UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

INTRODUCCIÓN A LA TEORÍA DE COHOMOLOGÍA DE GRUPOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

PRESENTA:

CARLOS PÉREZ GÓMEZ

TUTORA

DRA. EDITH CORINA SÁENZ VALADEZ

Ciudad Universitaria, Ciudad de México, 2019

1. Datos del alumno
Pérez
Gómez
Carlos
9676747022
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
408006486

2. Datos del tutor
Dra.
Edith Corina
Sáenz
Valadez

3. Datos del sinodal 1
Dr.
Octavio
Mendoza
Hernández

4. Datos del sinodal 2
Dr.
Valente
Santiago
Vargas

5. Datos del sinodal 3
M. en C.
Clotilde
García
Villa

6. Datos del sinodal 4
M. en C.
Mindy Yaneli
Huerta
Pérez

7. Datos del trabajo escrito
Introducción a la Teoría de Cohomología de Grupos
89 p
2019

Dedicado a mis padres
Andrés y Rosa

Agradecimientos

Agradezco profundamente:

A mis Padres que me han guiado por la vida con amor y paciencia, por toda la comprensión y confianza que siempre me han brindado a lo largo de todos estos años. Hoy ven forjado un anhelo, una ilusión, un deseo y quiero que sepan que este logro también es de ustedes y que la fuerza que me ayudó a conseguirlo fue su apoyo en cada momento.

A mis hermanos: Lucio, Cecy y Migue por brindarme su cariño, su compañia y su apoyo en las buenas y en las malas.

A mi asesora la Dra. Edith Corina Sáenz Valadez por la valiosa oportunidad de trabajar bajo su dirección, por su paciencia y sus recomendaciones.

A la Profesora Clotilde García por el tiempo que le dedicó a la revisión de este trabajo, por sus valiosas sugerencias, por ser mi maestra en muchas materias y sobre todo por ser mi amiga.

A mi Psiquiatra la Dra. Guillen por sus terapias para controlar mi ansiedad y también por las valiosas recomendaciones que hicieron posible que iniciara y terminara este trabajo.

A mis amigos de la carrera: Diana Yareth, Manuel Esteban, Wilfrido Antonio, Fabio Alejandro, Victor Alfonso, Carlos Alberto, Pablo, César, Leonel, Fernando, Yael, Esteban, por todos esos momentos alegres y divertidos en los que disfruté de su agradable compañía.

Índice general

Introducción

La *Cohomología de Grupos* surgió de la extensa algebraización de la Topología Combinatoria. El punto de partida de la teoría fue el trabajo de Hurewicz en 1936 sobre "espacios no esféricos". Aproximadamente un año antes, Hurewicz definió los grupos de homotopía de grado superior $\pi_n(X)$ de un espacio X para $n \geq 2$ y se enfocó en el estudio de aquellos espacios X conexos por trayectorias, cuyos grupos de homotopía de grado superior son todos triviales, pero cuyo grupo fundamental $\pi = \pi_1(X)$ no necesariamente es trivial. A éstos espacios los llamó *espacios no esféricos*.

Hurewicz demostró, entre otras cosas, que el tipo de homotopía de un espacio no esférico X está completamente determinado por su grupo fundamental π. Más adelante Hopf en 1942 y Eckmann, Eilenberg-MacLane, Freudenthal hicieron avances y en 1949 se tenía una definición puramente algebraica de la cohomología de grupos, de la cual se hizo evidente que el tema era de interés tanto para los algebristas como para los topólogos. De hecho, se observó que los grupos de cohomología en dimensiones bajas coincidían con grupos que se habían estudiado en los trabajos de Schur sobre "representaciones proyectivas" y en los trabajos de Schreier sobre extensiones de grupos.

En este trabajo iniciamos estudiando el anillo de grupo RG, donde G es cualquier grupo y R un anillo asociativo con 1. Después desarrollamos el resto de la teoría trabajando únicamente sobre el anillo de grupo $\mathbb{Z}G$. Lo anterior nos sirve como fundamento para definir a los grupos de cohomología

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

de un grupo G con coeficientes en un G-módulo M.

Ahora bien, el objetivo principal de este trabajo es mostrar interpretaciones concretas de los grupos de cohomología $H^0(G, M)$, $H^1(G, M)$ y $H^2(G, M)$. Sin embargo, también incluimos algunos resultados interesantes como son: el cálculo de los grupos de cohomología $H^k(C_n, M)$, para C_n un grupo cíclico finito de orden n y la demostracion del *Teorema de Schur-Zassenhaus*, el cual establece condiciones necesarias pero no suficientes para que un grupo finito G con $K \lhd G$ sea un producto semidirecto de K por G/K. Para ello supondremos que el lector tiene los conocimientos básicos de la *Teoría de Grupos*, *Anillos* y *Módulos* que se ofrecen en los cursos de Licenciatura en Matemáticas de la Facultad de Ciencias de la UNAM.

El trabajó está dividido como sigue:

En el *Capítulo 1* definimos al anillo de grupo RG y demostramos algunas propiedades

de este anillo y de su ideal de aumento I_G.

En el *Capítulo 2* definimos para cada entero $n \geq 0$ el grupo de cohomología $H^n(G, M)$ de un grupo G con coeficientes en un G-módulo M y nos centramos en el estudio del grupo $H^0(G, M)$ y de los grupos $H^n(C_k, M)$ con C_k un grupo cíclico finito de orden k. Posteriormente construimos algunas resoluciones proyectivas que usamos en el *Capítulo 3* y en el *Capítulo* 4 para calcular los grupos de cohomología $H^2(G, M)$ y $H^1(G, M)$.

