamente. Por el Teorema 1.3.19 existe un isomorfismo natural $\mathrm{Hom}_S(B \otimes_R A, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$, al tomar los complejos truncos $\mathbf{P}_{B\otimes A}$ y $\mathbf{P}'_A$ esto nos induce un isomorfismo de complejos: $\mathrm{Hom}_S(\mathbf{P}_{B\otimes A}, C) \cong \mathrm{Hom}_R(\mathbf{P}'_A, \mathrm{Hom}_S(B, C))$, así, por el Teorema 1.4.8 $H^n(\mathrm{Hom}_S(\mathbf{P}_{B\otimes A}, C)) \cong H^n(\mathrm{Hom}_R(\mathbf{P}'_A, \mathrm{Hom}_S(B, C)))$, esto es:

$$\begin{aligned} Ext^n_R(B \otimes_S A, C) &= H^n(\mathrm{Hom}_S(\mathbf{P}_{B\otimes A}, C)) \\ &\cong H^n(\mathrm{Hom}_R(\mathbf{P}'_A, \mathrm{Hom}_S(B, C))) \\ &= Ext^n_S(A, \mathrm{Hom}_R(B, C)). \end{aligned}$$

■

Capítulo 2

Extensiones de Grupos

Uno de los procedimientos usuales al estudiar módulos es el análisis de los submódulos y módulos cociente asociados a ellos; en éste contexto surge de manera muy natural el problema de la extensión: Dados dos R-módulos A y B, donde R es un anillo fijo, ¿qué módulos E existen que tengan a A como submódulo y que $B \cong E/A$?.

En nuestro caso trabajaremos con módulos sobre el anillo de grupo $\mathbb{Z}G$. Veremos que dado un $\mathbb{Z}G$-módulo A y una extensión de A por G, ésta induce en A una nueva estructura como $\mathbb{Z}G$-módulo. Aquí el problema de la extensión se traduce en describir las extensiones de A por G en las cuales la estructura de A como $\mathbb{Z}G$ módulo coincide con la inducida por la extensión. Dada la naturaleza del problema la primera pregunta que surge es: Si A es un G-módulo, donde G es un grupo cualquiera, ¿podemos dar una extensión de A por G?, para dar una respuesta es necesario caracterizar al grupo E.

2.1. El problema de la extensión

Definición 2.1.1 *Sea $(G, *)$ un grupo multiplicativo. El anillo de grupo sobre los enteros, denotado por $\mathbb{Z}G$, es el $\mathbb{Z}$-módulo libre con base G. Un elemento típico de $\mathbb{Z}G$ es de la forma $\sum_{x\in G} m_x x$ con $m_x \in \mathbb{Z}$, $x \in G$ y $m_x = 0$ excepto para un número finito de ellos. El producto de dos elementos de $\mathbb{Z}G$ está dado por:*

$$\sum_{x\in G} m_x x \cdot \sum_{y\in G} n_y y = \sum_{x,y\in G} m_x n_y \,(x * y)\,.$$

Obsérvese que la parte aditiva de $\mathbb{Z}G$ es el grupo libre generado por G y no es difícil ver que $\mathbb{Z}G$ es un anillo. El anillo de grupo está caracterizado por la siguiente propiedad universal donde $i : G \longrightarrow \mathbb{Z}G$, la inclusión i.e. $g \overset{i}{\longmapsto} 1g$.

Teorema 2.1.1 ***Propiedad Universal del Anillo de Grupo***. *Para cada anillo R y para cada función $f : G \longrightarrow R$ que cumpla $f(xy) = f(x)f(y)$ y $f(1_G) = 1_R$, existe un único homomorfismo de anillos*

$$\tilde{f} : \mathbb{Z}G \longrightarrow R$$

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

Demostración. Sea R un anillo y $f : G \longrightarrow R$ una función que satisface $f(xy) = f(x)f(y)$ y $f(1_G) = 1_R$. Definimos $\tilde{f} : \mathbb{Z}G \longrightarrow R$ por:

$$\tilde{f}\left(\sum_{x\in G} m_x x\right) = \sum_{x\in G} m_x f(x)$$

Es claro que $\tilde{f}$ es morfismo de anillos. Obsérvese que si $x \in G$ entonces:

$$\tilde{f}i(x) = \tilde{f}(1x) = 1f(x) = f(x)$$

Por último, supongamos que existe otro morfismo de anillos $\hat{f} : \mathbb{Z}G \longrightarrow R$ que cumple que $\hat{f}i = f$ entonces, $\hat{f}i = \tilde{f}i$ y así:

$$\hat{f}i(x) - \tilde{f}i(x) = (\hat{f} - \tilde{f})i(x) = 0_R \text{ para todo } x \in G$$

esto nos dice que $\hat{f} - \tilde{f}$ es el morfismo cero, lo cual implíca que $\hat{f} = \tilde{f}$. ■

Lo anterior significa que para dar un homomorfismo de $\mathbb{Z}G$ en cualquier anillo R es suficiente dar una función de G en R tal que $f(xy) = f(x)f(y)$ y $f(1_G) = 1_R$.

Nota: Para dotar a un grupo abeliano A de una estructura de $\mathbb{Z}G$-Módulo, es suficiente definir la acción de un elemento de G sobre un elemento de A de tal manera que:

$$\begin{aligned} g(a + a') &= ga + ga', \\ (gg')a &= g(g'a), \\ 1_G a &= a. \end{aligned}$$

Supongamos que G actúa sobre A y satisface las propiedades anteriores. Cada $g \in G$ determina un endomorfismo $\sigma_g : A \longrightarrow A$, definido por $\sigma_g(a) = ga$ y, por la propiedad universal del anillo de grupo, se tiene un acción de $\mathbb{Z}G$ sobre los elementos de A, esto es, A es un $\mathbb{Z}G$-módulo. Por otro lado, dado un grupo abeliano A, un homomorfismo $\sigma : G \longrightarrow Aut(A)$ determina una acción de G sobre A, como $Aut(A) \subset End(A)$, la propiedad universal del anillo de grupo garantiza la existencia de un homomorfismo:

$$\tilde{\sigma} : \mathbb{Z}G \longrightarrow End(A),$$

lo cual convierte a A en un módulo (izquierdo) sobre $\mathbb{Z}G$. Por esta razón no habrá confusión en llamar a los $\mathbb{Z}G$-módulos simplemente G-módulos siendo suficiente definir la acción de G sobre A.

Sea $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ un sucesión exacta de grupos donde E es un grupo no necesariamente abeliano, A es un subgrupo normal abeliano de E y $G = E/A$; usaremos la notación aditiva tanto para E como para A y notación multiplicativa para G, a partir de tal sucesión, daremos a A una estructura de $\mathbb{Z}G$-módulo para lo cual, como ya hemos dicho, es suficiente definir cómo actúa G sobre A. Sea $g : E \longrightarrow G$ un homomorfismo suprayectivo, para cada $x \in G$ definimos un **"levantamiento de x"** respecto a g como un elemento $\lambda x \in E$ tal que $g(\lambda x) = x$. En lo sucesivo trabajaremos con éste tipo de sucesiones donde, a menos que se diga lo contrario, entenderemos que A es abeliano y normal en E.

Lema. 2.1.2 *Dada una sucesión exacta* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *y para cada* $x \in G$ *un levantamiento de* x*, éste determina un homomorfismo*

$$\theta : G \longrightarrow Aut(A).$$

Demostración. Sea $x \in G$ y $\lambda x \in E$ un levantamiento de x. Definimos $\theta_x : A \longrightarrow A$ por $\theta_x(a) = \lambda x + a - \lambda x$ donde la operación del lado derecho es en E. Nótese que, como A es normal en E, $Im(\theta_x) \subset A$. La función $\theta : G \longrightarrow Aut(A)$ dada por $x \xmapsto{\theta} \theta_x$ está bien definida, es decir, θ_x no depende del levantamiento de x que tomemos pues si λx y $\lambda' x$ son dos levantamientos de x entonces $-\lambda' x + \lambda x \in A$ ya que $\pi(-\lambda' x + \lambda x) = 0$, dado que A es abeliano, entonces $(-\lambda' x + \lambda' x) + a = a + (-\lambda' x + \lambda' x)$ de lo cual se sigue que $\lambda x + a - \lambda x = \lambda' x + a - \lambda' x$ para todo $x \in G$. Por último θ es morfismo pues,

dado que θ_x no depende del levantamiento, podemos escoger $\lambda(xy) = \lambda x + \lambda y$, entonces, por un lado $\theta(xy) = \theta_{xy}$ que, en los elementos de A, está definido como $\theta_{xy}(a) = \lambda xy + a - \lambda xy$, por otro lado, en $Aut(A)$ la operación binaria es la composición, entonces:

$$\begin{aligned}(\theta_x \circ \theta_y)(a) &= \theta_x(\theta_y(a)) \\ &= \theta_x(\lambda y + a - \lambda y) \\ &= \lambda x + \lambda y + a - \lambda y - \lambda x \\ &= \lambda xy + a - \lambda xy \\ &= \theta_{xy}(a)\end{aligned}$$

Por lo tanto $\theta : G \longrightarrow Aut(A)$ es un homomorfismo de grupos. ■

Teorema 2.1.3 *Si* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *es una sucesión exacta entonces* A *es un* $\mathbb{Z}G$*-Módulo izquierdo.*

Demostración. La acción de G sobre A está dada por el homomorfismo del lema anterior, teniendo en cuenta la Nota, esto es:

$$x \cdot a = \theta_x(a) = \lambda x + a - \lambda x$$

como θ es homomorfismo se tiene que $1_G a = a$ y $(xy) = x(ya)$, con esto en mente, resulta natural definir la acción de un elemento arbitrario de $\mathbb{Z}G$ de la siguiente manera:

$$(\textstyle\sum_{x \in G} m_x x)a = \sum_{x \in G} m_x(xa)$$

■

Un G-módulo izquierdo A se llama **trivial** si la acción de G sobre A es trivial, es decir, si $x \cdot a = a$ para todo $x \in G$ y para todo $a \in A$.

Sea A un G-módulo izquierdo para el cual denotamos la acción de G como $x \cdot a$ y consideremos una sucesión exacta:

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

En virtud del Teorema 2.1.3, A adquiere una nueva estructura de G-módulo, ciertamente nada garantiza que esta nueva estructura de A, como G-módulo, coincida con la que ya poseía. Discutiremos cuándo es que ambas estructuras coinciden, para esto, diremos que un G-módulo izquierdo A **realiza los operadores** si las dos acciones de G sobre A coinciden, es decir:

$$x \cdot a = \theta_x(a) = \lambda x + a - \lambda x$$

Definición. 2.1.4 *Sea G un grupo y A un G-módulo. Una* ***extensión de A por G*** *es una sucesión exacta corta* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *donde A realiza los operadores.*

Es así como planteamos el problema de la extensión el cual será el tema principal de este capítulo, apegándonos a la definición anterior, dicho problema consiste en clasificar las extensiones de A por G.

En nuestro intento por dar una extensión de A por G, lo primero que estamos tentados a hacer es tomar el producto cartesiano de A por G y definir la suma como $(a, x) + (b, y) = (a + b, xy)$, dicha operación es asociativa, con esto $A \times G$ adquiere estructura de grupo donde el inverso de (a, x) es $(-a, x^{-1})$ y el neutro es $(0, 1_G)$; se tiene un monomorfismo $i : A \longrightarrow A \times G$ definido por $i(a) = (a, 1_G)$ y un epimorfismo $\pi : A \times G \longrightarrow$ definido por $\pi(a, x) = x$, además $i(A)$ es normal en $A \times G$. Así, la sucesión

$$0 \longrightarrow A \xrightarrow{i} A \times G \xrightarrow{\pi} G \longrightarrow 1$$

es exacta y sólo faltaría verificar que A realiza los operadores. Por el Teorema 1.1.4 sabemos que A adquiere una nueva estructura de G-módulo, si $*$ denota la nueva acción de G sobre A, queremos que $x * a = \lambda x + a - \lambda x$ y teniendo en cuenta que la operación del lado derecho es en E esto se vería como:

$$x * a = (0, x) + (a, 1_G) - (0, x)$$

sin embargo, al realizar ésta operación tenemos que:

$$x * a = (0, x) + (a, 1_G) - (0, x) = (a, 1_G)$$

esto significa que la estructura de A como G-módulo es trivial y no necesariamente coincide con la estructura de G-módulo que A poseía en un principio. Así, para obtener una extensión de A por G, vemos que no basta con definir la operación entrada a entrada en el producto cartesiano. Al revisar nuevamente: $x * a = (0, x) + (a, 1_G) - (0, x) = (a, 1_G)$, notamos que la única diferencia se da en la primera entrada, esto nos dice que es necesario introducir una operación de manera que, en la primera entrada, aparezca la acción de G sobre A que ya teníamos, es así como introducimos el concepto de producto semidirecto de A por G.

Definición 2.1.5 *Dado un grupo G y un G-módulo A, definimos su producto semidirecto el cual denotamos como $A \times G$. El conjunto soporte de $A \times G$ es el conjunto de parejas ordenadas (a, x) con $a \in A$, $x \in G$ y la operación en $A \times G$ se define como sigue:*

$$(a, x) + (a', y) = (a + xa', xy)$$

Como esta operación es asociativa, tiene elemento neutro $(0, 1_G)$ e inverso de (a, x) a $(-x^{-1}a, x^{-1})$, el producto semidirecto $A \times G$ es un grupo.

Dados el monomorfismo $i : A \longrightarrow A \times G$ definido por $i(a) = (a, 1_G)$ y el epimorfismo $p : A \times G \longrightarrow$ definido por $p(a, x) = x$, es fácil ver que $i(A)$ es normal en $A \times G$ y que $(A \times G)/i(A) \cong G$, por lo que la siguiente sucesión es exacta:

$$0 \longrightarrow A \xrightarrow{i} A \times G \xrightarrow{p} G \longrightarrow 1 \quad \textbf{(1.1)}$$

Más aún, si denotamos como $*$ a la nueva acción de G sobre A, se tiene:

$$\begin{aligned} x * a &= (0, x) + (a, 1_G) - (0, x) \\ &= (xa, x) + (0, x^{-1}) \\ &= (xa, xx^{-1}) \\ &= (xa, 1_G) \end{aligned}$$

Es decir, la extensión más simple de A por G que podemos dar es aquella donde se considera un producto semidirecto; vale la pena caracterizar a éstas extensiones, ello dará la pauta para poder resolver el problema de la extensión de manera general.

Definición 2.1.6 *Una extensión $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ se escinde si existe un morfismo $\lambda : G \longrightarrow E$ tal que $\pi\lambda = id_G$*

Nótese que, para la extensión (1.1), la función definida por:

$$\begin{aligned} q : G &\longrightarrow A \times G \\ x &\longmapsto (0, x) \end{aligned}$$

es evidentemente un morfismo de grupos que cumple $pq(x) = p(0, x) = x$, esto es, la extensión (1,1) se escinde.

Teorema 2.1.7 *Una extensión*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

se escinde si y sólo si E contiene un subgrupo $C \cong G$ (no necesariamente normal) tal que $A + C = E$ y $A \cap C = \{0\}$

Demostración. Supongamos que dicha sucesión se escinde, es decir, existe un morfismo $\lambda : G \longrightarrow E$ tal que $\pi\lambda = id_G$. Denotemos $Im(\lambda) = C$, λ es monomorfismo pues tiene inverso izquierdo y por tanto es un isomorfismo entre G y C. Dicho esto, vemos que cada elemento de C, distinto de cero, corresponde a una única clase en G módulo A distinta de la clase del 1 por lo que C está determinado por un conjunto completo de representantes módulo A (se dice en este caso que C es un transversal de A en E). Ahora, cada $y \in E$ se puede escribir como

$$y = y - \lambda\pi(y) + \lambda\pi(y)$$

donde es claro que $y - \lambda\pi(y) \in Ker(\pi) = A$ y $\lambda\pi(y) \in Im(\lambda) = C$ lo cual muestra que $E = A + C$. Por último, si $x \in A$ entonces $\pi(x) = \bar{1}$ y si $x \in C$ entonces $x = \lambda(g)$ para algún $g \in G$ por lo que $\pi(x) = \pi(\lambda(g)) = g$, así, si $x \in A \cap C$ vemos que $x = \lambda(\bar{1})$ y, dado que λ es morfismo, $\lambda(\bar{1}) = 0$, por lo tanto $x = 0$, ésto quiere decir que $A \cap C = \{0\}$.