En el *Capítulo 3* estudiamos las extensiones de grupos con núcleo abeliano, esto con la finalidad de mostrar una manera de clasificarlas mediante el grupo $H^2(G, M)$.

Por último, en el *Capítulo 4* estudiamos a los morfismos estabilizadores de una extensión y su relación con las derivaciones, los cuales usamos para identificar al grupo $H^1(G, M)$. Finalizamos enunciando y demostrando el *Teorema de Schur-Zassenhaus*.

Capítulo 1

Anillos de Grupo

En este capítulo comenzamos con la noción de módulo libre y después definimos el anillo de grupo RG de un grupo G con coeficientes en un anillo R. Estudiamos algunas propiedades del anillo RG y de su ideal de aumento I_G.

A lo largo de este trabajo supondremos que R es un anillo asociativo con 1_R.

1.1. Módulos libres

Definición 1.1.1. Sea M un R-módulo. Un subconjunto finito $\{a_1, a_2, \ldots, a_n\}$ de M es *linealmente independiente* si para todo $r_1, \ldots, r_n \in R$ la igualdad

$$\sum_{i=1}^{n} r_i a_i = 0,$$

implica que $r_i = 0$ para cada i.

Ejemplo. Si R es un anillo y $M = R$, entonces $\{1\}$ es un conjunto linealmente independiente.

Definición 1.1.2. Sean M un R-módulo y S un subconjunto de M. Decimos que S es *linealmente independiente* si cada subconjunto finito de S es linealmente independiente.

Ejemplo. Sean R un anillo y $M = R[x]$ (el anillo de polinomios con coeficientes en R), entonces $S = \{1, x, x^2, \ldots\}$ es un conjunto linealmente independiente.

Definición 1.1.3. Sea X un conjunto. Un R-módulo *libre* sobre X está dado por un R-módulo ${}_RL(X)$ junto con una función $j_X : X \to {}_RL(X)$, que cumplen con lo siguiente: Para todo R-módulo M y toda función $f : X \to M$ existe un único morfismo de R-módulos $g : {}_RL(X) \to M$ tal que $gj_X = f$, es decir, el siguiente diagrama conmuta.

$$\begin{array}{ccc} X & \xrightarrow{j_X} & {}_RL(X) \\ {\scriptstyle f}\downarrow & \swarrow_{g} & \\ M & & \end{array}$$

Lema 1.1.4. *Sea X un conjunto. Si existe un R-módulo libre sobre X este es único salvo isomorfismos.*

Demostración. Sean L y L' R-módulos libres sobre X con $j : X \to L$ y $j' : X \to L'$ las funciones correspondientes a L y L', entonces existen morfismos únicos $g : L \to L'$ y $g' : L' \to L$ tales que gj=j' y $g'j' = j$.

$$\begin{array}{ccc} X & \xrightarrow{j} & L \\ {\scriptstyle 1_X}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{j'} & L' \\ {\scriptstyle 1_X}\downarrow & & \downarrow{\scriptstyle g'} \\ X & \xrightarrow[j]{} & L \end{array}$$

Por otro lado, $1_L j = j = g'j' = g'gj$, se sigue de la unicidad que $g'g = 1_L$. De forma similar se demuestra que $gg' = 1_{L'}$. □

Definición 1.1.5. Sea M un R-módulo. Diremos que $S \subseteq M$ es una *base* de M si S es linealmente independiente y S genera al R-módulo M.

Ejemplo. Sean R un anillo y $\alpha : X \to R$ una función. Definimos el *soporte* de α como

$$\textit{Sop}(\alpha) = \big\{x \in X : \alpha(x) \neq 0\big\}.$$

Consideremos el R-módulo $R^{(X)} = \big\{\alpha : X \to R \mid \textit{Sop}(\alpha) \textit{ es finito}\big\}$. Para cada $x \in X$ definimos $\delta_x : X \to R$, llamada la *función característica de* x ó *función indicadora*, como

$$\delta_x(y) = \begin{cases} 1 & \textit{si } y = x \\ 0 & \textit{si } y \neq x \end{cases}$$

la cual claramente es de soporte finito, y $S = \big\{\delta_x : x \in X\big\}$ es un subconjunto de $R^{(X)}$ linealmente independiente. En efecto, si $x_1, \ldots, x_n \in X$ y $r_1, \ldots, r_n \in R$ satisfacen que

$$\sum_{i=1}^{n} r_i \delta_{x_i} = 0,$$

entonces para cada $j \in \{1, \ldots, n\}$

$$0 = \sum_{i=1}^{n} r_i \delta_{x_i}(x_j) = r_j \delta_{x_j}(x_j) = r_j.$$

Por lo tanto S es linealmente independiente. Por otro lado, si $\alpha \in R^{(X)}$, entonces

$$\alpha = \sum_{x \in X} \alpha(x)\delta_x \in \langle S \rangle .$$

Esta última igualdad se verifica evaluando en un elemento arbitrario de X, digamos y,

$$\left(\sum_{x\in X}\alpha(x)\delta_x\right)(y)=\sum_{x\in X}\alpha(x)\delta_x(y)=\alpha(y)\delta_y(y)=\alpha(y).$$

Por lo tanto $S=\{\delta_x : x\in X\}$ es una base para $R^{(X)}$.

Teorema 1.1.6. *Para todo conjunto X, existe un R-módulo libre sobre X.*

Demostración. Sean ${}_RL(X)=R^{(X)}$ y $j_X : X\to {}_RL(X)$ la función dada por

$$j_X(x)=\delta_x,$$

entonces si M es un R-módulo y $f : X\to M$ es una función arbitraria, definimos $g : {}_RL(X)\to M$ como

$$g(\alpha)=\sum_{x\in X}\alpha(x)f(x),$$

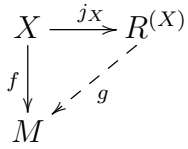
g definido así resulta ser un R-morfismo. En efecto,

$$g(\alpha+\beta)=\sum_{x\in X}(\alpha+\beta)(x)f(x)=\sum_{x\in X}\alpha(x)f(x)+\sum_{x\in X}\beta(x)f(x)=g(\alpha)+g(\beta)$$

y

$$g(r\alpha)=\sum_{x\in X}(r\alpha)(x)f(x)=\sum_{x\in X}r\alpha(x)f(x)=r\sum_{x\in X}\alpha(x)f(x)=rg(\alpha),$$

además g hace conmutar el siguiente diagrama



pues $gj_X(y)=g(\delta_y)=\sum\limits_{x\in X}\delta_y(x)f(x)=\delta_y(y)f(y)=f(y)$. Finalmente, g es única ya que si $g' : R^{(X)}\to M$ es otro R-morfismo tal que $g'j_X=f$, entonces

$$g'(\alpha)=g'\left(\sum_{x\in X}\alpha(x)\delta_x\right)=\sum_{x\in X}\alpha(x)g'(\delta_x)=\sum_{x\in X}\alpha(x)g'j_X(x)=\sum_{x\in X}\alpha(x)f(x)=g(\alpha).$$

□

1.2. El anillo de Grupo RG

En esta sección veremos que si G es un grupo (el cual siempre será pensado multiplicativamente), entonces el R-módulo libre $R^{(G)}$ admite estructura de anillo.

Definición 1.2.1. Sean G un grupo y R un anillo con identidad. El *anillo de grupo* de G con coeficientes en R, denotado por RG ó $R[G]$, es el R-módulo libre $R^{(G)}$ con base G, con la siguiente operación producto: Para cualesquiera α y $\beta \in R^{(G)}$

$$(\alpha\beta)(x) = \sum_{y\in G} \alpha(y)\beta(y^{-1}x) = \sum_{yz=x} \alpha(y)\beta(z).$$

La siguiente Proposición nos muestra que en efecto RG es un anillo.

Proposición 1.2.2. *Sean G un grupo y R un anillo, entonces RG es un anillo.*

Demostración. De la definición de RG se tiene que $(RG, +)$ es un grupo abeliano. Por otro lado, el producto cumple lo siguiente: si α, β y $\gamma \in R^{(G)}$, entonces

$$\begin{aligned}
\big((\alpha\beta)\gamma\big)(x) &= \sum_{yz=x} (\alpha\beta)(y)\gamma(z) = \sum_{yz=x}\left(\sum_{st=y} \alpha(s)\beta(t)\right)\gamma(z) \\
&= \sum_{stz=x} \big(\alpha(s)\beta(t)\big)\gamma(z) = \sum_{stz=x} \alpha(s)\big(\beta(t)\gamma(z)\big) \\
&= \sum_{s\in G} \alpha(s)\left(\sum_{tz=s^{-1}x} \beta(t)\gamma(z)\right) \\
&= \sum_{s\in G} \alpha(s)\left(\sum_{t\in G} \beta(t)\gamma\big(t^{-1}(s^{-1}x)\big)\right) \\
&= \sum_{s\in G} \alpha(s)(\beta\gamma)(s^{-1}x) = \big(\alpha(\beta\gamma)\big)(x)
\end{aligned}$$

El elemento δ_{1_G} es neutro multiplicativo

$$(\alpha\delta_{1_G})(x) = \sum_{yz=x} \alpha(y)\delta_{1_G}(z) = \alpha(x)\delta_{1_G}(1_G) = \alpha(x),$$

análogamente $\delta_{1_G}\alpha = \alpha$. Finalmente, el producto se distribuye sobre la suma

$$\begin{aligned}
\big((\alpha+\beta)\gamma\big)(x) &= \sum_{yz=x} (\alpha+\beta)(y)\gamma(z) = \sum_{yz=x} \big(\alpha(y)\gamma(z) + \beta(y)\gamma(z)\big) \\
&= \sum_{yz=x} \alpha(y)\gamma(z) + \sum_{yz=x} \beta(y)\gamma(z) = (\alpha\gamma)(x) + (\beta\gamma)(x) \\
&= (\alpha\gamma + \beta\gamma)(x)
\end{aligned}$$

Y de manera similar, se muestra que $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$. Por lo tanto RG es un anillo. □

A continuación veremos algunas de las propiedades del anillo de grupo RG.

Proposición 1.2.3. *Sean G un grupo y R un anillo. Entonces R es isomorfo a un subanillo de RG.*

Demostración. Para cada $r \in R$, definimos $\varphi(r) : G \to R$ como:

$$\varphi(r)(x) = \begin{cases} r & \textit{si } x = 1_G \\ 0 & \textit{si } x \neq 1_G \end{cases}$$

Notemos que $\varphi(r)$ está en RG. Veamos que $\varphi : R \to RG$ dada por $r \mapsto \varphi(r)$ es un morfismo de anillos.