Recíprocamente, supongamos que cada $x \in E$ se puede escribir de manera única como $x = a + c$ con $a \in A$ y $c \in C$, sabemos que π es epimorfismo, entonces, la restricción $\pi \mid_C$ también lo es, más aún, $\pi \mid_C$ es isomorfismo, por lo cual basta definir $\lambda : G \longrightarrow E$ como $\lambda := (\pi \mid_C)^{-1}$. ■

Definición. 2.1.8 *Sea* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *una extensión.*
Un levantamiento es una ***función*** $\lambda : G \longrightarrow E$ *que cumple* $\pi\lambda = id_G$ *y* $\lambda(1_G) = 0$

Lema. 2.1.9 *Una extensión se escinde si y sólo si existe un levantamiento que es un homomorfismo.* ■

Teorema 2.1.10 *Una extensión* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *se escinde si y sólo si existe un levantamiento λ tal que la función $\varphi : E \longrightarrow A \times G$ definida por* $a + \lambda x \xmapsto{\varphi} (a, x)$ *es un isomorfismo.*

Demostración. Supongamos que se tiene una extensión

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

y que dicha extensión se escinde. La existencia del levantamiento λ está garantizada por el lema anterior, más aún, λ es un homomorfismo. Nótese que φ es morfismo pues:

$$\begin{aligned}(a + \lambda x) + (a' + \lambda y) &= a + \lambda x + a' - \lambda x + \lambda x + \lambda y \\ &= a + (\lambda x + a' - \lambda x) + \lambda x + \lambda y \\ &= a + xa' + \lambda(xy)\end{aligned}$$

Por lo cual, se tiene que:

$$\begin{aligned}\varphi((a + \lambda x) + (a' + \lambda y)) &= \varphi(a + xa' + \lambda(xy)) \\ &= (a + xa', xy) \\ &= (a, x) + (a', y) \\ &= \varphi(a + \lambda x) + \varphi(a' + \lambda y)\end{aligned}$$

Por último, el Teorema 2.1.7 dice que la expresión de los elementos $e \in E$ como $e = a + \lambda x$ es única, de lo cual se sigue que φ está bien definida y es biyectiva, por lo tanto es un isomorfismo.

Recíprocamente, defínase $\lambda' : G \longrightarrow A \times G$ como $x \mapsto (0, x)$ y obsérvese que λ' es morfismo, además, $\lambda' = \varphi\lambda$ y como φ es isomorfismo por hipótesis entonces $\lambda = \varphi^{-1}\lambda'$ es un homomorfismo, así, por el Lema 2.1.9 la extensión se escinde. ■

Los Teoremas 2.1.7 y 2.1.10 explican el por qué llamamos a $A \times G$ producto semidirecto; lo primero es que el complemento de A, $Im(\lambda) = C$, no necesariamente es único, también, para que $A \times G = E$ sea un producto directo requiere, además de $E = A + C$ y $A \cap C = 0$, que tanto A como C sean normales en E lo cual sólo podemos garantizar para A.

Para poder resolver el problema de la extensión en su forma general, considerese la siguiente situación. Supongamos que se tiene una extensión de A

por $G\ \ 0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ y un levantamiento $\lambda : G \longrightarrow E$ (λ no necesariamente es un homomorfismo), por un argumento similar al del Teorema 2.1.7 tenemos que $Im(\lambda)$ es un transversal de A en E. Dado que $\lambda(\bar{1}) = 0$ entonces, cada elemento de E puede ser expresado de manera única como $a + \lambda x$, por lo cual, caracterizar al grupo E significa decir cómo se suman sus elementos, para esto, primero nótese que λxy y $\lambda x + \lambda y$ representan la misma clase módulo A pues se tiene que:

$$\begin{aligned}\pi(\lambda x + \lambda y - \lambda xy) &= \pi(\lambda x + \lambda y)\pi(-\lambda xy) \\ &= \pi(\lambda x)\pi(\lambda y))(\pi\lambda xy)^{-1} \\ &= xy(xy)^{-1} \\ &= \bar{1}\end{aligned}$$

Lo anterior quiere decir que $\lambda x + \lambda y - \lambda xy \in A$, así, $(\lambda x + \lambda y) - \lambda xy = \tilde{a}$ para algún $\tilde{a} \in A$ por lo cual tenemos que $(\lambda x + \lambda y) = \tilde{a} + \lambda xy$. Ahora, para definir la suma en E pedimos que $(a + \lambda x) + (a' + \lambda y) = a'' + \lambda z$, para algún $a'' \in A$ y algún $\lambda z \in Im(\lambda)$, entonces:

$$(a + \lambda x) + (a' + \lambda y) = a + \lambda x + a' - \lambda x + \lambda x + \lambda y =$$
$$(a + \lambda x + a' - \lambda x) + \lambda x + \lambda y = (a + \lambda x + a' - \lambda x + \tilde{a}) + \lambda xy$$

Así, haciendo $a'' = a + \lambda x + a' - \lambda x - \tilde{a}$ y $\lambda z = \lambda xy$ hemos obtenido la suma en E, obsérvese que el elemento $\tilde{a}$ da cuenta de la relación entre $\lambda(xy)$ y $\lambda x + \lambda y$ al definir la suma en E, más aún, $\tilde{a}$ está determinado por la diferencia $\lambda x + \lambda y - \lambda xy$; si denotamos a $\tilde{a}$ como $f(x, y)$ ya que depende de x y y entonces, esto nos determina una función $f : G \times G \longrightarrow A$. Estas funciones serán la herramienta que nos permitirá dar respuesta al problema de la extensión pues dado un grupo E, al saber cómo son sus elementos, habremos de recurrir a dichas funciones para dar la operación en E.

Definición. 2.1.11 *Dado un levantamiento $\lambda : G \longrightarrow E$. A la función $f : G \times G \longrightarrow A$ definida por $f(x, y) = \lambda x + \lambda y - \lambda(xy)$ se le llama conjunto factor.*

Es evidente que los conjuntos factor están dados en términos de levantamientos. Nótese que, cuando una sucesión se escinde, tenemos un levantamiento que también es homomorfismo y el conjunto factor asociado a éste es la función cero.

Teorema 2.1.12 *Sea A un G-módulo. Una función $f : G \times G \longrightarrow A$ es un conjunto factor si y sólo si cumple, para todo $x, y, z \in G$:*
i) $f(x, 1) = 0 = f(1, x)$
ii) $xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$

Supongamos que la función $f : G \times G \longrightarrow A$ es un conjunto factor. Entonces

$$f(x, 1) = \lambda x + \lambda 1 - \lambda(1x) = \lambda x + 0 - \lambda x = 0.$$

Análogamente se prueba que $f(1, x) = 0$ lo cual demuestra $i)$. Ahora:

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) =$$
$$x(\lambda y + \lambda z - \lambda yz) - (\lambda xy + \lambda z - \lambda xyz) + (\lambda x + \lambda yz - \lambda xyz) - (\lambda x + \lambda y - \lambda xy) =$$

todos estos términos son elementos de A y, dado que A es abeliano, podemos conmutar los dos términos de en medio y nos queda:

$$x(\lambda y + \lambda z - \lambda yz) + (\lambda x + \lambda yz - \lambda xyz) - (\lambda xy + \lambda z - \lambda xyz) - (\lambda x + \lambda y - \lambda xy)$$

el primero de estos términos es de la forma xa y sabemos que $xa = \lambda x + a - \lambda x$ por lo cual tenemos

$$\lambda x + (\lambda y + \lambda z - \lambda yz) - \lambda x + (\lambda x + \lambda yz - \lambda xyz) - (\lambda xy + \lambda z - \lambda xyz) - (\lambda x + \lambda y - \lambda xy)$$

esto, después de conmutar los dos últimos términos y cancelar usando la asociatividad de la suma en E, nos queda

$$\lambda x + \lambda y + \lambda z - \lambda xyz - \lambda x - \lambda y - \lambda z + \lambda xyz =$$
$$\lambda x + \lambda y + \lambda z - \lambda xyz - (\lambda x + \lambda y + \lambda z - \lambda xyz) = 0$$

lo cual prueba $ii)$.

Recíprocamente, supongamos que tenemos una función $f : G \times G \longrightarrow A$ que cumple con $i)$ y $ii)$. Debemos construir una extensión de A por G y escoger un levantamiento λ de tal manera que f satisfaga $f(x, y) = \lambda x + \lambda y - \lambda(xy)$. Sea A un G-módulo y consideremos $A \ltimes G$ el conjunto de parejas ordenadas donde la suma se define como:

$$(a, x) + (a', y) = (a + xa' + f(x, y), xy) \tag{2.1}$$

Esta operación es asociativa y tiene por elemento neutro a $(0, 1)$ y como inverso de (a, x) a $(-x^{-1}a - x^{-1}f(x, x^{-1}), x^{-1})$, por tanto, $E = A \ltimes G$ es un grupo y $A \lhd A \ltimes G$. Defínase:

$$\begin{array}{c}\pi : E \longrightarrow G \\ (a,x) \longmapsto x\end{array}$$

claramente π es un epimorfismo cuyo núcleo es el conjunto $\{(a,1) \mid a \in A\}$ el cual identificamos con A mediante la inclusión, así, obtenemos una sucesión

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1\ .$$

Si $\lambda : G \longrightarrow E$ es un levantamiento cualquiera veamos que A realiza los operadores, dado $x \in G$, $\lambda x = (a', x)$ para algún $a' \in A$, así:

$$\begin{aligned}\lambda x + (a,1) - \lambda x &= (a',x) + (a,1) - (a',x) \\ &= (a' + xa + f(x,1), x) + (-x^{-1}a' - x^{-1}f(x,x^{-1}), x^{-1}) \\ &= (a' + xa + x[-x^{-1}a' - x^{-1}f(x,x^{-1})] + f(x,x^{-1}), 1) \\ &= (a' + xa - a' - f(x,x^{-1}) + f(x,x^{-1}), 1) \\ &= (xa, 1)\end{aligned}$$

Dado que en la sucesión anterior identificamos a A con la imagen de la inclusión i, lo anterior nos dice que $xa = \lambda x + a - \lambda x$, es decir, A realiza los operadores de dicha sucesión. Por último debemos ver que f es el conjunto factor determinado por algún levantamiento, si definimos $\hat{\lambda} : G \longrightarrow E$ por $\hat{\lambda}x = (0,x)$ entonces:

$$\begin{aligned}\hat{\lambda}x + \hat{\lambda}y - \hat{\lambda}xy &= (0,x) + (0,y) - (0,xy) \\ &= (f(x,y), xy) + (-(xy)^{-1}f(xy,(xy)^{-1}), (xy)^{-1}) \\ &= (f(x,y) + xy[-(xy)^{-1}f(xy,(xy)^{-1})] + f(xy,(xy)^{-1}), 1) \\ &= (f(x,y) - f(xy,(xy)^{-1}) + f(xy,(xy)^{-1}, 1) \\ &= (f(x,y), 1)\end{aligned}$$

recordando que $\hat{\lambda}x + \hat{\lambda}y - \hat{\lambda}xy \in A$, esto quiere decir que $f(x,y) = \hat{\lambda}x + \hat{\lambda}y - \hat{\lambda}xy$, es decir, $f(x,y) + \hat{\lambda}xy = \hat{\lambda}x + \hat{\lambda}y$, dicho de otra manera, f es el conjunto factor determinado por este levantamiento. ■

Teorema 2.1.13 *Sea A un G-módulo y $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ una extensión. Si $f : G \times G \longrightarrow A$ es un conjunto factor determinado por un levantamiento λ, entonces la función:*

$$\eta : E \longrightarrow A \ltimes G$$

$$e = a + \lambda x \mapsto (a, x)$$

es un isomorfismo. Donde la operación en $A \ltimes G$ está definida como en (2.1).

Demostración. Sea $\lambda : G \longrightarrow E$ un levantamiento, éste determina un conjunto factor $f : G \times G \longrightarrow A$ dado por $\lambda x + \lambda y = f(x, y) + \lambda xy$. Sabemos que cada elemento $e \in E$ tiene una expresión única $e = a + \lambda x$ con $a \in A$ y $x \in G$, la unicidad de dicha expresión implica que la función η está bien definida y es biyectiva. Por último se tiene que:

$$\begin{aligned}
\eta(a + \lambda x + b + \lambda y) &= \eta(a + \lambda x + b - \lambda x + \lambda x + \lambda y) \\
&= \eta(a + xb + \lambda x + \lambda y) \\
&= \eta(a + xb + f(x, y) + \lambda xy) \\
&= (a + xb + f(x, y), xy) \\
&= (a, x) + (b, y) \text{ (por def. de suma en } A \ltimes G) \\
&= \eta(a + \lambda x) + \eta(b + \lambda y)
\end{aligned}$$

lo cual demuestra que η es un morfismo. ■

Éste último resultado describe a las extensiones de A por G, nótese que los grupos E están determinados (salvo isomorfismo) en términos de los conjuntos factor.

2.2. Extensiones equivalentes

Hemos visto que al tomar un levantamiento λ de este se deriva un conjunto factor, dicho conjunto factor caracteriza la suma en E, la siguiente pregunta es: ¿qué sucede con el conjunto factor al considerar un levantamiento, λ', distinto?, de esto hablan los siguientes resultados.

Definición. 2.2.1 *$Z^2(G, A)$ es el grupo abeliano de los conjuntos factor bajo la adición puntual.*

Respecto de este grupo, es importante aclarar quién es el neutro y quién el inverso. Dados dos conjuntos factor, f y f', su suma está definida como: $(f + f')(x, y) = f(x, y) + f'(x, y)$ entonces, el neutro aditivo será un elemento que cumpla:

$$(f + f')(x, y) = f(x, y) \text{ para todo } (x, y) \in G \times G$$

sabemos que $f(x, y) = \lambda x + \lambda y - \lambda xy$ y $f'(x, y) = \lambda' x + \lambda' y - \lambda' xy$, al sustituir esto, queremos saber en qué caso la siguiente igualdad es válida

$$\lambda x + \lambda y - \lambda xy + \lambda' x + \lambda' y - \lambda' xy = \lambda x + \lambda y - \lambda xy$$

lo anterior es válido si y sólo si $\lambda' x + \lambda' y - \lambda' xy = 0$, es decir, si y sólo si $\lambda' x + \lambda' y = \lambda' xy$ para todo $x, y \in G$ lo cual sólo ocurre cuando consideramos a $E = A \times G$, el producto semidirecto. En otras palabras, el neutro aditivo de $Z^2(G, A)$ es el conjunto factor asociado al producto semidirecto de A por G. Ahora, el inverso aditivo debe ser un conjunto factor que cumpla:

$$(f + f')(x, y) = 0 \text{ para todo } (x, y) \in G \times G$$

observando que tanto $f(x, y)$ como $f'(x, y)$ están en A, queda claro que el inverso de f en $Z^2(G, A)$ queda determinado por el inverso de $f(x, y)$ en A, es decir, $-f(x, y) = -(\lambda x + \lambda y - \lambda xy)$ lo cual evidentemente también es un conjunto factor.

Teorema 2.2.2 *Sea* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *una extensión y sean* λ *y* λ' *dos levantamientos. Si* f *y* f' *son los conjuntos factor asociados a* λ *y* λ' *respectivamente entonces, existe una función:*

$$d : G \longrightarrow A$$

que satisface:
i)$d(1) = 0$
ii)$f'(x, y) - f(x, y) = xd(y) - d(xy) + d(x)$ *para todo* $x, y \in G$

Demostración. Para dar la función d, primero nótese que para cualquier $x \in G$, λx y $\lambda' x$ están en la misma clase de equivalencia de G (módulo A) por lo que existe $a \in A$ tal que $a = \lambda x - \lambda' x$ entonces, definimos:

$$d : G \longrightarrow A$$

$$d(x) = \lambda' x - \lambda x$$

Dado que $\lambda(\bar{1}) = \lambda'(\bar{1}) = 0$ se tiene $d(1) = 0$ lo cual prueba $i)$. Para probar $ii)$ tenemos:

$$\begin{aligned}
\lambda' x + \lambda' y &= \lambda' x - \lambda x + \lambda x + \lambda' y - \lambda y + \lambda y \\
&= d(x) + \lambda x + d(y) + \lambda y \\
&= d(x) + (\lambda x + d(y) - \lambda x) + \lambda x + \lambda y \\
&= d(x) + xd(y) + \lambda x + \lambda y \\
&= d(x) + xd(y) + f(x,y) + \lambda xy \\
&= d(x) + xd(y) + f(x,y) + \lambda xy - \lambda' xy + \lambda' xy \\
&= d(x) + xd(y) + f(x,y) - d(xy) + \lambda' xy
\end{aligned}$$

Todos los términos del lado derecho están en A el cual es abeliano, conmutando y restando nos queda:

$$\lambda' x + \lambda' y - \lambda' xy - f(x,y) = d(x) + xd(y) - d(xy)$$

esto último es:

$$f'(x,y) - f(x,y) = d(x) + xd(y) - d(xy)$$

■

Definición. 2.2.3 *$B^2(G,A)$ es el conjunto de todas las funciones*

$$f : G \times G \longrightarrow A$$

para las que existe una función $d : G \longrightarrow A$ con $d(1) = 0$ tal que:

$$f(x,y) = xd(y) - d(xy) + d(x)$$

A los elementos de $B^2(G,A)$ se les llama cofronteras.

Proposición. 2.2.4 *$B^2(G,A)$ es un subgrupo de $Z^2(G,A)$.*

Demostración. Sean $f,\ f' \in B^2$ y $d, d' : G \longrightarrow A$ las funciones de la Definición 2.2.3 asociadas a f y f' respectivamente. Para $f + f'$ tomamos $\bar{d} : G \longrightarrow A$ como $\bar{d}(x) = d(x) + d'(x)$ y tenemos que $\bar{d}(1) = d(1) + d'(1) = 0$, además es tal que:

$$\begin{aligned}
(f + f')(x,y) &= f(x,y) + f'(x,y) \\
&= xd(y) - d(xy) + d(x) + xd'(y) - d'(xy) + d'(x) \\
&= x(d(y) + d'(y)) - (d(xy) + d'(xy)) + d(x) + d'(x) \\
&= x\bar{d}(y) + \bar{d}(xy) + \bar{d}(x)
\end{aligned}$$

por lo cual, B^2 es cerrado bajo la suma. El Teorema 2.1.12 da una caracterización de los conjuntos factor, así, basta verificar que si $f \in B^2$:

i) $f(1,x) = 0 = f(x,1)$ para todo $x \in G$

$f(1,x) = 1d(x) - d(x) + d(1) = d(x) - d(x) + 0 = 0$, de manera análoga se muestra que $f(x,1) = 0$

ii) $xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$

tenemos que:
$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) =$
$x(yd(z) - d(yz) + d(y)) - (xyd(z) - d(xyz) + d(xy)) + (xd(yz) - d(xyz) + d(x)) - (xd(y) - d(xy) + d(x))$
todos estos términos están en A, así que podemos conmutar y nos queda:
$xyd(z) - xyd(z) + xd(yz) - xd(yz) + xd(y) - xd(y) + d(xyz) - d(xyz) + d(xy) - d(xy) + d(x) - d(x) = 0$
Por lo tanto los elementos de B^2 son conjuntos factor. Sólo resta observar que para el neutro aditivo, el cual corresponde al conjunto factor asociado al producto semidirecto de A por G, tomamos la función $d : G \longrightarrow A$ tal que $d(x) = 0$ para todo $x \in G$ con lo cual se cumplen $i)$ y $ii)$, así, $B^2(G,A)$ es subgrupo de $Z^2(G,A)$. ■

Definición. 2.2.5 *Tomando en cuenta el resultado anterior, tiene sentido el cociente:* $e(G,A) = Z^2(G,A)/B^2(G,A)$.

En resumen, dada una extensión $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$, al tomar dos levantamientos λ y λ', esencialmente definen el mismo conjunto factor en el sentido de que representan al mismo elemento en $e(G,A)$.

Corolario. 2.2.6 *Dos conjuntos factor de una extensión, derivados de levantamientos distintos, determinan el mismo elemento de* $e(G,A)$. ■

Este último resultado nos conduce a la siguiente relación de equivalencia.

Definición. 2.2.7 *Dadas dos extensiones* $0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ *y* $0 \longrightarrow A \longrightarrow E' \longrightarrow G \longrightarrow 1$ *decimos que son equivalentes si existen conjuntos factor* f *y* $\bar{f}$ *de cada una de ellas tal que* $f - \bar{f} \in B^2(G,A)$.

De lo anterior concluimos que el conjunto factor asociado a una extensión no depende del levantamiento que escojamos. Por otro lado, el siguiente teorema nos aclara qué sucede con dos extensiones equivalentes al tomar conjuntos factor distintos.

Teorema 2.2.8 *Tomemos dos extensiones equivalentes:*
$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ *y* $0 \longrightarrow A \longrightarrow E' \longrightarrow G \longrightarrow 1$ *es decir, existen conjuntos factor* f *y* $\bar{f}$ *asociados a ellas respectivamente tales que* $f - \bar{f} \in B^2(G, A)$. *Si* f' *y* $\bar{f}'$ *son otros dos conjuntos factor asociados a dichas extensiones, entonces* $f' - \bar{f}' \in B^2(G, A)$.

Demostración. Por hipótesis $f - \bar{f} \in B^2(G, A)$, sabemos que existe $d : G \longrightarrow A$ tal que $d(1) = 0$ y

$$f(x, y) - \bar{f}(x, y) = xd(y) - d(xy) + d(x) \text{ para todo } x, y \in G \quad (1)$$

También, por el Teorema 2.2.2, sabemos que para f y f', existe $g : G \longrightarrow A$ con $g(1) = 0$ y

$$f(x, y) - f'(x, y) = xg(y) - g(xy) + g(x) \text{ para todo } x, y \in G \quad (2)$$

igualmente, para $\bar{f}$ y $\bar{f}'$, existe $h : G \longrightarrow A$ tal que $h(1) = 0$ y

$$\bar{f}(x, y) - \bar{f}'(x, y) = xh(y) - h(xy) + h(x) \text{ para todo } x, y \in G \quad (3)$$

Ahora, según la definición de B^2, debemos dar una función $d' : G \longrightarrow A$ tal que, $d'(1) = 0$ y $f'(x, y) - \bar{f}'(x, y) = xd'(y) - d'(xy) + d'(x)$, para ello, basta observar que podemos escribir la diferencia $f' - \bar{f}'$ como

$$f'(x, y) - \bar{f}'(x, y) = \bar{f}(x, y) - \bar{f}'(x, y) - \{f(x, y) - f'(x, y)\} + f(x, y) - \bar{f}(x, y)$$

considerando (1), (2) y (3), resulta natural definir

$$d'(x) = (h - g + d)(x)$$

Por último tenemos:

$$i) d'(1) = (h - g + d)(1) = h(1) - g(1) + d(1) = 0$$

$$ii) f'(x, y) - \bar{f}'(x, y) = \bar{f}(x, y) - \bar{f}'(x, y) - \{f(x, y) - f'(x, y)\} + f(x, y) - \bar{f}(x, y)$$

$$= xh(y) - h(xy) + h(x) - \{xg(y) - g(xy) + g(x)\} + xd(y) - d(xy) + d(x)$$

$$= xh(y) - h(xy) + h(x) - xg(y) + g(xy) - g(x) + xd(y) - d(xy) + d(x)$$

$$= xh(y) - xg(y) + xd(y) - h(xy) + g(xy) - d(xy) + h(x) - g(x) + d(x)$$

$$= x[h(y) - g(y) + d(y)] - \{h(xy) - g(xy) + d(xy)\} + h(x) - g(x) + d(x)$$

$= xd'(y) - d'(xy) + d'(x)$

Por lo tanto $f' - \bar{f}' \in B^2(G, A)$. ■

Teorema 2.2.9 *Dos extensiones de A por G* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *y* $0 \longrightarrow A \xrightarrow{i} E' \xrightarrow{\pi} G \longrightarrow 1$ *son equivalentes si y sólo si existe un morfismo $\varphi : E \longrightarrow E'$ tal que el siguiente diagrama conmuta:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id_G} & & \\ 0 & \longrightarrow & A & \xrightarrow[i']{} & E' & \xrightarrow[\pi']{} & G & \longrightarrow & 1 \end{array}$$

Más aún, todo morfismo φ que haga conmutar dicho diagrama es un isomorfismo.

Demostración. Supongamos que las extensiones son equivalentes. Deduciremos cómo debe ser el morfismo φ. Sean $\lambda : G \longrightarrow E$ y $\lambda' : G \longrightarrow E'$ dos levantamientos y consideremos el diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \underset{\lambda}{\overset{\pi}{\rightleftarrows}} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id_G} & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & E' & \underset{\lambda'}{\overset{\pi'}{\rightleftarrows}} & G & \longrightarrow & 1 \end{array}$$

Sean f y f' los conjuntos factor asociados a λ y λ' respectivamente. Por la definición de equivalencia de extensiones sabemos que existe $h : G \longrightarrow A$ tal que:

$$f(x, y) - f'(x, y) = xh(y) - h(xy) + h(x)$$

Cada elemento $e \in E$ se escribe de manera única como $e = a + \lambda x$ con $a \in A$ y $x \in G$, igualmente cada $e' \in E'$ se escribe como $e' = a + \lambda' x$, tomando esto en cuenta resulta natural pensar en definir $\varphi(a + \lambda x) = a + \lambda' x$, nótese que, definiendola así, φ hace conmutar el diagrama. Para el primer cuadrado recordemos que $\lambda 1 = 0$ y $\lambda' 1 = 0$, por lo que $i(a) = a + 0 = a + \lambda 1$ y $i'(a) = a + 0 = a + \lambda' 1$; para el segundo cuadrado basta recordar que

$\pi(a + \lambda x) = x = \pi'(a + \lambda' x)$, todo esto garantiza la conmutatividad de los siguientes cuadrados:

$$\begin{array}{ccc} a & \xrightarrow{i} & a + \lambda 1 \\ {\scriptstyle id_A}\downarrow & & \downarrow{\scriptstyle \varphi} \\ a & \xrightarrow{i'} & a + \lambda' 1 \end{array} \qquad \begin{array}{ccc} a + \lambda x & \xrightarrow{\pi} & x \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle id_G} \\ a + \lambda' x & \xrightarrow[\pi']{} & x \end{array}$$

Sólo falta asegurar que φ es morfismo, es decir, queremos saber si la siguiente igualdad es válida:

$$\varphi(a + \lambda x + a' + \lambda y) = \varphi(a + \lambda x) + \varphi(a' + \lambda y) \quad (1)$$

Sabemos que la suma en E está dada en términos del conjunto factor f asociado a λ (Teorema 2.1.12), es decir: $a+\lambda x+a'+\lambda y = a+xa'+f(x,y)+\lambda xy$ y análogamente para la suma en E'. Entonces el primer término de la igualdad (1) es:

$$\varphi(a + \lambda x + a' + \lambda y) = \varphi(a + xa' + f(x,y) + \lambda xy) = a + xa' + f(x,y) + \lambda' xy$$

y por otro lado, el segundo término de la igualdad nos queda:

$$\varphi(a + \lambda x) + \varphi(a' + \lambda y) = a + \lambda' x + a' + \lambda' y = a + xa' + f'(x,y) + \lambda' xy$$

Entonces, la igualdad (1) es válida si y sólo si:

$$a + xa' + f(x,y) + \lambda' xy = a + xa' + f'(x,y) + \lambda' xy$$

y al cancelar $a + xa'$ y $\lambda' xy$, esto es equivalente a $f(x,y) = f'(x,y)$. En otras palabras, φ tal como fue definido, es morfismo si y sólo si $f(x,y) - f'(x,y) = 0$ para todo $x, y \in G$; sin embargo esto no siempre sucede y por tanto la definición que hemos dado de φ no sirve. Lo que sí podemos garantizar es que, por definición de equivalencia de extensiones:

$$f(x,y) - f'(x,y) = xh(y) - h(xy) + h(x)$$

Es de esta igualdad que nos valdremos para deducir la definición correcta de φ; todos los términos de dicha igualdad están en A y como A es abeliano podemos conmutarlos de tal manera que nos quede:

$$h(xy) + f(x,y) = xh(y) + h(x) + f'(x,y)$$

y sumando $a + xa'$ tenemos:

$$\begin{aligned} a + xa' + h(xy) + f(x,y) &= a + xa' + xh(y) + h(x) + f'(x,y) \\ &= a + h(x) + x(a' + h(y)) + f'(x,y) \end{aligned}$$

recordando que $x(a' + h(y)) = \lambda' x + (a' + h(y)) - \lambda' x$ y que $f'(x,y) + \lambda' xy = \lambda' x + \lambda' y$, al sumar $\lambda' xy$ a ambos miembros de la igualdad obtenemos:

$$a + xa' + h(xy) + f(x,y) + \lambda' xy = a + h(x) + \lambda' x + (a' + h(y)) - \lambda' x + \lambda' x + \lambda' y$$

con lo que finalmente llegamos a la expresión:

$$a + xa' + h(xy) + f(x,y) + \lambda' xy = (a + h(x) + \lambda' x) + (a' + h(y) + \lambda' y)$$

Al observar esta última igualdad, no es difícil convencerse de que la definición correcta de φ es:

$$\varphi(a + \lambda x) = a + h(x) + \lambda' x$$

donde $h : G \longrightarrow A$ es tal que $h(1) = 0$ (Teorema 2.2.2). Los siguientes cuadrados muestran que φ hace conmutar el diagrama, sólo obsérvese que $i'(a) = a + 0 = a + h(1) + \lambda' 1$:

$$\begin{array}{ccc} a & \overset{i}{\longmapsto} & a + \lambda 1 \\ {\scriptstyle id_A}\downarrow & & \downarrow{\scriptstyle \varphi} \\ a & \overset{i'}{\longmapsto} & a + h(1) + \lambda' 1 \end{array} \qquad \begin{array}{ccc} a + \lambda x & \overset{\pi}{\longmapsto} & x \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle id_G} \\ a + h(x) + \lambda' x & \underset{\pi'}{\longmapsto} & x \end{array}$$

Es claro, por la construcción que se hizo, que φ es morfismo, más aún, φ es necesariamente un isomorfismo pues en el diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \overset{i}{\longrightarrow} & E & \overset{\pi}{\longrightarrow} & G & \longrightarrow & 1 \\ & & {\scriptstyle id_A}\downarrow & & {\scriptstyle \varphi}\downarrow & & {\scriptstyle id_G}\downarrow & & \\ 0 & \longrightarrow & A & \underset{i'}{\longrightarrow} & E' & \underset{\pi'}{\longrightarrow} & G & \longrightarrow & 1 \end{array}$$

ambas sucesiones son exactas por definición y tanto id_A como id_G son isomorfismos.

Ahora, supongamos que existe φ un morfismo que hace conmutar el diagrama. Queremos ver que las sucesiones son equivalentes, es decir, que existen

conjuntos factor f y f', asociados respectivamente a dichas sucesiones, de tal manera que $f - f' \in B^2(G, A)$. Si $\lambda : G \longrightarrow E$ es un levantamiento que determina al conjunto factor f y $\lambda' : G \longrightarrow E'$, a su vez, determina un conjunto factor f' entonces, por la conmutatividad del primer cuadrado, para $f(x, y) \in A$:

$$f(x, y) = \varphi(f(x, y)) \text{ para todo } x, y \in G \quad (*)$$

Por otro lado, obsérvese que $\varphi\lambda(1) = \varphi(0) = 0$ y para toda $x \in G$ $\pi'\varphi(\lambda x) = x = id_G(x)$, por lo cual $\varphi\lambda : G \longrightarrow E'$ es un levantamiento; al aplicar φ a la ecuación que define al conjunto factor: $\lambda x + \lambda y = f(x, y) + \lambda xy$ y considerando $(*)$ obtenemos:

$$\varphi\lambda x + \varphi\lambda y = f(x, y) + \varphi\lambda xy$$

por lo que el levantamiento $\varphi\lambda : G \longrightarrow E'$ también define al conjunto factor f, lo que significa que f es un conjunto factor asociado a la extensión

$$0 \longrightarrow A \xrightarrow{i'} E' \xrightarrow{\pi'} G \longrightarrow 1$$

y como f' es otro conjunto factor asociado a la misma extensión, el Teorema 2.2.2 asegura que $f - f' \in B^2(G, A)$, esto es, las extensiones son equivalentes.

■

Corolario 2.2.10 *Si $e(G, A) = 0$ entonces toda extensión*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

se escinde y E es un producto semidirecto.

Demostración. Por definición $e(G, A) = Z^2(G, A)/B^2(G, A)$, si $e(G, A) = 0$ entonces todos los conjuntos factor son, en particular, equivalentes al conjunto factor asociado al producto semidirecto de A por G. Por el Teorema anterior la extensión dada es equivalente a la extensión:

$$0 \longrightarrow A \longrightarrow A \times G \longrightarrow G \longrightarrow 1$$

Por último, sabemos que cuando E es un producto semidirecto la extensión se escinde. ■

2.3. Automorfismos que estabilizan una extensión

En la relación de equivalencia entre extensiones, definida en la sección anterior, la condición que φ sea un isomorfismo es necesaria mas no suficiente. Es esencial pedir la conmutatividad del diagrama tal como lo ilustra el siguiente ejemplo.

Sean p un primo impar, A un grupo cíclico de orden p generado por a y E un grupo cíclico de orden p^2 generado por x, definimos $i : A \longrightarrow E$ como $i(a) = px$, $i' : A \longrightarrow E$ como $i'(a) = 2px$ entonces se tiene el diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & E/i(A) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & A & \xrightarrow[i']{} & E & \xrightarrow[\pi]{} & E/i'(A) & \longrightarrow & 0 \end{array}$$

Nótese que $i(A) = i'(A)$ por lo cual podemos usar el mismo morfismo π en ambas extensiones. Supongamos que $\varphi : E \longrightarrow E$ es un automorfismo. La conmutatividad del primer cuadrado diría que $\varphi(x) = 2x$ y la conmutatividad del segundo cuadrado dice que $\pi(x) = \pi\varphi(x)$, es decir $x + Im(\ i) = 2x + Im(\ i)$, es decir, $x = i(na)$ para algún $na \in A$ con $n < p$, esto implica que el orden de E es menor que p^2 lo cual es una contradicción.

El ejemplo ilustra también que, en general, no podemos garantizar que todo automorfismo de E haga conmutar el diagrama; la pregunta que surge entonces es: ¿qué debe cumplir un automorfismo φ para garantizar que el diagrama conmuta?. Los siguientes resultados nos aclaran la situación.