Sean $r, s \in R$. Para $x = 1_G$

$$\begin{aligned} \varphi(r+s)(1_G) &= r + s = \varphi(r)(1_G) + \varphi(s)(1_G) \\ &= \big(\varphi(r) + \varphi(s)\big)(1_G) \end{aligned}$$

y

$$\begin{aligned} \big(\varphi(r)\varphi(s)\big)(1_G) &= \sum_{y \in G} \varphi(r)(y)\varphi(s)(y^{-1}) \\ &= \varphi(r)(1_G)\varphi(s)(1_G) \\ &= rs \\ &= \varphi(rs)(1_G) \end{aligned}$$

Si $x \neq 1_G$

$$\varphi(r+s)(x) = 0 = 0 + 0 = \varphi(r)(x) + \varphi(s)(x)$$

y

$$\begin{aligned} \big(\varphi(r)\varphi(s)\big)(x) &= \sum_{y \in G} \varphi(r)(y)\varphi(s)(y^{-1}x) \\ &= \varphi(r)(1_G)\varphi(s)(x) \\ &= r \cdot 0 \\ &= 0 \\ &= \varphi(rs)(x) \end{aligned}$$

Por lo tanto, $\varphi(r+s) = \varphi(r) + \varphi(s)$ y $\varphi(rs) = \varphi(r)\varphi(s)$, además

$$\varphi(1_R)(x) = \begin{cases} 1_R & \textit{si } x = 1_G \\ 0 & \textit{si } x \neq 1_G \end{cases} = \delta_{1_G}(x),$$

es decir, $\varphi(1_R) = \delta_{1_G} = 1_{RG}$. Por último, si $r \in \textit{Ker}(\varphi)$, entonces $r = \varphi(r)(1_G) = 0$. Por lo tanto, φ es inyectiva y así $R \simeq \textit{Im}(\varphi) \leq RG$. □

Proposición 1.2.4. *El grupo de unidades de RG contiene un subgrupo isomorfo a G.*

Demostración. Denotemos por $RG^\times$ al grupo de unidades de RG. Para cada $x \in G$ se tiene que $\delta_x \in RG^\times$, ya que

$$\begin{aligned}\Big(\delta_x\delta_{x^{-1}}\Big)(z) &= \sum_{y\in G}\delta_x(y)\delta_{x^{-1}}(y^{-1}z)\\ &= \delta_x(x)\delta_{x^{-1}}(x^{-1}z)\\ &= \delta_{x^{-1}}(x^{-1}z) = \begin{cases}1 & \textit{si } x^{-1}z = x^{-1}\\ 0 & \textit{si } x^{-1}z \neq x^{-1}\end{cases}\\ &= \begin{cases}1 & \textit{si } z = 1_G\\ 0 & \textit{si } z \neq 1_G\end{cases} = \delta_{1_G}(z),\end{aligned}$$

esto es, $\delta_x\delta_{x^{-1}} = \delta_{1_G} = 1_{RG}$, del mismo modo se prueba que $\delta_{x^{-1}}\delta_x = 1_{RG}$. Definimos $\psi : G \to RG^\times$ como $\psi(x) = \delta_x$, el cual resulta ser un morfismo de grupos.

$$\begin{aligned}\big(\psi(x)\psi(y)\big)(z) = (\delta_x\delta_y)(z) &= \sum_{w\in G}\delta_x(w)\delta_y(w^{-1}z)\\ &= \delta_x(x)\delta_y(x^{-1}z) = \delta_y(x^{-1}z)\\ &= \begin{cases}1 & \textit{si } x^{-1}z = y\\ 0 & \textit{si } x^{-1}z \neq y\end{cases} = \begin{cases}1 & \textit{si } z = xy\\ 0 & \textit{si } z \neq xy\end{cases}\\ &= \delta_{xy}(z) = \psi(xy)(z)\end{aligned}$$

Por lo tanto, $\psi(xy) = \psi(x)\psi(y)$. □

Sean $\alpha, \beta \in R^{(X)}$ y $r \in R$, definiendo $r_x = \alpha(x)$, $s_x = \beta(x)$ y la identificación $x = \delta_x$ se obtiene lo siguiente:

$$\begin{aligned}\alpha + \beta &= \sum_{x\in X}(\alpha+\beta)(x)\delta_x = \sum_{x\in X}\big(\alpha(x)+\beta(x)\big)\delta_x = \sum_{x\in X}(r_x + s_x)x\\ r\alpha &= \sum_{x\in X}(r\alpha)(x) = \sum_{x\in X} r\alpha(x) = \sum_{x\in X} rr_x\end{aligned}$$

Si $X = G$ es un grupo, el producto en el anillo RG se ve como

$$\alpha\beta = \sum_{z\in G}(\alpha\beta)(z)\delta_z = \sum_{z\in G}\left(\sum_{xy=z}\alpha(x)\beta(y)\right)\delta_z = \sum_{z\in G}\left(\sum_{xy=z} r_x s_y\right)z.$$

Teniendo esto en mente, de ahora en adelante pensaremos en el R-módulo libre con base en X como el conjunto de sumas formales de elementos de X, esto es,

$$L_X = \left\{\alpha = \sum_{x\in X} r_x x : r_x \in R \textit{ y } r_x = 0 \textit{ para casi todo } x \in X\right\}$$

donde las operaciones están dadas como sigue: Si $\alpha = \sum_{x\in X} r_x x$, $\beta = \sum_{x\in X} s_x x \in L_X$ y $r \in R$, entonces

$$\alpha + \beta = \sum_{x\in X} r_x x + \sum_{x\in X} s_x x = \sum_{x\in X} (r_x + s_x)x$$
$$r\alpha = r\sum_{x\in X} r_x x = \sum_{x\in X} (rr_x)x.$$

1.3. Ideales del anillo RG

En esta sección se presentan algunos de los ideales del anillo de grupo junto con algunas de sus propiedades.