Definición 2.3.1 *Un automorfismo $\varphi : E \longrightarrow E$ estabiliza una extensión $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ si el siguiente diagrama conmuta:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id_G} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

El conjunto de automorfismos de E que estabilizan una extensión dada, al que denotamos por $St(G, A)$, es un subgrupo de $Aut(E)$ donde la operación binaria es la composición.

Lema 2.3.2 *Sea* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *una extensión.*
Si $\lambda : G \longrightarrow E$ *es un levantamiento, entonces, todo morfismo* $\varphi : E \longrightarrow E$ *que estabiliza a la extensión es de la forma:*

$$\varphi(a + \lambda x) = a + d(x) + \lambda x$$

donde $d(x) \in A$ *es independiente del levantamiento.*

Demostración. Si $\varphi : E \longrightarrow E$ es un morfismo que estabiliza la extensión, entonces hace conmutar el siguiente diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id_G} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

Primero obsérvese que dado que φ estabiliza, si $a \in A$, la comutatividad del primer cuadrado nos dice que $\varphi(a) = a$, también, por la conmutatividad del segundo cuadrado, $\pi\varphi = \pi$. Si $\lambda : G \longrightarrow E$ es un levantamiento, sabemos que todo elemento de E tiene una expresión única de la forma $a+\lambda x$, donde $a \in A$ y $x \in G$; $\varphi(\lambda x) \in E$, por tanto, existe $\bar{a} \in A$ y $y \in G$ tales que $\varphi(\lambda x) = \bar{a}+\lambda y$; nuestro interés es determinar quienes son $\bar{a}$ y λy. Nótese que, por la unicidad de la expresión, $\bar{a}$ está determinado de manera única por x, en otras palabras, tenemos una función $d : G \longrightarrow A$, dada por $d(x) = \bar{a}$, así, para cada $x \in G$, $\varphi(\lambda x) = d(x) + \lambda y$ donde $d(x)$ está determinado unívocamente. Por último veamos qué se puede decir de y. Si $x \in G$, tenemos que:

$$x = \pi(\lambda x) = \pi\varphi(\lambda x) = \pi(d(x) + \lambda y) = y$$

es decir, la expresión para $\varphi(\lambda x)$ sólo compromete a x, $\varphi(\lambda x) = d(x) + \lambda x$, por lo que, si $a + \lambda x \in E$, entonces:

$$\varphi(a + \lambda x) = \varphi(a) + \varphi(\lambda x) = a + d(x) + \lambda x$$

Finalmente, sea $\lambda' : G \longrightarrow E$ otro levantamiento tal que $\varphi(\lambda' x) = d'(x) + \lambda' x$ para algún $d'(x) \in A$, entonces, como $\lambda' x \in E$, éste se escribe de manera única como $\lambda' x = a' + \lambda x$, donde λ es el primer levantamiento que tomamos; de la expresión $\varphi(\lambda' x) = d'(x) + \lambda' x$ se sigue:

$$\begin{aligned} d'(x) &= \varphi(\lambda' x) - \lambda' x \\ &= \varphi(a' + \lambda x) - \lambda' x \\ &= a' + d(x) + \lambda x - \lambda' x \\ &= d(x) + a' + \lambda x - \lambda' x \end{aligned}$$

sabemos que $\lambda' x = a' + \lambda x$ por lo que $a' + \lambda x - \lambda' x = 0$, así, $d'(x) = d(x)$, es decir, $d(x)$ es independiente del levantamiento. ■

Podemos ir más allá al caracterizar los morfismos que estabilizan una extensión. En el resultado anterior obtuvimos una función $d : G \longrightarrow A$ al determinar la expresión para φ y es de esperarse que la relación que guarda φ con dicha función sea más profunda.

Corolario 2.3.3 *Sea* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *una extensión. La función* $\varphi : E \longrightarrow E$ *dado por* $\varphi(a+\lambda x) = a+d(x)+\lambda x$ *es un morfismo que estabiliza la extensión si y sólo si, para todo* $x, y \in G$*, la función* $d : G \longrightarrow A$ *satisface:*

$$d(xy) = d(x) + xd(y)$$

Demostración. Supongamos que $\varphi(a + \lambda x) = a + d(x) + \lambda x$. Sabemos que existe un conjunto factor $f : G \times G \longrightarrow A$ tal que $\lambda x + \lambda y = f(x, y) + \lambda xy$. Así, por un lado tenemos:

$$\begin{aligned}
\varphi(\lambda x + \lambda y) &= \varphi(\lambda x) + \varphi(\lambda y) \\
&= d(x) + \lambda x + d(y) + \lambda y \\
&= d(x) + \lambda x + d(y) - \lambda x + \lambda x + \lambda y \\
&= d(x) + xd(y) + \lambda x + \lambda y \\
&= d(x) + xd(y) + f(x, y) + \lambda xy
\end{aligned}$$

Por otro lado:

$$\begin{aligned}
\varphi(\lambda x + \lambda y) &= \varphi(f(x, y) + \lambda xy) \\
&= f(x, y) + d(xy) + \lambda xy
\end{aligned}$$

Entonces, $f(x, y) + d(xy) + \lambda xy = d(x) + xd(y) + f(x, y) + \lambda xy$, al cancelar $\lambda(xy)$, los términos restantes están en A el cual es abeliano, así, al conmutar y cancelar $f(x, y)$ tenemos:

$$d(xy) = d(x) + xd(y)$$

Recíprocamente, sea $\varphi(a + \lambda x) = a + d(x) + \lambda x$, donde $d(x)$ satisface la igualdad anterior, notemos que $d(1) = d(1 * 1) = d(1) + 1d(1)$, por lo que

$d(1) = 0$; el siguiente cálculo muestra que φ es morfismo:

$$\begin{aligned}
\varphi(a + \lambda x + a' + \lambda y) &= \varphi(a + xa' + f(x,y) + \lambda xy) \\
&= a + xa' + f(x,y) + d(xy) + \lambda xy \\
&= a + xa' + f(x,y) + d(x) + xd(y) + \lambda xy \\
&= a + xa' + d(x) + xd(y) + f(x,y) + \lambda xy \\
&= a + xa' + xd(y) + d(x) + \lambda x + \lambda y \\
&= a + d(x) + x(a' + d(y)) + \lambda x + \lambda y \\
&= a + d(x) + \lambda x + a' + d(y) - \lambda x + \lambda x + \lambda y \\
&= a + d(x) + \lambda x + a' + d(y) + \lambda y \\
&= \varphi(a + \lambda x) + \lambda(a' + \lambda y)
\end{aligned}$$

Por otro lado, tenemos los siguientes cuadrados:

$$\begin{array}{ccc}
a & \overset{i}{\longmapsto} & a + \lambda 1 \\
{\scriptstyle id_A}\downarrow & & \downarrow{\scriptstyle \varphi} \\
a & \overset{i}{\longmapsto} & a + d(1) + \lambda 1
\end{array}
\qquad
\begin{array}{ccc}
a + \lambda x & \overset{\pi}{\longmapsto} & x \\
{\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle id_G} \\
a + d(x) + \lambda x & \underset{\pi}{\longmapsto} & x
\end{array}$$

en otras palabras, φ hace conmutar el diagrama:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \overset{i}{\longrightarrow} & E & \overset{\pi}{\longrightarrow} & G & \longrightarrow & 1 \\
 & & {\scriptstyle id_A}\downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id_G} & & \\
0 & \longrightarrow & A & \underset{i}{\longrightarrow} & E & \underset{\pi}{\longrightarrow} & G & \longrightarrow & 1
\end{array}$$

por lo tanto es un automorfismo que estabiliza la extensión. ■

Con esto hemos dado respuesta a la pregunta que inició esta sección, la importancia de las funciones $d : G \longrightarrow A$ que surgieron al caracterizar los morfismo que estabilizan es tal que se les da un nombre especial.

Definición 2.3.4 *Una derivación (u homomorfismo cruzado) es una función $d : G \longrightarrow A$ que cumple $d(xy) = xd(y) + d(x)$.*

El conjunto de las derivaciones, $Der(A, G)$, es un grupo abeliano bajo la adición puntual. Si A es un G-módulo trivial, entonces $Der(A, G) = \mathrm{Hom}(A, G)$

pues en este caso $d(xy) = d(y) + d(x)$. Lo que hemos visto entonces es que cada automorfismo $\varphi : E \longrightarrow E$ que estabiliza una extensión determina una derivación $d : G \longrightarrow A$ y recíprocamente, dada una derivación $d : G \longrightarrow A$ y una extensión $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$, ésto determina determina un automorfismo que estabiliza la extensión.

Teorema 2.3.5 *Sea* $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ *una extensión. La función*

$$\begin{aligned} \sigma : St(G, A) &\longrightarrow Der(G, A) \\ \varphi &\longmapsto d \end{aligned}$$

donde $\varphi(a + \lambda x) = a + d(x) + \lambda x$*, es un isomorfismo.*

Demostración. Los lemas anteriores dicen que si φ es un automorfismo que estabiliza, entonces $\varphi(a + \lambda x) = a + d(x) + \lambda x$, donde d es una derivación que no depende del levantamiento que consideremos por lo que σ está bien definida, ahora, sean $\varphi, \varphi' \in St(G, A)$, denotemos: $\sigma(\varphi' \circ \varphi) = \bar{d}$, $\sigma(\varphi) = d$ y $\sigma(\varphi') = d'$, de la definición de φ y φ' tenemos:

$$\begin{gathered} \bar{d}(x) = -a + (\varphi' \circ \varphi)(a + \lambda x) - \lambda x = -a + \varphi'(a + d(x) + \lambda x) - \lambda x = \\ -a + a + d(x) + d'(x) + \lambda x - \lambda x = d(x) + d'(x) \end{gathered}$$

para todo x en G, por tanto, σ es morfismo.
Damos ahora el inverso de σ. Si $d \in Der(G, A)$ definimos $\varphi : E \longrightarrow E$ como $\varphi(a + \lambda x) = a + d(x) + \lambda x$. Por el corolario 2.3.3 φ es un automorfismo que estabiliza la extensión, y así la asignación $\gamma : d \mapsto \varphi$ claramente es inversa de σ. ■

De este resultado se desprende que $St(G, A)$ es abeliano pues es isomorfo a $Der(G, A)$ el cual es abeliano.

Definición 2.3.6 *Una derivación principal es una función* $d_0 : G \longrightarrow A$ *dada por* $d_0(x) = xa_0 - a_0$*, para algún* $a_0 \in A$*. Denotamos al conjunto de las derivaciones principales como* $PDer(G, A)$

Nótese que $PDer(G, A)$ es un subgrupo de $Der(G, A)$ pues si d_0 es una derivación principal, entonces:

$$\begin{aligned} xd_0(y) + d_0(x) &= x(ya_0 - a_0) + xa_0 - a_0 \\ &= xya_0 - xa_0 + xa_0 - a_0 \\ &= xya_0 - a_0 \\ &= d_0(xy) \end{aligned}$$

Definición 2.3.7 *Un automorfismo φ de E se llama automorfismo interior si es la conjugación por algún elemento de E, es decir, $\varphi(x) = a_0 + x - a_0$ para algún $a_0 \in E$.*

Con esto en mente, podemos caracterizar a aquellos automorfismos que estabilizan una extensión y que tienen la particularidad de que están dados por una derivación principal

Lema 2.3.8 *Sea $0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$ una extensión y tomemos $\lambda : G \longrightarrow A$ un levantamiento.*
$\varphi : E \longrightarrow E$ es un automorfismo interior que estabiliza a la extensión si y sólo si en la definición de φ:

$$\varphi(a + \lambda x) = a + d(x) + \lambda x$$

se tiene que d es una derivación principal, es decir, $d(x) = xa_0 - a_0$ para algún $a_0 \in A$.

Demostración. Si $\varphi : E \longrightarrow E$ es un automorfismo interior que estabiliza la extención entonces, por el Lema 2.3.2, es de la forma $\varphi(a+\lambda x) = a+d(x)+\lambda x$ y,por otro lado, el hecho de que sea interior nos dice que $\varphi(a + \lambda x) = a_0 + a + \lambda x - a_0$, para algún $a_0 \in A$. Pero obsérvese que:

$$a_0 + a + \lambda x - a_0 = a_0 + a + \lambda x - a_0 - \lambda x + \lambda x = a_0 + a - xa_0 + \lambda x$$

de lo cual tenemos:

$$a + d(x) + \lambda x = a_0 + a - xa_0 + \lambda x$$

y por lo tanto, al cancelar a y λx obtenemos $d(x) = a_0 - xa_0$. Recíprocamente, si $\varphi(a+\lambda x) = a+xa_0-a_0+\lambda x$ entonces, para cada x hacemos $d(x) = xa_0-a_0$ lo cual es una derivación principal, con esto φ toma la forma: $\varphi(a + \lambda x) = a + d(x) + \lambda x$ y por el Corolario 2.3.3 φ es un automorfismo que estabiliza; por último, φ es la conjugación por $-a_0$ pues:

$$\begin{aligned} -a_0 + (a + \lambda x) + a_0 &= -a_0 + a + \lambda x + a_0 - \lambda x + \lambda x \\ &= -a_0 + a + xa_0 + \lambda x \\ &= a + xa_0 - a_0 + \lambda x \\ &= \varphi(a + \lambda x) \end{aligned}$$

lo cual quiere decir que φ es un automorfismo interior. ■

Denotemos como $Inn(G, A)$ al conjunto de automorfismos interiores que estabilizan. Es claro que $Inn(G, A)$ es un subgrupo de $St(G, A)$. Recordando que $St(G, A)$ es abeliano tiene sentido tomar el cociente.

Definición 2.3.9 $Stab(G, A) = St(G, A)/Inn(G, A)$.

Teorema 2.3.10 $Stab(G, A) \cong Der(G, A)/PDer(G, A)$.

Demostración. Basta probar que $\sigma(Inn(G, A)) = PDer(G, A)$ donde σ es el isomorfismo del Teorema 2.3.5. Si $\varphi \in Inn(G, A)$, por el lema anterior, $\varphi(a + \lambda x) = a + xa_0 - a_0 + \lambda x$, luego $\sigma(\varphi) = d$ con $d(x) = xa_0 - a_0$, es decir, $\sigma(\varphi)$ es una derivación principal lo cual muestra que $\sigma(\varphi) \in PDer(G, A)$. Por otro lado, si $d_0 \in PDer(A, G)$, tomando $\varphi_0 : E \longrightarrow E$ definido por $\varphi_0(a + \lambda x) = a + d_0(x) + \lambda x$, nuevamente, por el lema anterior sabemos que $\varphi_0 \in Inn(G, A)$ y $d_0 = \sigma(\varphi_0)$. ■

Teorema 2.3.11 *Sea E un producto semidirecto de A por G y sean C, C' complementos de A en E. Si $Stab(G, A) = \{0\}$ entonces C y C' son conjugados.*

Demostración. Consideremos la extensión:

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

Dado que E es un producto semidirecto, por el Lema 2.1.9 existen levantamientos λ y λ' que además son homomorfismos tales que $Im(\lambda) = C$ y $Im(\lambda') = C'$. Sabemos que los conjuntos factor f y f' asociados a dichos levantamientos respectivamente, son identicamente cero, así, $f - f' = 0$; por el Teorema 2.2.2, existe $d : G \longrightarrow A$, dada por $d(x) = \lambda' x - \lambda x$, tal que

$$0 = f(x, y) - f'(x, y) = xd(y) - d(xy) + d(x) \text{ para todo } x, y \in G.$$

por lo que $d(xy) = xd(y) + d(x)$, es decir, d es una derivación. Por hipótesis $Stab(G, A) = \{0\}$ y por tanto, todas las derivaciones son principales por lo que existe $a_0 \in A$ tal que $d(x) = xa_0 - a_0$. Como $d(x) = \lambda' x - \lambda x$ tenemos $xa_0 - a_0 = \lambda x - \lambda' x$ y al despejar λx nos queda:

$$\lambda x = xa_0 - a_0 + \lambda' x = -a_0 + (\lambda' x + a_0 - \lambda' x) + \lambda' x = -a_0 + \lambda' x + a_0$$

o equivalentemente $\lambda' x = a_0 + \lambda x - a_0$. Como $Im(\lambda) = C$ y $Im(\lambda') = C'$ esto quiere decir que C' es la conjugación de C por a_0. ■

Finalizamos este capítulo dando una caracterización del grupo $Der(G, A)$. Notemos que si $\alpha : A \longrightarrow A'$ es un morfismo de G-módulos y $d : G \longrightarrow A$ es una derivación entonces, $\alpha d : G \longrightarrow A'$ es nuevamente una derivación pues $(\alpha d)(xy) = \alpha(d(xy)) = \alpha(xd(y) + d(x)) = x\alpha d(y) + \alpha d(x)$. Con esto, $Der(G, -) : {}_G\mathbf{Mod} \longrightarrow \boldsymbol{Ab}$ se convierte en un funtor, definido en objetos $A \in {}_G\mathbf{Mod}$ como $Der(G, A)$ y en morfismos $\alpha : A \longrightarrow A'$ como $Der(G, \alpha) = \alpha d$, donde $d : G \longrightarrow A$ es una derivación. Usaremos la notación $Der(G, \alpha) = \bar{\alpha}$.