Proposición 1.3.1. *Sean G un grupo, R un anillo e I un ideal izquierdo de R. Definimos el conjunto IG como*

$$IG = \left\{ \sum_{x\in G} r_x x \in RG : r_x \in I \text{ para todo } x \in G \right\}.$$

Entonces IG es un ideal izquierdo de RG.

Demostración. IG es no vacío pues I es no vacío. Sean $\alpha = \sum_{x\in G} s_x x$, $\beta = \sum_{x\in G} t_x x \in IG$ y $\gamma = \sum_{x\in G} r_x x \in RG$, entonces

$$\alpha - \beta = \sum_{x\in G} (s_x - t_x)x \in IG \qquad \text{Pues } s_x - t_x \in I \text{ por ser } I \text{ ideal de } R$$
$$\gamma\alpha = \sum_{z\in G} \left(\sum_{xy=z} r_x s_y \right) z \in IG \qquad \text{Pues } r_x s_y \in I \text{ para todo } x, y \in G$$

□

Del mismo modo podemos definir para un ideal derecho J de R el conjunto

$$JG = \left\{ \sum_{x\in G} r_x x \in RG : r_x \in J \text{ para todo } x \in G \right\}$$

y en este caso JG resulta ser un ideal derecho de RG. Si I es un ideal bilateral de R, entonces IG es un ideal bilateral de RG.

Proposición 1.3.2. *Sean G, H grupos y $f : G \to H$ un morfismo de grupos, entonces f induce un morfismo entre anillos de grupo $\overline{f} : RG \to RH$ dado por*

$$\overline{f}\left(\sum_{x\in G} r_x x \right) = \sum_{x\in G} r_x f(x).$$

Demostración. Si $\alpha = \sum_{x\in G} r_x x$ y $\beta = \sum_{x\in G} s_x x \in RG$, entonces

$$\begin{aligned}
\overline{f}(\alpha+\beta) &= \overline{f}\left(\sum_{x\in G}(r_x+s_x)x\right) = \sum_{x\in G}(r_x+s_x)f(x) = \sum_{x\in G}\big(r_xf(x)+s_xf(x)\big)\\
&= \sum_{x\in G} r_xf(x) + \sum_{x\in G} s_xf(x) = \overline{f}(\alpha)+\overline{f}(\beta)\\
\overline{f}(\alpha\beta) &= \overline{f}\left(\sum_{x,y\in G}(r_xs_y)xy\right) = \sum_{x,y\in G} r_xs_yf(xy)\\
&= \sum_{x,y\in G}(r_xs_y)f(x)f(y) = \left(\sum_{x\in G} r_xf(x)\right)\left(\sum_{y\in G} s_yf(y)\right)\\
&= \overline{f}(\alpha)\overline{f}(\beta)\\
\overline{f}(1_{RG}) &= \overline{f}(1_R1_G) = 1_Rf(1_G) = 1_R1_H = 1_{RH}.
\end{aligned}$$

□

En particular, si $H = \{1\}$ y $f : G \to H$ es el morfismo trivial, f induce el morfismo $\varepsilon = \overline{f} : RG \to RH \simeq R$ que está dado por

$$\varepsilon\left(\sum_{x\in G} r_x x\right) = \sum_{x\in G} r_x.$$

Al morfismo ε se le llama el ***morfismo de aumento*** y su núcleo

$$\mathit{Ker}(\varepsilon) = \left\{\sum_{x\in G} r_x x \in RG : \sum_{x\in G} r_x = 0\right\}$$

resulta ser un ideal bilateral llamado ***ideal de aumento***, el cual denotaremos por I_G.

Proposición 1.3.3. *El ideal de aumento I_G es un R-módulo libre con base en el conjunto*

$$\big\{x - 1_G : x \in G^\times\big\}$$

donde $G^\times = G \setminus \{1_G\}$.

Demostración. Si $\alpha = \sum_{x\in G} r_x x \in I_G$, entonces $\sum_{x\in G} r_x = 0$. Se sigue que

$$\begin{aligned}
\alpha &= \sum_{x\in G} r_x x - \left(\sum_{x\in G} r_x\right)1_G\\
&= \sum_{x\in G} r_x(x-1_G)\\
&= \sum_{x\in G^\times} r_x(x-1_G)
\end{aligned}$$

es decir, $\alpha \in \left\langle \{x - 1 : x \in G^\times\} \right\rangle$. Finalmente, si $s_1, \ldots, s_n \in R$ y $x_1, \ldots, x_n \in G^\times$ satisfacen que $\sum_{i=1}^{n} s_i(x_i - 1_G) = 0$, entonces

$$\begin{aligned} 0 &= \sum_{i=1}^{n} s_i(x_i - 1_G) \\ &= \sum_{i=1}^{n} s_i x_i + \Big(-\sum_{i=1}^{n} s_i\Big) 1_G \end{aligned}$$

y como RG es un R-módulo libre con base en G se tiene que $s_i = 0$ para todo $i \in \{1, \ldots, n\}$. □

Capítulo 2

Cohomología de Grupos

En este capítulo definimos para cada entero $n \geq 0$ el grupo de cohomología $H^n(G, M)$ de un grupo G con coeficientes en un G-módulo M y nos centramos en el estudio del grupo $H^0(G, M)$, para ello damos por conocido las nociones básicas del *Álgebra Homológica*. Una vez descrita la cohomología de grupo de grado cero, procedemos a calcular la cohomología de los grupos cíclicos finitos. Posteriormente construimos la resolución estándar, la resolución barra y la resolución barra normalizada del G-módulo trivial $\mathbb{Z}$, las cuales usamos después para dar interpretaciones concretas de los grupos de cohomología en dimensiones bajas.

2.1. G-módulos

Definición 2.1.1. Sean G un grupo y $(M, +)$ un grupo abeliano. Diremos que M es un G-módulo izquierdo si existe una función $\mu : G \times M \to M$ escrita como $\mu(x, a) = x \cdot a$ tal que:

a) $1_G \cdot a = a$ para todo $a \in M$

b) $(xy) \cdot a = x \cdot (y \cdot a)$ para todo $x, y \in G$ y $a \in M$

c) $x \cdot (a + b) = x \cdot a + x \cdot b$ para todo $x \in G$ y $a, b \in M$.

Es decir, G opera en el grupo abeliano M por la izquierda. A la función μ se le llama una ***acción*** de G en M.

Si E es un grupo (no necesariamente abeliano). El grupo de ***automorfismos*** de E se define como:

$$\boldsymbol{Aut}(E) = \big\{\varphi : E \to E \mid \varphi \text{ es un isomorfismo}\big\}$$

en donde la operación está dada por la composición de funciones. Un automorfismo φ es un ***automorfismo interior*** si es una conjugación, es decir, si existe un elemento $c \in E$ tal que

$$\varphi(e) = cec^{-1}$$

para todo $e \in E$. Un automorfismo es exterior si no es interior. El subconjunto $\boldsymbol{Inn}(E)$ de todos los automorfismos interiores es un subgrupo normal de $\boldsymbol{Aut}(E)$; al grupo cociente $\boldsymbol{Aut}(E)/\boldsymbol{Inn}(E)$ se le llama el *grupo de automorfismos exteriores* y se denota por $\boldsymbol{Out}(E)$.

La siguiente Proposición nos muestra algunas de las equivalencias acerca del concepto de G-módulo.

Proposición 2.1.2. *Sean G un grupo y $(M,+)$ un grupo abeliano. Los siguientes enunciados son equivalentes.*

a) M *es un G-módulo izquierdo.*

b) Existe un morfismo de grupos $\lambda : G \to \boldsymbol{Aut}(M)$.

c) M *es un $\mathbb{Z}G$-módulo izquierdo.*

Demostración.

a) $\Rightarrow$ *b)* Supongamos que M es un G-módulo izquierdo, definimos $\lambda : G \to \boldsymbol{Aut}(M)$ mediante $\lambda(x)(a) = x \cdot a$. Para cada $x \in G$, $\lambda(x) : M \to M$ es un morfismo de grupos

$$\lambda(x)(a+b) = x \cdot (a+b) = x \cdot a + x \cdot b = \lambda(x)(a) + \lambda(x)(b),$$

además $\lambda(x^{-1})$ es inverso de $\lambda(x)$, pues

$$\begin{aligned}\big(\lambda(x) \circ \lambda(x^{-1})\big)(a) &= \lambda(x)\big(\lambda(x^{-1})(a)\big) \\ &= \lambda(x)(x^{-1} \cdot a) \\ &= x \cdot (x^{-1} \cdot a) \\ &= (xx^{-1}) \cdot a \\ &= 1_G \cdot a \\ &= a\end{aligned}$$

se sigue que $\lambda(x) \circ \lambda(x^{-1}) = 1_M$, análogamente obtenemos que $\lambda(x^{-1}) \circ \lambda(x) = 1_M$. Por lo tanto $\lambda(x)$ es un isomorfismo. Finalmente,

$$\lambda(xy)(a) = (xy) \cdot a = x \cdot (y \cdot a) = \lambda(x)(y \cdot a) = \lambda(x)\big(\lambda(y)(a)\big) = \big(\lambda(x) \circ \lambda(y)\big)(a)$$

es decir, $\lambda(xy) = \lambda(x) \circ \lambda(y)$.

b) $\Rightarrow$ *a)* Sea $\lambda : G \to \boldsymbol{Aut}(M)$ un morfismo de grupos, definimos $\mu : G \times M \to M$ como

$$\mu(x,a) = x \cdot a = \lambda(x)(a).$$

Entonces,

1) $1_G \cdot a = \lambda(1_G)(a) = 1_M(a) = a$

2) $(xy) \cdot a = \lambda(xy)(a) = \big(\lambda(x) \circ \lambda(y)\big)(a) = \lambda(x)\big(\lambda(y)(a)\big) = \lambda(x)(y \cdot a) = x \cdot (y \cdot a)$