La función $\psi : G \longrightarrow \mathbb{Z}$, $\psi(x) = 1$ para todo $x \in G$ induce, por la propiedad universal del anillo de grupo, un morfismo:

$$\begin{gathered} \varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z} \\ \sum m_x x \mapsto \sum m_x \end{gathered}$$

llamado morfismo de aumentación con $Ker(\varepsilon) = \mathcal{G}$ un ideal bilateral de $\mathbb{Z}G$ llamado ideal de aumentación.

Lema 2.3.12 *Como grupo abeliano, el ideal de aumentacion, $\mathcal{G} = Ker(\varepsilon)$, es libre con base $\{x - 1 \mid x \in G \text{ y } x \neq 1_G\}$.*

Demostración. Un elemento $a = \sum m_x x \in Ker(\varepsilon)$ si y sólo si $\sum m_x = 0$. Entonces:

$$a = a - 0 = a - (\sum m_x)1_G = \sum m_x x - (\sum m_x)1_G = \sum m_x(x - 1_G)$$

por lo que $Ker(\varepsilon)$ está generado por $\{x - 1 \mid x \in G \text{ y } x \neq 1_G\}$. Ahora suponga-mos que $\sum m_x(x - 1_G) = 0$ entonces:

$$0 = \sum m_x(x - 1_G) = \sum m_x x - (\sum m_x)1_G$$

esto es una combinación de elementos de G pero, como grupo abeliano, $\mathbb{Z}G$ es libre con base G, por lo que cada $m_x = 0$. ■

Teorema 2.3.13 *Los morfismos $t_A : \mathrm{Hom}_G(\mathcal{G}, A) \longrightarrow Der(G, A)$, definidos por $t_A(f) = d$ donde $d(x) = f(x - 1)$, constituyen una equivalencia natural de funtores.*

Demostración. Primero nótese que si $f \in \mathrm{Hom}_G(\mathcal{G}, A)$ entonces $t_A(f) = d$ es una derivación pues:

$$d(xy) = f(xy-1) = f(xy) + f(-1) = f(xy - x + x - 1) = \\ f(xy-x) + f(x-1) = xf(y-1) + f(x-1) = xd(y) + d(x)$$

Sean $f, f' \in \mathrm{Hom}_G(\mathcal{G}, A)$, haciendo $t_A(f + f') = \bar{d}$, $t_A(f) = d$ y $t_A(f') = d'$, tenemos:

$\bar{d}(x) = (f + f')(x-1) = f(x-1) + f'(x-1) = d(x) + d'(x)$ para todo $x \in G$

por tanto t_A es morfismo.

Ahora construimos la inversa de t_A. Sea $d \in Der(G, A)$ definimos

$$f : \mathcal{G} \longrightarrow A \\ f(x-1) = d(x)$$

estamos definiendo a f sobre los elementos de la base de $\mathcal{G}$ por lo cual está bien definido y es un morfismo de G-módulos pues nótese que, si $z \in G$, podemos escribir $z(x-1) = zx - z = zx - 1 + 1 - z = (zx-1) - (z-1)$ por lo que:

$$\begin{aligned} f(z(x-1)) &= f((zx-1) - (z-1)) \\ &= f(zx-1) - f(z-1) \\ &= d(zx) - d(x) \end{aligned}$$

y aplicando la igualdad $d(zx) = zd(x) + d(x)$ tenemos:

$$d(zx) - d(x) = zd(x) + d(x) - d(x) = zd(x) = z(f(x-1))$$

definiendo $s_A : Der(G, A) \longrightarrow \mathrm{Hom}(\mathcal{G}, A)$ por $s_A(d) = f$ donde $f(x-1) = d(x)$ hemos dado la inversa de t_A. Por último debemos ver que si $\alpha : A \longrightarrow B$ es un morfismo de G-módulos entonces el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathrm{Hom}_G(\mathcal{G}, A) & \xrightarrow{t_A} & Der(G, A) \\ \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \bar{\alpha}} \\ \mathrm{Hom}_G(\mathcal{G}, B) & \xrightarrow[t_B]{} & Der(G, B) \end{array}$$

donde $\alpha_*(f) = \alpha f$ y $\bar{\alpha}(d) = \alpha d$. Sea $f \in \mathrm{Hom}_G(\mathcal{G}, A)$, por un lado tenemos:

$$t_B(\alpha_*(f)) = t_B(\alpha f) = \bar{d} \text{ con } \bar{d} \in Der(G, B)$$

donde $\bar{d}$, la derivación asociada al morfismo αf, esta definida como:

$$\bar{d}(x) = (\alpha f)(x-1) = \alpha(f(x-1)) \text{ para todo } x \in G$$

por otro lado:

$$(\bar{\alpha} t_A)(f) = \bar{\alpha}(t_A(f)) = \bar{\alpha}(d) = \alpha d$$

sabemos que αd es nuevamente una derivación donde d, la derivación asociada al morfismo f via t_A, está definida como $d(x) = f(x-1)$ para todo $x \in G$ por lo que $\alpha d(x) = \alpha(f(x-1)) = \bar{d}(x)$, esto muestra que $t_B \alpha_* = \bar{\alpha} t_A$. ■

Capítulo 3

Grupos de Cohomología

3.1. Definición de cohomología

Nuestro objetivo aquí es describir los grupos de cohomología en términos de los grupos obtenidos en el capítulo anterior. Con esto daremos una interpretación de los grupos de cohomología de dimensiones bajas y así se hará más tangible la definición de dichos grupos. Sean F_0 el G-módulo libre generado por un conjunto con un único elemento al que denotamos como $[\,]$ y, para $n \geq 1$, F_n el G-módulo libre con base G^n el producto cartesiano de n copias de G, denotemos a los elementos de la base G^n como $[x_1, x_2, \ldots, x_n]$ y considerese la siguiente sucesión:

$$F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \quad (1)$$

donde:

$$\begin{aligned} d_3[x,y,z] &= x[y,z] - [xy,z] + [x,yz] - [x,y] \\ d_2[x,y] &= x[y] - [xy] + [x] \\ d_1[x] &= x[\,] - [\,] \end{aligned}$$

Obsérvese que $F_0 \cong \mathbb{Z}G$. Sabemos que dado un R-módulo libre F con base X y una función $f : X \longrightarrow A$, con A un R-módulo, podemos extender f a un único morfismo $\bar{f} : F \longrightarrow A$. Cada d_i está definido sobre elementos de la

base de F_i por lo que puede extenderse a un morfismo de G-módulos. Ahora, compárese ésto con las fórmulas que obtuvimos en el capítulo anterior:

Conjuntos factor :	$xf(x,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$
Cofronteras :	$xh(y) - h(xy) + h(x) = f(x,y)$
Derivaciones :	$xd(y) - d(xy) + d(x) = 0$
Derivaciones principales :	$xa_0 - a_0 = d(x)$

Se hace evidente la semejanza entre las funciones de esta lista y los morfismos d_i de la sucesión anterior. Nótese que, por ejemplo, los conjuntos factor son funciones de $G \times G$ en A y el morfismo d_3 van de F_3 en F_2, considerando esto, si aplicamos el funtor contravariante $\mathrm{Hom}_G(-, A)$ a la sucesión (1), donde A es un G-módulo, esto nos induce otra sucesión:

$$\mathrm{Hom}_G(F_3, A) \xleftarrow{d_3^*} \mathrm{Hom}_G(F_2, A) \xleftarrow{d_2^*} \mathrm{Hom}_G(F_1, A) \xleftarrow{d_1^*} \mathrm{Hom}_G(F_0, A)$$

Ahora, para ilustrar la situación, identifiquemos los elementos de $Ker({d_3}^*)$. Sea $f \in \mathrm{Hom}_G(F_2, A)$; $f \in Ker({d_3}^*)$ si y sólo si $d_3^*(f) = 0$, es decir, $f \in Ker({d_3}^*)$ si y sólo si $fd_3 = d_3^*(\alpha) = 0$, esto es:

$$0 = fd_3[x,y,z] = f(x[y,z] - [xy,z] + [x,yz] - [x,y]) = \\ xf[y,z] - f[xy,z] + f[x,yz] - f[x,y]$$

Identifiquemos los elementos de $Im(d_2^*)$. Sea $g \in Im(d_2^*)$, $g : F_2 \longrightarrow A$, entonces existe $h \in \mathrm{Hom}_G(F_1, A)$ tal que $d_2^*(h) = hd_2 = g$, esto es, existe h tal que:

$$g[x,y] = hd_2[x,y] = h(x[y] - [xy] + [x]) = xh[y] - h[xy] + h[x]$$

Recordando la definición de $e(G, A)$ estamos tentados a pensar que es isomorfo a $Ker({d_3}^*)/Im(d_2^*)$ (por su parte, este cociente nos debe recordar la definición de Ext^n). En resumen, la idea aquí expuesta es que, para dar una descripción de los grupos de cohomología en términos de los grupos del capítulo anterior, debemos construir una resolución libre de $\mathbb{Z}$ a la cual le aplicamos el funtor $\mathrm{Hom}_G(-, A)$ para así obtener la lista anterior de fórmulas. Así, planteamos el primer resultado de este capítulo, si recordamos el morfismo de aumentación $\varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$ entonces, la primera sucesión que dimos queda:

$$F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z}$$

donde $\varepsilon[\,] = 1$.

Lema 3.1.1 *En la sucesión de G-módulos*

$$F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z}\ ,$$

se tiene que $Im(d_2) \subseteq Ker(d_1)$ *y* $Im(d_3) \subseteq Ker(d_2)$ *donde cada* d_i $(i = 1, 2, 3)$ *y* ε *están definidos en la base de* F_i *por:*

$$\begin{aligned} d_3[x, y, z] &= x[y, z] - [xy, z] + [x, yz] - [x, y], \\ d_2[x, y] &= x[y] - [xy] + [x], \\ d_1[x] &= x[\,] - [\,], \\ \varepsilon[\,] &= 1. \end{aligned}$$

(Tal sucesión es el inicio de una resolución G-libre de $\mathbb{Z}$ *al que consideramos como G-módulo trivial)*

Demostración. Más adelante (Proposición 3.4.4) se completará esta resolución de $\mathbb{Z}$ y se probará su exactitud. Si $d_2[x, y] \in Im(d_2)$ entonces al aplicar d_1 resulta:

$$\begin{aligned} d_1 d_2[x, y] = d_1(x[y] - [xy] - [x]) = x d_1[y] - d_1[xy] + d_1[x] = \\ x(y - 1) - (xy - 1) + (x - 1) = 0 \end{aligned}$$

Ésto prueba que $Im(d_2) \subseteq Ker(d_1)$. Ahora, si $d_3[x, y, z] \in Im(d_3)$, aplicandole d_2 nos da:

$$\begin{aligned} d_2 d_3[x, y, z] &= d_2(x[y, z] - [xy, z] + [x, yz] - [x, y]) \\ &= x d_2[y, z] - d_2[xy, z] + d_2[x, yz] - d_2[x, y] \\ &= x(y[z] - [yz] + [z]) - (xy[z] - [xyz] + [z]) \\ &\quad + x[yz] - [xyz] + [yz] - (x[y] - [xy] + [x]) \\ &= xy[z] - x[yz] + x[z] - xy[z] + [xyz] - [z] \\ &\quad + x[yz] - [xyz] + [yz] - x[y] + [xy] - [x] \\ &= 0 \end{aligned}$$

lo cual muestra que $Im(d_3) \subseteq Ker(d_2)$.

■

3.2. $H^0(G, A)$

La discusión de la sección anterior sugiere de manera natural la siguiente definición.

Definición 3.2.1 *Sean G un grupo y A un G-módulo. Definimos el n-ésimo grupo de cohomología de G con coeficientes en A como:*

$$H^n(G, A) = Ext^n_{\mathbb{Z}G}(\mathbb{Z}, A)$$

donde $\mathbb{Z}$ es considerado como un G-módulo trivial.

Nuestro deseo es identificar los grupos de cohomología, $H^n(G, A)$, en relación con lo hecho en el capítulo anterior. Empezaremos por identificar al grupo $H^0(G, A)$ que por definición es $H^0(G, A) = Ext^0{}_{\mathbb{Z}G}(\mathbb{Z}, A)$. Por el Teorema 1.5.8, sabemos que $Ext^0{}_{\mathbb{Z}G}(\mathbb{Z}, A) \cong \mathrm{Hom}_G(\mathbb{Z}, A)$; considérese el submódulo de puntos fijos de A bajo la acción de G:

$$A^G = \{a \in A \mid xa = a \ \forall x \in G\}$$

si $f : A \longrightarrow B$ es un morfismo de G-módulos y $a \in A^G$ entonces $f(a) = f(xa) = xf(a)$, es decir, $f(a) \in B^G$ con lo cual tenemos un funtor:

Definición 3.2.2 *$Fix^G(-) :\ {}_G\mathbf{Mod} \longrightarrow {}_G\mathbf{Mod}$ es un funtor llamado funtor de puntos fijos, definido en objetos A en ${}_G\mathbf{Mod}$ como $Fix^G(A) = A^G$ y en morfismos $f : A \longrightarrow B$ como $Fix^G(f) = f\mid_{A^G}$*

Ahora estamos en posibilidades de identificar a $H^0(G, A)$. Necesitaremos el siguiente lema técnico. Sabemos que en general, para un anillo R cualquiera, $\mathrm{Hom}_R(A, B)$ no siempre es un módulo pero cuando $R = \mathbb{Z}G$ la situación cambia pues $\mathrm{Hom}_G(A, B)$ adquiere estructura de G-módulo.

Lema 3.2.3 *Sean G un grupo y A, B G-módulos.* $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ *se convierte en G-módulo definiendo la acción de un elemento $g \in G$ sobre $\varphi \in$* $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ *como:*

$$(g \cdot \varphi)(a) = g\varphi(g^{-1}a)$$

Más aún, $Fix^G(\mathrm{Hom}_{\mathbb{Z}}(A, B)) = \mathrm{Hom}_G(A, B)$.

Demostración. Primero notemos que $g \cdot \varphi \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$ pues si $a, b \in A$ y si $\alpha \in \mathbb{Z}$:

$$(g \cdot \varphi)(a+b) = g\varphi(g^{-1}(a+b)) = g\varphi(g^{-1}a) + g\varphi(g^{-1}b) = (g \cdot \varphi)(a) + (g \cdot \varphi)(b)$$

y

$$(g \cdot \varphi)(\alpha a) = g\varphi(g^{-1}(\alpha a)) = g\varphi(\alpha(g^{-1}a)) = g\alpha\varphi(g^{-1}a) = \alpha g\varphi(g^{-1}a) = \alpha(g \cdot \varphi)(a)$$

Por otro lado, si $g, g' \in G$ veamos que $g \cdot (g' \cdot \varphi) = (gg') \cdot \varphi$. Sea $a \in A$:

$$((gg') \cdot \varphi)(a) = gg'\varphi((gg')^{-1}a) = gg'\varphi(g'^{-1}g^{-1}a)$$

usando que $g' \cdot \varphi \in \mathrm{Hom}_G(A, B)$, al calcular $(g \cdot (g' \cdot \varphi))(a)$ tenemos:

$$(g \cdot (g' \cdot \varphi))(a) = g[(g' \cdot \varphi)(g^{-1}a)] = g[g'\varphi(g'^{-1}g^{-1}a)] = gg'\varphi(g'^{-1}g^{-1}a)$$

por último, es evidente que $g(\varphi + \varphi') = g\varphi + g\varphi'$.