3) $x \cdot (a+b) = \lambda(x)(a+b) = \lambda(x)(a) + \lambda(x)(b) = x \cdot a + x \cdot b$

b) $\Rightarrow$ *c)* Por la Propiedad Universal del anillo $\mathbb{Z}G$, el morfismo de grupos

$$\lambda : G \to \boldsymbol{Aut}(M) \subseteq \boldsymbol{End}_{\mathbb{Z}}(M)$$

determina un único morfismo de anillos $\psi : \mathbb{Z}G \to \boldsymbol{End}_{\mathbb{Z}}(M)$, induciendo en M una estructura de $\mathbb{Z}G$-módulo izquierdo.

c) $\Rightarrow$ *b)* Ya que M es un $\mathbb{Z}G$-módulo, existe un morfismo de anillos $\psi : \mathbb{Z}G \to \boldsymbol{End}_{\mathbb{Z}}(M)$. Por otro parte, los elementos de G son unidades en $\mathbb{Z}G$, se sigue que $\psi(G) \subseteq \boldsymbol{End}_{\mathbb{Z}}(M)^{\times} = \boldsymbol{Aut}(M)$ y por lo tanto la restrición $\psi\,|_G \colon G \to \boldsymbol{Aut}(M)$ es un morfismo de grupos.

□

La Proposición 2.1.2 nos permite hablar indistintamente de un G-módulo izquierdo M o de un $\mathbb{Z}G$-módulo izquierdo M y así lo haremos a lo largo de este trabajo, teniendo en cuenta lo siguiente: dada la acción $\cdot : G \times M \to M$ de G sobre M la estructura de $\mathbb{Z}G$-módulo en M queda definida de la siguiente manera: Si $\sum_{x\in G} r_x x \in \mathbb{Z}G$ y $a \in M$, entonces

$$\left(\sum_{x\in G} r_x x\right) a = \sum_{x\in G} r_x (x \cdot a).$$

Recordemos también que si M es un R-módulo izquierdo entonces M es un R^{op}-módulo derecho, donde R^{op} denota al anillo opuesto de R. En el caso de que $R = \mathbb{Z}G$ podemos asegurar que todo $\mathbb{Z}G$-módulo izquierdo M es también un $\mathbb{Z}G$-módulo derecho, esto ultimo se debe a que $\mathbb{Z}G$ y $\mathbb{Z}G^{op}$ son anillos isomorfos como se muestra a continuación: la función $\varphi : \mathbb{Z}G \to \mathbb{Z}G^{op}$ definida como

$$\varphi\left(\sum_{x\in G} r_x x\right) = \sum_{x\in G} r_x x^{-1}$$

es biyectiva ya que para cada $\alpha = \sum_{x\in G} r_x x \in \mathbb{Z}G$

$$\varphi\big(\varphi(\alpha)\big) = \varphi\left(\sum_{x\in G} r_x x^{-1}\right) = \sum_{x\in G} r_x \big(x^{-1}\big)^{-1} = \sum_{x\in G} r_x x = \alpha,$$

es decir, ella misma es su propio inverso. Además, para cada $\alpha = \sum_{x\in G} r_x x$, $\beta = \sum_{x\in G} s_x x \in \mathbb{Z}G$

$$\begin{aligned}
\varphi(\alpha+\beta) &= \varphi\left(\sum_{x\in G} (r_x + s_x)x\right) \\
&= \sum_{x\in G} (r_x + s_x) x^{-1} \\
&= \sum_{x\in G} r_x x^{-1} + \sum_{x\in G} s_x x^{-1} \\
&= \varphi(\alpha) + \varphi(\beta)
\end{aligned}$$

y

$$\begin{aligned}\varphi(\alpha\beta) &= \varphi\left(\sum_{y,z\in G}(r_y s_z)yz\right)\\ &= \sum_{y,z\in G}(r_y s_z)(yz)^{-1}\\ &= \sum_{y,z\in G}(s_z r_y)\left(z^{-1}y^{-1}\right)\\ &= \left(\sum_{x\in G}s_x x^{-1}\right)\left(\sum_{x\in G}r_x x^{-1}\right)\\ &= \varphi(\beta)\varphi(\alpha)\end{aligned}$$

y así φ se traduce a un isomorfismo de $\mathbb{Z}G$ en $\mathbb{Z}G^{op}$.

Definición 2.1.3. Sean G un grupo y $(M,+)$ un grupo abeliano. Diremos que M es un G-módulo ***trivial*** si $x\cdot a = a$ para todo $x\in G$ y $a\in M$.

Es claro entonces que todo grupo abeliano M admite estructura de G-módulo trivial, simplemente definiendo en M dicha acción. En este caso, la estructura de $\mathbb{Z}G$-módulo sobre M se puede escribir en términos del morfismo de aumento $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ como sigue: si $\alpha = \sum_{x\in G} r_x x \in \mathbb{Z}G$ y $a\in M$, entonces

$$\left(\sum_{x\in G} r_x x\right)a = \sum_{x\in G} r_x(x\cdot a) = \sum_{x\in G} r_x a = \varepsilon(\alpha)a.$$

Por ejemplo, cuando hablemos del grupo de los números enteros $\mathbb{Z}$ lo estaremos pensando como G-módulo trivial, es decir, $x\cdot m = m$ para todo $x\in G$ y $m\in\mathbb{Z}$.

Ahora estamos listos para definir a nuestros objetos de estudio.