Para mostrar que $Fix^G(\mathrm{Hom}_{\mathbb{Z}}(A, B)) = \mathrm{Hom}_G(A, B)$ debemos probar que $f \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$ es un morfismo de G-módulos si y sólo si, para todo $g \in G$, $g \cdot f = f$. Sean $f \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$, $a \in A$ y $g \in G$. Supongamos que f es un morfismo de G-módulos entonces, $(g \cdot f)(a) = gf(g^{-1}a) = f(gg^{-1}a) = f(a)$. Inversamente, supongamos que $f \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$ es tal que $g \cdot f = f$ entonces, $gf(a) = gf(g^{-1}ga)$, con fines de claridad hagamos $b = ga$, lo anterior queda como $gf(g^{-1}b) = (g \cdot f)(b) = f(b) = f(ga)$, por lo tanto, $gf(a) = f(ga)$. ■

Teorema 3.2.4 *Si $\mathbb{Z}$ es considerado como un G-módulo trivial entonces los morfismos:*

$$\begin{aligned} \tau_A : \mathrm{Hom}_G(\mathbb{Z}, A) &\longrightarrow A^G \\ f &\mapsto f(1) \end{aligned}$$

constituyen una equivalencia natural de funtores:

$$\mathrm{Hom}_G(\mathbb{Z}, -) \cong Fix^G(-)$$

Demostración. Probaremos que cada τ_A es un isomorfismo; $\mathbb{Z}$ es un G-módulo trivial por lo que $x1 = 1$ para todo $x \in G$. Si $f \in \mathrm{Hom}_G(\mathbb{Z}, A)$ sabemos que f está determinado por el valor que toma en 1, al aplicar f a la igualdad anterior tenemos: $f(1) = f(x1) = xf(1)$, es decir $f(1) \in A^G$. Ahora, si f es tal que $\tau_A(f) = f(1) = 0$ entonces f no tiene otra opción que ser el morfismo cero, es decir, τ_A es inyectiva. Si $a \in A^G$, entonces $xa = a$ para todo $x \in G$; definimos $f_a : \mathbb{Z} \longrightarrow A$ como $f_a(1) = a$, con esto f_a es tal

que $\tau_A(f_a) = f_a(1) = a$ por lo tanto τ_A es sobreyectiva. Si $f, f' \in \mathrm{Hom}_G(\mathbb{Z}, A)$ entonces por un lado $\tau_A(f+f') = (f+f')(1) = f(1)+f'(1) = \tau_A(f)+\tau_A(f')$, por otro lado si $g \in G$, $\tau_A(g \cdot f) = (g \cdot f)(1) = gf(g^{-1}1) = gf(1) = g(\tau_A(f))$, por lo cual cada τ_A es un morfismo de G-módulos. Por último, si $f : A \longrightarrow B$ es un morfismo de G-módulos, debemos comprobar que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathrm{Hom}_G(\mathbb{Z}, A) & \xrightarrow{f_*} & \mathrm{Hom}_G(\mathbb{Z}, B) \\ \downarrow{\scriptstyle \tau_A} & & \downarrow{\scriptstyle \tau_B} \\ A^G & \xrightarrow[Fix(f)]{} & B^G \end{array}$$

Sea $g \in \mathrm{Hom}_G(\mathbb{Z}, A)$, hacemos los cálculos:

$$\tau_B f_*(g) = \tau_B(f \circ g) = (f \circ g)(1) = f(g(1))$$

por otro lado, recordando que $Fix(f) = f \mid_{A^G}$,

$$(f \mid_{A^G}) \tau_A(g) = (f \mid_{A^G}) (g(1))$$

pero, como ya vimos, $g(1) \in A^G$, por lo que $f \mid_{A^G} (g(1)) = f(g(1))$, esto es: $\tau_B \circ f_* = Fix(f) \circ \tau_A$. Por lo tanto:

$$\mathrm{Hom}_G(\mathbb{Z}, -) \cong Fix^G(-)$$

■

Este resultado indica que $H^0(G, A) = \mathrm{Hom}(\mathbb{Z}, A) = A^G$.

3.3. $H^1(G, A)$

Toca ahora el turno de identificar $H^1(G, A)$. Regresemos a la sucesión inducida al aplicar $\mathrm{Hom}_G(-, A)$ a la sucesión del Lema 3.1.1:

$$\mathrm{Hom}_G(F_3, A) \xleftarrow{d_3^*} \mathrm{Hom}_G(F_2, A) \xleftarrow{d_2^*} \mathrm{Hom}_G(F_1, A) \xleftarrow{d_1^*} \mathrm{Hom}_G(F_0, A)$$

Por definición $H^1(G, A) = Ker(d_2^*/Im(d_1^*)$; sabemos que basta conocer el efecto de un morfismo de G-módulos $f \in \mathrm{Hom}_G(F_n, A)$ sobre la base G^n, por lo cual, para los morfismos $h \in \mathrm{Hom}_G(F_1, A)$, se cumple $h(x[y]) = xh[y]$

para todo $x, y \in G$. Al identificar los elementos de $Ker(d_2^*$ tenemos que $h \in Ker(d_2^*$ si y sólo si para todo $x, y \in G$:

$$\begin{aligned} 0 &= (d_2^* h)[x, y] \\ &= h d_2[x, y] \\ &= h(x[y] - [xy] + [x]) \\ &= xh[y] - h[xy] + h[x] \end{aligned}$$

de donde se sigue que $h[xy] = xh[y] + h[x]$, lo que significa que los elementos de $Ker(d_2^*)$ son derivaciones.

Proposición 3.3.1 $H^1(G, A) = Der(G, A)/PDer(G, A) = Stab(G, A)$.

Demostración. El cálculo que se hizo previo a esta proposición muestra que $Ker(d_2^* \subset Der(G, A)$. Si $d \in Der(G, A)$ entonces cumple $d[x, y] = xd[y]+d[x]$ para todo $x, y \in G$ de lo cual se sigue que $xd[y] - d[x, y] + d[x] = 0$ por lo que:

$$\begin{aligned} (d_2^* d)[x, y] &= d d_2[x, y] \\ &= d(x[y] - [xy] + [x]) \\ &= xd[y] - d[xy] + d[x] \\ &= 0 \end{aligned}$$

y de esto $d \in Ker(d_2^*$, por lo que $Ker(d_2^* = Der(G, A)$. Por último probaremos que $Im(d_1^*) = PDer(G, A)$. Dado $\alpha \in \mathrm{Hom}_G(F_0, A)$, $\alpha[\,] = a_0$ para algún $a_0 \in A$. Entonces:

$$(d_1^* \alpha)[x] = \alpha(d_1[x]) = \alpha(x[\,] - [\,]) = x\alpha[\,] - \alpha[\,] = xa_0 - a_0$$

y por tanto $d_1^* \alpha$ es una derivación principal, es decir, $Im(d_1^*) \subset PDer(G, A)$. Para la inclusión faltante sea $p : G \longrightarrow A$ una derivación principal. Entonces $p[x] = xb_0 - b_0$ para algún $b_0 \in A$. $\beta : F_0 \longrightarrow A$ definido por $\beta[\,] = b_0$ es tal que:

$$(d_1^* \beta)[x] = \beta d_1[x] = \beta(x[\,] - [\,]) = x\beta[\,] - \beta[\,]) = xb_0 - b_0 = p[x]$$

y así $p \in Im(d_1^*)$, por lo que $Im(d_1^*) = PDer(G, A)$. Por lo tanto $H^1(G, A) = Ker(d_2^*/Im(d_1^*) = Der(G, A)/PDer(G, A) = Stab(G, A)$. ■

3.4. $H^2(G, A)$

Ahora consideremos $H^2(G, A) = Ker(d_3^*/Im(d_2^*)$. Si $f \in Ker(d_3^*$ entonces $d_3^* f = f d_3 = 0$, así, para cualesquiera $x, y, z \in G$ tenemos:

$$\begin{aligned} 0 &= f d_3[x, y, z] \\ &= f(x[y, x] - [xy, z] + [x, yz] - [x, y]) \\ &= xf[y, x] - f[xy, z] + f[x, yz] - f[x, y] \end{aligned}$$

Ésta igualdad es una de las propiedades que caracterizan a los conjuntos factor (Teorema 2.1.12), así que f sería un conjuto factor si, además, cumpliera $f[x, 1] = 0 = f[1, x]$ pero esto no lo podemos asegurar. Con los elementos de $Im(d_2^*)$ ocurre una historia similar; si g es un elemento de $Im(d_2^*)$ entonces existe algún morfismo $h : F_1 \longrightarrow A$ tal que $g = Im(d_2^*(h)) = h d_2$ por lo que, para todo $x, y \in G$:

$$\begin{aligned} g[x, y] &= h d_2[x, y] \\ &= h(x[y] - [xy] + [x]) \\ &= xh[y] - h[xy] + h[x] \end{aligned}$$

siendo esta última igualdad es parte de la definición de cofrontera y para que lo sea, debe cumplir que $h[1] = 0$ y esto tampoco podemos asegurarlo.

Nuestro objetivo será demostrar que $H^2(G, A)$=$Z^2(G, A)/B^2(G, A)$=$e(G, A)$. La idea se apoya en el hecho de que los grupos de homología de un complejo de cadena no dependen de la resolución proyectiva que tomemos, así que construiremos una resolución proyectiva de $\mathbb{Z}$ de tal manera que nos permita garantizar las igualdades faltantes para los elementos de $Ker(d_3^*$ y $Im(d_2^*)$, empezaremos por completar la resolución del Lema 3.1.1.

Definición 3.4.1 *Sea G un grupo. La resolución de barra de $\mathbb{Z}$ es la sucesión:*

$$\mathbf{B}(G) : \cdots \longrightarrow B_3 \xrightarrow{d_3} B_2 \xrightarrow{d_2} B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

donde B_0 es el G-módulo libre generado por $\{[\,]\}$, $\varepsilon : B_0 \longrightarrow \mathbb{Z}$ es el morfismo de aumentación, B_n es el G-módulo libre con base $\{[x_1, x_2, \ldots, x_n] \mid x_i \in G\}$

y $d_n : B_n \longrightarrow B_{n-1}$ *está dado por:*

$$d_n[x_1, x_2, \ldots, x_n] = x_1[x_2, x_3, \ldots, x_n] + \sum_{i=1}^{n-1}(-1)^i[x_1, \ldots, x_i x_{i+1}, \ldots, x_n] + (-1)^n[x_1, \ldots, x_{n-1}]$$

Nótese que para $n = 1, 2, 3$, las fórmulas para d_n coinciden con aquellas del Lema 3.1.1:

$$\begin{aligned} d_1[x] &= x[\,] - [\,] \\ d_2[x,y] &= x[y] - [xy] + [x] \\ d_3[x,y,z] &= x[y,z] - [xy,z] + [x,yz] - [x,y] \end{aligned}$$

Debemos probar que $\mathbf{B}(G)$ es un complejo y para ello compararemos a $\mathbf{B}(G)$ con cierta resolución de $\mathbb{Z}$ en el sentido de que mostraremos una sucesión exacta que será isomorfa a $\mathbf{B}(G)$.

Definición 3.4.2 *Sea* G *un grupo. La resolución homogénea,* $\mathbf{P}(G)$*, de* $\mathbb{Z}$ *es:*

$$\mathbf{P}(G) : \cdots \longrightarrow P_3 \xrightarrow{\delta_3} P_2 \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

en donde P_n *es el grupo abeliano libre con base* $\{(x_0, x_1, \ldots, x_n) \mid x_i \in G\}$*, en particular,* P_0 *es el grupo abeliano libre con base* $\{(g) \mid g \in G\}$*. A dichos grupos les damos estructura de* G*-módulo definiendo la acción de* G *como:*

$$x(x_0, x_1, \ldots, x_n) = (xx_0, xx_1, \ldots, xx_n)$$

El morfismo $\varepsilon : P_0 \longrightarrow \mathbb{Z}$ *está dado por* $\sum_{g\in G} m_g(g) \mapsto \sum_{g\in G} m_g$*, definimos* $\delta_n : P_n \longrightarrow P_{n-1}$ *para* $n \geq 1$ *como:*

$$\delta_n(x_0, x_1, \ldots, x_n) = \textstyle\sum_{i=1}^{n}(-1)^i(x_0, \ldots, \hat{x_i}, \ldots, x_n)$$

donde $\hat{x_i}$ *significa suprimir esa entrada.*

Veamos que $\mathbf{P}(G)$ es efectivamente una resolución de $\mathbb{Z}$. Primero verifiquemos que $\mathbf{P}(G)$ es un complejo, es decir, que se cumple: $\delta_{n-1}\delta_n = 0$. Por definición de δ_n tenemos que:

$$\delta_n(x_0, x_1, \ldots, x_n) = \textstyle\sum_{i=0}^{n}(-1)^i(x_0, \ldots, \hat{x_i}, \ldots, x_n)$$

esto, al aplicar δ_{n-1} es:

$$\begin{aligned}\delta_{n-1}\delta_n(x_0,x_1,\ldots,x_n) &= \delta_{n-1}(\sum_{i=0}^{n}(-1)^i(x_0,\ldots,\hat{x_i},\ldots,x_n))\\ &= \sum_{i=1}^{n}(-1)^i\delta_{n-1}(x_0,\ldots,\hat{x_i},\ldots,x_n)\end{aligned}$$

cada elemento $\delta_{n-1}(x_0,\ldots,\hat{x_i},\ldots,x_n)$ de esta suma es de la forma:

$$\delta_{n-1}(x_0,\ldots,\hat{x_i},\ldots,x_n) = \textstyle\sum_{j=0}^{n-1}(-1)^j(x_0,\ldots,\hat{x_j},\ldots,\hat{x_i},\ldots,x_n)$$

escribimos más explícitamente esta última suma:

$$\begin{aligned}\sum_{j=0}^{n-1}(-1)^j(x_0,\ldots,\hat{x_j},\ldots,\hat{x_i},\ldots,x_n) = (\hat{x_0},x_1,\ldots,\hat{x_i},\ldots,x_n)+\cdots\\ +(-1)^{i-1}(x_0,\ldots,\hat{x_{i-1}},\hat{x_i},\ldots,x_n)\\ +(-1)^i(x_0,\ldots,\hat{x_i},\hat{x_{i+1}},\ldots,x_n)+\cdots\\ +(-1)^{n-1}(x_0,x_1,\ldots,\hat{x_i},\ldots,\hat{x_n})\end{aligned}$$

nótese que el signo de $(x_0,\ldots,\hat{x_i},\ldots,\hat{x_k},\ldots,x_n)$, cuando $k \geq i+1$ es $(-1)^{k-1}$ pues el término x_k está en el lugar $k-1$ de $(x_0,\ldots,\hat{x_i},\ldots,\hat{x_k},\ldots,x_n)$, entonces podemos separar la suma en dos partes:

$$\begin{aligned}\delta_{n-1}(x_0,\ldots,\hat{x_i},\ldots,x_n) = &\sum_{j=0}^{i-1}(-1)^j(x_0,\ldots,\hat{x_j},\ldots,\hat{x_i},\ldots,x_n)\\ &+\sum_{k=i+1}^{n-1}(-1)^k(x_0,\ldots,\hat{x_i},\ldots,\hat{x_k},\ldots,x_n)\end{aligned}$$

Para ejemplificar lo que sucede con esta suma fijemos la atención en el término $(x_0,\ldots,\hat{x_i},\hat{x_{i+1}},\ldots,x_n)$ de $\delta_{n-1}\delta_n(x_0,x_1,\ldots,x_n)$, nótese que dicho término aparece en dos ocasiones, una al calcular $\delta_{n-1}(x_0,\ldots,\hat{x_i},\ldots,x_n)$ y la otra al calcular $\delta_{n-1}(x_0,\ldots,\hat{x_{i+1}},\ldots,x_n)$, el primero de ellos tiene signo $(-1)^{i-1}$ mientras que el signo del otro es $(-1)^i$ por tanto se cancelan, es decir, los términos de la suma

$$\delta_{n-1}\delta_n(x_0, x_1, \ldots, x_n) = \sum_{i=1}^{n}(-1)^i\delta_{n-1}(x_0, \ldots, \hat{x_i}, \ldots, x_n)$$

se cancelan dos a dos, por lo que al final $\delta_{n-1}\delta_n = 0$.

Sólo falta verificar que $\mathbf{P}(G)$ es exacta. Diremos que una resolución libre es una resolución G-libre si está constituida por G-módulos.

Proposición 3.4.3 *La resolución homogénea* $\boldsymbol{P}$(G)*, es una resolución G-libre de $\mathbb{Z}$ considerado como G-módulo trivial.*

Demostración. Por el Teorema 1.4.13 es suficiente construir una homotopía de contracción:

$$\cdots \longleftarrow P_3 \xleftarrow{s_2} P_2 \xleftarrow{s_1} P_1 \xleftarrow{s_0} P_0 \xleftarrow{s_{-1}} \mathbb{Z}$$

tal que $\varepsilon s_{-1} = id_{\mathbb{Z}}$ y $\delta_{n+1}s_n + s_{n-1}\delta_n = id_{P_n}$ para todo $n \geq 0$. Defínase $s_{-1} : \mathbb{Z} \longrightarrow P_0$ por $m \mapsto m \cdot (1_G)$ y para $n \geq 0$ definimos:

$$\begin{gathered} s_n : P_n \longrightarrow P_{n+1} \\ (x_0, x_1, \ldots, x_n) \mapsto (1_G, x_0, x_1, \ldots, x_n) \end{gathered}$$

con esto tenemos $\varepsilon s_{-1}(m) = \varepsilon(s_{-1}(m)) = \varepsilon(m \cdot (1_G)) = m$ y, si $n \geq 0$,

$$\begin{aligned} \delta_{n+1}s_n(x_0, x_1, \ldots, x_n) &= \delta_{n+1}(1_G, x_0, x_1, \ldots, x_n) \\ &= \sum_{i=-1}^{n}(-1)^{i+1}(1_G, x_0, \ldots, \hat{x_i}, \ldots, x_n) \text{ } \textit{donde } x_{-1} = 1_G \\ &= (x_0, x_1, \ldots, x_n) + \sum_{i=0}^{n}(-1)^{i+1}(1_G, x_0, \ldots, \hat{x_i}, \ldots, x_n) \end{aligned}$$

para $s_{n-1}\delta_n$ tenemos:

$$\begin{aligned} s_{n-1}\delta_n(x_0, x_1, \ldots, x_n) &= s_{n-1}(\sum_{j=0}^{n}(-1)^j(x_0, \ldots, \hat{x_j}, \ldots, x_n)) \\ &= \sum_{j=0}^{n}(-1)^j s_{n-1}(x_0, \ldots, \hat{x_j}, \ldots, x_n) \\ &= \sum_{j=0}^{n}(-1)^j(1_G, x_0, \ldots, \hat{x_j}, \ldots, x_n) \end{aligned}$$

así, al sumar:

$$\begin{aligned}(\delta_{n+1}s_n + s_{n-1}\delta_n)(x_0, x_1, \ldots, x_n) = (x_0, x_1, \ldots, x_n) \\ + \sum_{i=0}^{n}(-1)^{i+1}(1_G, x_0, \ldots, \hat{x_i}, \ldots, x_n) \\ + \sum_{j=0}^{n}(-1)^{j}(1_G, x_0, \ldots, \hat{x_j}, \ldots, x_n)\end{aligned}$$

es claro que cada término de $\sum_{i=0}^{n}(-1)^{i+1}(1_G, x_0, \ldots, \hat{x_i}, \ldots, x_n)$ se cancela con un término de $\sum_{j=0}^{n}(-1)^{j}(1_G, x_0, \ldots, \hat{x_j}, \ldots, x_n)$ por lo que al final nos queda $\delta_{n+1}s_n + s_{n-1}\delta_n(x_0, x_1, \ldots, x_n) = (x_0, x_1, \ldots, x_n)$, es decir, $\delta_{n+1}s_n + s_{n-1}\delta_n = id_{P_n}$. Esto muestra que los s_n constituyen una homotopía de contracción por lo que $\boldsymbol{P}(\mathrm{G})$ es exacta y por tanto es una resolución G-libre de $\mathbb{Z}$. ■

Ahora estamos en posición de poder probar que $\mathbf{B}(G)$ es una resolución G-libre de $\mathbb{Z}$. El proceso consiste en probar que es un complejo apoyándonos de $\mathbf{P}(G)$ para después probar que es una sucesión exacta.

Proposición 3.4.4 $\boldsymbol{B}(\mathrm{G})$ *es una resolución G-libre de* $\mathbb{Z}$.

Demostración. Definimos para cada $n \geq 0$:

$$\begin{gathered}\tau_n : P_n \longrightarrow B_n \\ (x_0, \ldots, x_n) \mapsto x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_{n-1}^{-1}x_n]\end{gathered}$$

cuya inversa está dada por:

$$\begin{gathered}\sigma_n : B_n \longrightarrow P_n \\ [x_1, \ldots, x_n] \mapsto (1, x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2\cdots x_n)\end{gathered}$$

Efectivamente una es inversa de la otra. Si $[x_1, \ldots, x_n] \in B_n$ entonces:

$$\begin{aligned}\tau_n\sigma_n[x_1, \ldots, x_n] &= \tau_n(1, x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2\cdots x_n) \\ &= [x_1, x_1^{-1}x_1x_2, \ldots, (x_1x_2\cdots x_{n-1})^{-1}(x_1x_2\cdots x_n)] \\ &= [x_1, x_2, \ldots, x_n]\end{aligned}$$

y si $(x_o, \ldots, x_n) \in P_n$:

$$\begin{aligned}\sigma_n\tau_n(x_o, \ldots, x_n) &= \sigma_n x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_n^{-1}x_n] \\ &= x_0\sigma_n[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_n^{-1}x_n] \\ &= x_0(1, x_0^{-1}x_1, x_0^{-1}x_1x_1^{-1}x_2, \ldots, x_0^{-1}x_1x_1^{-1}x_2\cdots x_{n-1}x_{n-1}^{-1}x_n) \\ &= (x_0, x_2, \ldots, x_n)\end{aligned}$$

Sólo debemos verificar que $\tau = \{\tau_n\}$ es un morfismo de cadenas, es decir, que el siguiente diagrama conmuta para toda $n > 0$

$$\begin{array}{ccc} P_n & \xrightarrow{\delta n} & P_{n-1} \\ {\scriptstyle \tau_n}\downarrow & & \downarrow{\scriptstyle \tau_{n-1}} \\ B_n & \xrightarrow[d_n]{} & B_{n-1} \end{array}$$

si $(x_0, x_2, \ldots, x_n) \in P_n$ entonces:

$$\begin{aligned}d_n\tau_n(x_1, x_2, \ldots, x_n) &= d_n(x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_n^{-1}x_n]) \\ &= x_0 d_n[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_n^{-1}x_n]\end{aligned}$$

y recordando que:

$$\begin{aligned}d_n[x_1, x_2, \ldots, x_n] = x_1[x_2, x_3, \ldots, x_n] &+ \sum_{i=1}^{n-1}(-1)^i[x_1, \ldots, x_ix_{i+1}, \ldots, x_n] \\ &+(-1)^n[x_1, \ldots, x_{n-1}]\end{aligned}$$

tenemos:

$$\begin{aligned}d_n\tau_n(x_1, x_2, \ldots, x_n) &= x_0 d_n[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_n^{-1}x_n] \\ &= x_0 {x_0}^{-1}x_1[{x_1}^{-1}x_2, {x_2}^{-1}x_3, \ldots, x_{n-1}^{-1}x_n] \\ &\quad + \sum_{i=1}^{n-1}(-1)^i x_0[x_0^{-1}x_1, \ldots, x_{i-1}^{-1}x_{i+1}, \ldots, x_n] \\ &\quad +(-1)^n x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_{n-2}^{-1}x_{n-1}] \\ \\ &= x_1[{x_1}^{-1}x_2, {x_2}^{-1}x_3, \ldots, x_{n-1}^{-1}x_n] \\ &\quad + \sum_{i=1}^{n-1}(-1)^i x_0[x_0^{-1}x_1, \ldots, x_{i-1}^{-1}x_{i+1}, \ldots, x_n] \\ &\quad +(-1)^n x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_{n-2}^{-1}x_{n-1}]\end{aligned}$$

Por otro lado:

$$\begin{aligned}\tau_{n-1}\delta_n(x_0, x_2, \ldots, x_n) &= \tau_{n-1}(\sum_{i=0}^{n}(-1)^i(x_0, \ldots, \hat{x_i}, \ldots, x_n)) \\ &= \sum_{i=0}^{n}(-1)^i\tau_{n-1}(x_0, \ldots, \hat{x_i}, \ldots, x_n)\end{aligned}$$

el primer término de esta última suma es:

$$\tau_{n-1}(\hat{x_0}, x_1, \ldots, x_n) = x_1[x_1^{-1}x_2, x_2^{-1}x_3, \ldots, x_{n-1^{-1}}x_n]$$

y el último es:

$$\tau_{n-1}(x_0, x_1, \ldots, \hat{x_n}) = (-1)^n x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_{n-2}^{-1}x_{n-1}]$$

por lo que podemos escribir dicha suma como:

$$\begin{aligned}\sum_{i=0}^{n}(-1)^i\tau_{n-1}(x_0, \ldots, \hat{x_i}, \ldots, x_n) = x_1[x_1^{-1}x_2, x_2^{-1}x_3, \ldots, x_{n-1}^{-1}x_n] \\ + \sum_{i=1}^{n-1}(-1)^i x_0[x_0^{-1}x_1, \ldots, x_{i-1}^{-1}x_{i+1}, \ldots, x_n] \\ +(-1)^n x_0[x_0^{-1}x_1, x_1^{-1}x_2, \ldots, x_{n-2}^{-1}x_{n-1}]\end{aligned}$$

esto quiere decir que $d_n\tau_n = \tau_{n-1}\delta_n$ lo cual implica que $d_n = \tau_{n-1}\delta_n\tau_n^{-1}$, así, como $\delta_n\delta_{n+1} = 0$ tenemos que:

$$d_n d_{n+1} = \tau_{n-1}\delta_n\tau_n^{-1}\tau_n\delta_{n+1}\tau_{n+1} = \tau_{n-1}\delta_n\delta_{n+1}\tau_{n+1} = 0$$

Esto prueba que $\mathbf{B}(G)$ es un complejo. Finalmente, por la proposición 3.4.3 $\mathbf{P}(G)$ es una sucesión exacta, lo cual implica que su homología $H^n(\mathbf{P})$ es igual a cero. Dado que acabamos de probar que $\mathbf{P}(G) \cong \mathbf{B}(G)$ entonces $H^n(\mathbf{B}) \cong H^n(\mathbf{P}) = 0$ y por lo tanto $\mathbf{B}(G)$ es exacta. ■

Hasta aquí hemos construido una resolución G-libre de $\mathbb{Z}$ que coincide en sus primeros términos con aquella que dimos en el Lema 3.1.1. Sin embargo, sabemos que esta resolución no es adecuada para probar $H^2(G, A) = e(G, A)$ así que el último paso consiste en modificar la resolución $\mathbf{B}(G)$. Para tal efecto considérese $U_n \subset B_n$ el submódulo generado por

$$U = \{[x_1, x_2, \ldots, x_n] \mid \text{al menos un } x_i = 1\}$$

Sea $[x_1, \ldots . x_n] \in U$ donde el término $x_j = 1$ lo cual denotaremos como $[x_1, \ldots, 1_j, \ldots, x_n]$, entonces

$$d_n[x_1, \ldots, 1_j, \ldots, x_n] = x_1[x_2, \ldots, 1_j, \ldots, x_n] + \sum_{i=1}^{n-1}(-1)^i[x_1, \ldots, x_i x_{i+1}, \ldots, x_n] + (-1)^n[x_1, \ldots, 1_j, \ldots, x_{n-1}]$$

en la expresión $\sum_{i=1}^{n-1}(-1)^i[x_1, \ldots, x_i x_{i+1}, \ldots, x_n]$ aparece 1_j en todos los sumandos excepto en dos, cuando $i = j-1$ y cuando $i = j$ se tiene:

$$(-1)^{j-1}[x_1, \ldots, x_{j-1} \cdot 1_j, x_{j+1}, \ldots, x_n] + (-1)^j[x_1, \ldots, x_{j-1}, 1_j \cdot x_{j+1}, \ldots, x_n]$$

pero, como se puede ver, estos se cancelan por lo que $d_n[x_1, \ldots, 1_j, \ldots, x_n]$ es un elemento de U_{n-1}. En otras palabras, $d_n(U_n) \subset U_{n-1}$ así que tenemos un subcomplejo $\mathbf{U}(G)$ de $\mathbf{B}(G)$.

Definición 3.4.5 *La resolución normalizada de barra de $\mathbb{Z}$, es el complejo:*

$$\mathbf{B}^*(G) = \mathbf{B}(G)/\mathbf{U}(G) : \cdots \longrightarrow B_3^* \xrightarrow{\bar{d_3}} B_2^* \xrightarrow{\bar{d_2}} B_1^* \xrightarrow{\bar{d_1}} B_0^* \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

donde $B_n^* = B_n/U_n$.

Nótese que $U_0 = 0$ por lo que $B_0^* = B_0 \cong \mathbb{Z}G$, obsérvese también que el escribir $\bar{d_n}$ es sólo una cuestión de notación pues la definición de estos morfismos es esencialmente la misma que la de d_n, la única diferencia es que ahora se aplica sobre las clases de B_n/U_n las cuales denotamos como $[x_1, \ldots, x_n]^*$, en particular, si $x_i = 1$ para algún i entonces $[x_1, \ldots, x_n]^* = 0$. Antes de continuar es preciso observar que cada B_n^* es el G-módulo libre generado por las clases $[x_1, \ldots, x_n]^*$; B_0^* visto como $\mathbb{Z}$-módulo, es decir como grupo abeliano, es libre con base $\{x[\,] : x \in G\}$ así como el G-módulo B_n^* es un grupo abeliano libre con base $\{x[x_1, \ldots, x_n]^* : x, x_i \in G, x_i \neq 1 \ \forall i\}$ pues su elementos son combinaciones lineales del tipo:

$$\sum_{x \in G} m_x x[x_1, \ldots, x_n]^* \text{ con } m_x \in \mathbb{Z}$$

Teorema 3.4.6 *La resolución normalizada de barra, $\mathbf{B}^*(G)$, es una resolución G-libre de $\mathbb{Z}$.*

Demostración. Nuevamente, es suficiente construir una homotopía de contracción:

$$\cdots \longleftarrow B_3^* \xleftarrow{t_2} B_2^* \xleftarrow{t_1} B_1^* \xleftarrow{t_0} B_0^* \xleftarrow{t_{-1}} \mathbb{Z}$$

Definimos $t_{-1} : \mathbb{Z} \longrightarrow B_0^*$ por $m \mapsto m[\,]$ y para $n \geq 0$, definimos:

$$\begin{array}{c} t_n : B_n^* \longrightarrow B_{n+1}^* \\ x[x_1, \ldots, x_n]^* \mapsto [x, x_1, \ldots, x_n]^* \end{array}$$

nótese que cada t_n está definido sobre la base de B_n^* visto como grupo abeliano, lo cual es suficiente en vista del Teorema 1.1.7. Ahora debemos verificar dos cosas, la primera es que $\varepsilon t_{-1} = id_{\mathbb{Z}}$, entonces:

$$\varepsilon(t_{-1}(m)) = \varepsilon(m[\,]) = m$$

y la otra es checar que $\bar{d}_{n+1} t_n + t_{n-1} \bar{d}_n = id_{B_n^*}$:

$$\begin{aligned} \bar{d}_{n+1} t_n(x[x_1, \ldots, x_n]^*) &= \bar{d}_{n+1}[x, x_1, \ldots, x_n]^* \\ &= x[x_1, \ldots, x_n]^* + \sum_{i=1}^{n+1} (-1)^i [x, x_1, \ldots, x_i x_{i+1}, \ldots, x_n]^* \\ &\quad + (-1)^{n+1} [x, x_1, \ldots, x_{n-1}]^* \end{aligned}$$

y por otro lado:

$$\begin{aligned} t_{n-1} \bar{d}_n(x[x_1, \ldots, x_n]^*) &= t_{n-1}(x \bar{d}_n[x_1, \ldots, x_n]^*) \\ &= t_{n-1} x(x_1[x_2, \ldots, x_n]^* \\ &\quad + \sum_{i=1}^{n} (-1)^i [x_1, \ldots, x_i x_{i+1}, \ldots, x_n]^* \\ &\quad + (-1)^n [x_1, x_2, \ldots, x_{n-1}]^*) \\ \\ &= t_{n-1}(x x_1[x_2, \ldots, x_n]^*) \\ &\quad + \sum_{i=1}^{n} (-1)^i t_{n-1}(x[x_1, \ldots, x_i x_{i+1}, \ldots, x_n]^*) \\ &\quad + (-1)^n t_{n-1}(x[x_1, x_2, \ldots, x_{n-1}]^*) \\ \\ &= [x x_1, x_2, \ldots, x_n]^* \\ &\quad + \sum_{i=1}^{n} (-1)^i [x, x_1, \ldots, x_i x_{i+1}, \ldots, x_n]^* \end{aligned}$$

$$+(-1)^n[x,x_1,x_2,\ldots,x_{n-1}]^*$$

$$=\sum_{i=0}^{n}(-1)^i[x,x_1,\ldots,x_ix_{i+1},\ldots,x_n]^* +(-1)^n[x,x_1,x_2,\ldots,x_{n-1}]^*$$

Por lo que, al calcular $\left(\bar{d_{n+1}}t_n + t_{n-1}\bar{d_n}\right)(x[x_1,\ldots,x_n]^*)$, nos da:

$\bar{d_{n+1}}t_n(x[x_1,\ldots,x_n]^*) + t_{n-1}\bar{d_n}(x[x_1,\ldots,x_n]^*) =$

$(x[x_1,\ldots,x_n]^* + \sum_{i=1}^{n+1}(-1)^i[x,x_1,\ldots,x_ix_{i+1},\ldots,x_n]^* +$
$(-1)^{n+1}[x,x_1,\ldots,x_{n-1}]^*)$

$+(\sum_{i=0}^{n}(-1)^i[x,x_1,\ldots,x_ix_{i+1},\ldots,x_n]^* + (-1)^n[x,x_1,x_2,\ldots,x_{n-1}]^*)$

los términos $(-1)^{n+1}[x,x_1,\ldots,x_{n-1}]^*$ y $(-1)^n[x,x_1,x_2,\ldots,x_{n-1}]^*$ se cancelan, igualmente, los términos de $\sum_{i=1}^{n+1}(-1)^i[x,x_1,\ldots,x_ix_{i+1},\ldots,x_n]^*$ y $\sum_{i=0}^{n}(-1)^i[x,x_1,\ldots,x_ix_{i+1},\ldots,x_n]^*$, por lo que al final nos queda:

$$\left(\bar{d_{n+1}}t_n + t_{n-1}\bar{d_n}\right)(x[x_1,\ldots,x_n]^*) = x[x_1,\ldots,x_n]^*$$

es decir $\bar{d_{n+1}}t_n + t_{n-1}\bar{d_n} = id_{B_n^*}$, por lo tanto, $\mathbf{B}^*(G)$ es una resolución G-libre de $\mathbb{Z}$. ■

Teorema 3.4.7 $H^2(G,A) = e(G,A) = Z^2(G,A)/B^2(G,A)$

Demostración. Aplicamos $\mathrm{Hom}_G(-,A)$ a la resolución normalizada de barra y obtenemos:

$$\mathrm{Hom}_G(B_3^*,A) \xleftarrow{\bar{d_3}^*} \mathrm{Hom}_G(B_2^*,A) \xleftarrow{\bar{d_2}^*} \mathrm{Hom}_G(B_1^*,A) \xleftarrow{\bar{d_1}^*} \mathrm{Hom}_G(B_0^*,A)$$

por definición $H^2(G,A) = Ext^2_{\mathbb{Z}G}(\mathbb{Z},A) = Ker(\bar{d_3}^*)/Im(\bar{d_2}^*)$, sabemos que si $f \in Ker(\bar{d_3}^*)$ entonces cumple: $xf[y,x] - f[xy,z] + f[x,yz] - f[x,y] = 0$, más aún, ahora sí tenemos la igualdad $f[x,1] = 0 = f[1,x]$, por el Teorema 1.2.9, esto quiere decir que f es un conjunto factor, por tanto $Ker(\bar{d_3}^*) \subseteq Z^2(G,A)$. En lo que respecta a los elementos de $Im(\bar{d_2}^*)$, si $g \in Im(\bar{d_2}^*)$ ya sabemos que existe $h \in \mathrm{Hom}_G(B_1^*,A)$ tal que $g[x,y] = xh[y] - h[xy] + h[x]$, además, tenemos que $h[1] = 0$, es decir, g es una cofrontera, por lo cual $Im(\bar{d_2}^*) \subseteq B^2(G,A)$. La contención $Z^2(G,A) \subseteq Ker(\bar{d_3}^*)$ se sigue de manera inmediata del Teorema 1.2.9, inciso ii), la contención $B^2(G,A) \subseteq Im(\bar{d_2}^*)$

es inmediata de la definición de cofrontera, por lo tanto, $H^2(G, A) = e(G, A)$.
■

Para finalizar este trabajo, mostramos una aplicación de los grupos de cohomología a grupos cíclicos finitos. Primero, a partir de un grupo cíclico finito G, damos una resolución de $\mathbb{Z}$ para poder describir los grupos de cohomología con coeficientes en un G-módulo A. Después, definimos la dimensión cohomológica de un grupo y establecemos la relación entre la dimensión cohomológica de un grupo G y la dimensión cohomológica de un subgrupo de G, usando esto y calculando la dimensión cohomológica de grupos cíclicos finitos de orden distinto de 1, exhibimos que un grupo cuya dimensión cohomológica es finita es libre de torsión.

Proposición 3.4.8 *Sea $G =< x >$ un grupo cíclico finito de orden k. Sean $D = x - 1$ y $N = 1 + x + x^2 + \cdots + x^{k-1}$ elementos de $\mathbb{Z}G$. Entonces se tiene una resolución libre de $\mathbb{Z}$:*

$$\cdots \longrightarrow \mathbb{Z}G \xrightarrow{\bar{D}} \mathbb{Z}G \xrightarrow{\bar{N}} \mathbb{Z}G \xrightarrow{\bar{D}} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

donde los morfismos $\bar{D}$ y $\bar{N}$ son multiplicar por D y N respectivamente y ε es el morfismo de aumentación.

Demostración. Sabemos que, en este caso, $\mathbb{Z}G$ es conmutativo y esto nos permite ver fácilmente que $\bar{D}$ y $\bar{N}$ son morfismos de G-módulos. Por otro lado, tenemos que $ND = DN = x^k - 1 = 0$ lo cual quiere decir que $\bar{D} \circ \bar{N} = \bar{N} \circ \bar{D} = 0$ y, si $u \in \mathbb{Z}G$, entonces:

$$\varepsilon(\bar{D}u) = \varepsilon((x-1)u) = \varepsilon(x-1)\varepsilon(u) = 0 \text{ pues } x - 1 \in Ker(\varepsilon)$$

esto muestra que $Im(\bar{D}) \subset Ker(\varepsilon)$, por tanto tenemos un complejo y falta probar la exactitud. Nótese que $\varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$ es epimorfismo, el Lema 2.3.12 dice que $Ker(\varepsilon)$ está generado por los elementos de la forma $x - 1$ con $x \neq 1 \in G$, de lo cual se sigue que $Ker(\varepsilon) \subset Im(\bar{D})$.
i) $Ker(\bar{D}) \subset Im(\bar{N})$. Un elemento $u = \sum_{i=0}^{k-1} m_i x^i$ pertenece a $Ker(\bar{D})$ si y sólo si:

$$\begin{aligned}
0 &= Du \\
&= (x-1)[m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-1} x^{k-1}] \\
&= x m_0 + m_1 x^2 + m_2 x^3 + \cdots + m_{k-1} - m_0 - m_1 x - m_2 x^2 - \cdots - m_{k-1} x^{k-1} \\
&= (m_{k-1} - m_0)1 + (m_0 - m_1)x + \cdots + (m_{k-2} - m_{k-1})x^{k-1}
\end{aligned}$$

lo cual implica que los escalares son todos cero y por tanto $m_{k-1} = m_0 = \cdots = m_{k-2}$, esto quiere decir que la expresión para u se convierte en $u = \sum_{i=0}^{k-1} m_0 x^i = m_0 \sum_{i=0}^{k-1} x^i = m_0 N$, en otras palabras, $u \in Im(\bar{N})$.

ii) $Ker(\bar{N}) \subset Im(\bar{D})$. Si $u = \sum_{i=0}^{k-1} m_i x^i$ es un elemento de $Ker(\bar{N})$ entonces:

$$0 = \varepsilon(Nu) = \varepsilon(N)\varepsilon(u) = k\varepsilon(u)$$

como $k \neq 0$, $\varepsilon(u) = \sum_{i=0}^{k-1} m_i = 0$, así, podemos escribir a u como:

$$\begin{aligned} u &= -(x-1)(m_0 + (m_0 + m_1)x + \cdots + (m_0 + \cdots + m_{k-1})x^{k-1}) \\ &= -D(m_0 + (m_0 + m_1)x + \cdots + (m_0 + \cdots + m_{k-1})x^{k-1}) \end{aligned}$$

por tanto, $u \in Im(\bar{D})$. ■

Teorema 3.4.9 *Sea G un grupo cíclico finito de orden k. Si A es un G-módulo entonces, para todo $n \geq 1$*

$$\begin{gathered} H^0(G, A) \cong A^G \\ H^{2n}(G, A) \cong A^G/\bar{N}A \\ H^{2n-1}(G, A) \cong {}_N A/\bar{D}A \end{gathered}$$

donde ${}_N A = \{a \in A \mid Na = 0\}$.

Demostración. Por definición $H^m(G, A) = Ker(d_{m+1}^*)/Im(d_m^*)$. Considérese la resolución de la Proposición 3.4.8, en este caso $d_{2n+1} = \bar{D}$, $d_{2n} = \bar{N}$ y $d_0 = \varepsilon$, al aplicarle $\mathrm{Hom}_G(-, A)$ obtenemos la siguiente sucesión:

$$\mathrm{Hom}_G(\mathbb{Z}G, A) \xleftarrow{\bar{D}^*} \mathrm{Hom}_G(\mathbb{Z}G, A) \xleftarrow{\bar{N}^*} \mathrm{Hom}_G(\mathbb{Z}G, A) \xleftarrow{\bar{D}^*} \mathrm{Hom}_G(\mathbb{Z}G, A)$$

Nos interesa identificar a $Ker(\bar{D}^*)$, $Ker(\bar{N}^*)$, $Im(\bar{D}^*)$ y $Im(\bar{N}^*)$, comenzemos por identificar los núcleos.

Si $f \in Ker(\bar{D}^*)$ entonces $f(1) \in A^G$. En efecto, $\bar{D}^*(f) = f\bar{D} = 0$ lo cual implíca que $0 = f\bar{D}(1) = f((x-1)1) = (x-1)f(1) = xf(1) - f(1)$, lo cual equivale a $xf(1) = f(1)$. Lo anterior nos dice que cada elemento de $Ker(\bar{D}^*)$ nos determina un subconjunto de A^G, defínase la siguiente función, para cada $f \in Ker(\bar{D}^*)$:

$$\begin{gathered} \tau : Ker(\bar{D}^*) \longrightarrow A^G \\ \tau(f) = f(1) \end{gathered}$$

Afirmamos que τ es un isomorfismo. Primero:

i) $\tau(f+g) = (f+g)(1) = f(1) + g(1)$

ii) Sea $g \in G$, $\tau(gf) = g \cdot f(1) = gf(g^{-1}1) = f(gg^{-1}1) = f(1) = gf(1) = g\tau(f)$

Resta probar que es biyectiva. Si $\tau(f) = 0$ entonces $0 = \tau(f) = f(1)$ por lo cual f debe ser el morfismo cero. Por último, para un elemento $a \in A^G$ definimos $f_a(1) = a$, el siguiente cálculo muestra que $f_a \in Ker(\bar{D}^*)$:

$$\bar{D}^*(f_a) = f_a\bar{D}(1) = f_a((x-1)1) = (x-1)f_a(1) = (x-1)a = xa - a = 0$$

Por tanto, $Ker(\bar{D}^*) \cong A^G$. La demostración de que $Ker(\bar{N}^*) \cong {}_NA$ es completamente análoga, sólo hacemos la observación de que si $f \in Ker(\bar{N}^*)$ entonces $f(1) \in {}_NA$ pues $0 = f\bar{N}(1) = f((1 + x + x^2 + \cdots + x^{k-1})1) = (1 + x + x^2 + \cdots + x^{k-1})f(1)$, así, nuevamente cada elemento $f \in Ker(\bar{N}^*)$ nos determina un subconjunto de ${}_NA$. Esto nos determina un isomorfismo $\tau' : Ker(\bar{N}^*) \longrightarrow {}_NA$ dado por $\tau'(f) = f(1)$.

Para identificar a $Im(\bar{N}^*)$ y a $Im(\bar{D}^*)$, basta mostrar que $\tau(Im(\bar{N}^*)) = \bar{N}A$ y que $\tau'(Im(\bar{D}^*)) = \bar{D}A$. Sea $f \in Im(\bar{N}^*)$, existe $h \in \mathrm{Hom}_G(\mathbb{Z}G, A)$ tal que $\bar{N}^*(h) = h\bar{N} = f$, así, tenemos que $\tau(f) = f(1) = h(\bar{N}(1)) = h((x-1)1) = (x-1)h(1) = (x-1)a = \bar{N}(a)$ para algún $a \in A$, en otras palabras, $\tau(f) \in \bar{N}A$, esto prueba que $\tau(Im(\bar{N}^*)) \subset \bar{N}A$. Para probar la inclusión faltante, sea $x \in \bar{N}A$, $x = N\hat{a}$ para alguna $\hat{a} \in A$. Tomemos $h \in \mathrm{Hom}_G(\mathbb{Z}G, A)$ dado por $h(1) = \hat{a}$, con esto tenemos que $x = N\hat{a} = Nh(1) = h(N1) = h\bar{N}(1)$, tomando $f \in \mathrm{Hom}(\mathbb{Z}G, A)$ dado por $f(1) = h\bar{N}(1)$ vemos que $f \in Im(\bar{N}^*)$ y es tal que:

$$\tau(f) = f(1) = h\bar{N}(1) = Nh(1) = N\hat{a} = x$$

lo cual prueba que $\bar{N}A \subset \tau(Im(\bar{N}^*))$. Por tanto $\bar{N}A = \tau(Im(\bar{N}^*))$. La demostración de que $\tau'(Im(\bar{D}^*)) = \bar{D}A$ es totalmente análoga. En conclusión tenemos las siguientes igualdades, observando que la primera de ellas se debe al Teorema 3.2.4:

$$\begin{gathered} H^0(G, A) \cong A^G, \\ H^{2n}(G, A) = Ker(\bar{D}^*)/Im(\bar{N}^*) \cong A^G/\bar{N}A, \\ H^{2n-1}(G, A) = Ker(\bar{N}^*)/Im(\bar{D}^*) \cong {}_NA/\bar{D}A. \end{gathered}$$

■

Corolario 3.4.10 *Sea G un grupo cíclico finito de orden k. Si A es un G-módulo trivial entonces*

$$\begin{aligned} H^0(G, A) &\cong A, \\ H^{2n}(G, A) &\cong A/kA, \\ H^{2n-1}(G, A) &\cong {}_kA. \end{aligned}$$

donde ${}_kA = \{a \in A \mid ka = 0\}$. En particular, si $A = \mathbb{Z}$ entonces, $H^0(G, A) = \mathbb{Z}$, $H^{2n}(G, A) = \mathbb{Z}/k\mathbb{Z}$ y $H^{2n-1}(G, A) = 0$.

Definición 3.4.11 *Sea G un grupo. Decimos que G tiene dimensión cohomológica menor o igual que n si, para cualquier G-modulo A, $H^k(G, A) = 0$ para toda $k > n$. Denotamos esto como $cd(G) \leq n$. **La dimensión cohomológica de** G es el n más pequeño para el cual se cumple que $H^k(G, A) = 0$ si $k > n$, en este caso, denotamos $cd(G) = n$. Si tal n no existe entonces decimos que $cd(G) = \infty$.*

Si K es un subgrupo de G, ¿cuál es la relación entre $cd(K)$ y $cd(G)$?.

Teorema 3.4.12 *(Lema de Saphiro). Si K es un subgrupo de G y M es un K-módulo entonces, para todo $n \geq 0$:*

$$H^n(K, M) \cong H^n(G, \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G, M)$$

Demostración. Sabemos que $\mathrm{Hom}_K(\mathbb{Z}G, M)$ es un G-módulo por lo que la expresión tiene sentido. Recordemos la identidad del Teorema 1.5.9:

$$Ext^n_R(B \otimes_S A, C) \cong Ext^n_S(A, \mathrm{Hom}_R(B, C))$$

con ${}_SA$, ${}_RB_S$, ${}_RC$ y B R-proyectivo. En este caso $R = \mathbb{Z}K$, $S = \mathbb{Z}G$ y tomamos $B = \mathbb{Z}G$, $A = \mathbb{Z}$, $C = M$. Recordando que $\mathbb{Z}G \otimes_{\mathbb{Z}G} \mathbb{Z} \cong \mathbb{Z}$:

$$\begin{aligned} H^n(K, M) &= Ext^n_{\mathbb{Z}K}(\mathbb{Z}, M) \\ &\cong Ext^n_{\mathbb{Z}K}(\mathbb{Z}G \otimes_{\mathbb{Z}G} \mathbb{Z}, M) \\ &\cong Ext^n_{\mathbb{Z}G}(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G, M)) \\ &\cong Ext^n_{\mathbb{Z}G}(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G, M)) \\ &= H^n(G, \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G, M)) \end{aligned}$$

■

Corolario 3.4.13 *Si K es subgrupo de G entonces $cd(K) \leq cd(G)$.*

Demostración. Supongamos, sin pérdida de generalidad, que $cd(G) = n$. Si $k > n$ y A es un H-módulo entonces, por el Teorema 3.4.12, tenemos que:

$$H^k(K, A) \cong H^k(G, \mathrm{Hom}_K(\mathbb{Z}G, A)) = 0$$

por lo cual $cd(K)$ no puede ser mayor que n. ■

Corolario 3.4.14 *Si G es un grupo cíclico finito de orden distinto de 1 entonces $cd(G) = \infty$.*

Demostración. Sea $\mathbb{Z}$ considerado como G-módulo trivial y tomemos $A = \mathbb{Z}$ en el Corolario 3.4.10, el corolario dice que $H^{2n}(G, \mathbb{Z}) = \mathbb{Z}/k\mathbb{Z} \neq 0$ para todo n, es decir, no existe n tal que, si $k > n$, $H^{2k}(G, \mathbb{Z}) = 0$ así que, por definición, $cd(G) = \infty$. ■

Corolario 3.4.15 *Si $cd(G) < \infty$ entonces G es libre de torsión.*

Demostración. Supongamos que $cd(G) < \infty$ y que G contiene un elemento $x \neq 1$ de orden finito. Por el Corolario 3.4.13 tenemos que $cd(<x>) \leq cd(G)$ pero, por el Corolario 3.4.14, $cd(<x>) = \infty$ lo cual es una contradicción, por lo tanto, G es libre de torsión. ■

Bibliografía

[1] Beachy, J. A. *Introductory Notes on Rings and Modules*. Cambridge University Press, 1999.

[2] Hilton P.J., Stammbach U. *A Course in Homological Algebra*. Springer, 1971.

[3] Hilton, P. J., *A Brief, Subjective History of Homology and Homotopy Theory in This Century*. Mathematics Magazine 60 (5), p.p. 282–291, 1988.

[4] Rotman, J.J. *An Introduction to Homological Algebra*. Academic Press, 1979.

[5] Rotman, J.J. *An Introduction to Homological Algebra 2nd. Ed.* Springer, 2009.