Definición 2.1.4. Si M es un G-módulo y $n\geq 0$ es un entero, el n-***ésimo grupo de cohomología*** de G con coeficientes en M es

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

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

Recordemos que estos grupos se pueden calcular de dos formas. La primera de ellas es tomando una resolución proyectiva $\mathbf{P}$ del G-módulo trivial $\mathbb{Z}$, donde por último estos grupos resultan de considerar la homología del complejo $\mathit{Hom}_{\mathbb{Z}G}(\mathbf{P}_{\mathbb{Z}}, M)$, donde $\mathbf{P}_{\mathbb{Z}}$ es el complejo reducido (que se obtiene de $\mathbf{P}$ al suprimir a $\mathbb{Z}$); la segunda forma de hacerlo sería tomando una resolución inyectiva $\mathbf{E}$ de M para finalmente calcular la cohomología del complejo $\mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z},\mathbf{E}^M)$, donde $\mathbf{E}^M$ es el complejo reducido (que se obtiene de $\mathbf{E}$ al suprimir a M).

Observación. Algunas propiedades acerca de los funtores derivados se traducen a este contexto como sigue:

1. $H^0(G,M) = \mathit{Ext}^0_{\mathbb{Z}G}(\mathbb{Z},M) \simeq \mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z},M)$.
2. $H^n(G,M) = 0$ para todo $n \geq 1$ si M es un G-módulo inyectivo.
3. Dada una sucesión exacta corta de G-módulos

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$$

se tiene asociada la sucesión larga de cohomología

$$\cdots \longrightarrow H^i(G,L) \longrightarrow H^{i+1}(G,M) \longrightarrow H^{i+1}(G,N) \longrightarrow H^{i+1}(G,L) \longrightarrow \cdots$$

para $i \geq 0$.

2.2. $H^0(G,M)$

Nuestro estudio de estos grupos empieza por el más fácil de calcular, el $H^0(G,M)$, y que por definición corresponde al $\mathit{Ext}^0_{\mathbb{Z}G}(\mathbb{Z},M)$, el cual sabemos es isomorfo al $\mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z},M)$. Este último grupo resulta ser isomorfo a un submódulo de M. Para darnos una idea de esto consideremos la siguiente sucesión exacta

$$0 \longrightarrow I_G \xrightarrow{\ i\ } \mathbb{Z}G \xrightarrow{\ \varepsilon\ } \mathbb{Z} \longrightarrow 0$$

donde ε es el morfismo de aumento y I_G el ideal de aumento. Ya que el funtor $\mathit{Hom}_{\mathbb{Z}G}(\_,M)$ es exacto izquierdo, la sucesión

$$0 \longrightarrow \mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z},M) \xrightarrow{\ \varepsilon^*\ } \mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,M) \xrightarrow{\ i^*\ } \mathit{Hom}_{\mathbb{Z}G}(I_G,M)$$

es exacta, y como el $\mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,M) \simeq M$ concluimos que $\mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z},M)$ es isomorfo a un submódulo de M. En la siguiente Proposición mostramos que dicho submódulo corresponde al subconjunto de M formado por los elementos que quedan fijos bajo la acción de G:

$$M^G := \big\{a \in M : x \cdot a = a \text{ para todo } x \in G\big\}.$$

Claramente, M^G es por definición un G-módulo trivial, llamado el ***submódulo de invariantes*** de M. Además, M^G es el mayor G-submódulo trivial de M, es decir, si $N \subseteq M$ es cualquier submódulo con una acción trivial de G (i.e., $x \cdot a = a$ para cualquier $x \in G$ y $a \in N$), entonces $N \subseteq M^G$.

Por otro lado, si $\varphi : M \to N$ es un G-morfismo, entonces $\varphi(M^G) \subseteq N^G$ ya que si $a \in M^G$ y $x \in G$, entonces

$$x \cdot \varphi(a) = \varphi(x \cdot a) = \varphi(a),$$

es decir, $\varphi(a) \in N^G$ y así podemos definir $\varphi^G : M^G \to N^G$ como $\varphi^G := \varphi|_{M^G}$. Esta forma de asignar a φ el morfimo φ^G respeta la composición de morfismos, esto es, si $\psi : M \to N$ y $\varphi : N \to L$ son G-morfismos, entonces

$$\big(\varphi^G \circ \psi^G\big)(a) = \varphi\big(\psi(a)\big) = (\varphi \circ \psi)(a) = (\varphi \circ \psi)^G(a),$$

y por lo tanto $\varphi^G \circ \psi^G = (\varphi \circ \psi)^G$. Por último, si $1_M : M \to M$ es la identidad en M, $1_M^G(a) = 1_M(a) = a$, así $1_M^G = 1_{M^G}$. Todo lo hecho previamente se resume en lo siguiente: la asignación $\mathit{Fix}^G : {}_{\mathbb{Z}G}\mathbf{Mod} \to {}_{\mathbb{Z}G}\mathbf{Mod}$ dada por $\mathit{Fix}^G(M) = M^G$ y $\mathit{Fix}^G(\varphi) = \varphi^G$ es un funtor llamado el ***funtor de puntos fijos***.

Proposición 2.2.1. *Si $\mathbb{Z}$ es considerado como G-módulo trivial, entonces existe un isomorfismo natural*

$$\mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z}, \_) \simeq \mathit{Fix}^G$$

En particular, Fix^G es exacto izquierdo.

Demostración. Sean M un G-módulo y $f : \mathbb{Z} \to M$ un G-morfismo, entonces para todo $x \in G$,

$$x \cdot f(1) = f(x \cdot 1) = f(1),$$

así $f(1) \in M^G$. Definimos $\eta_M : \mathit{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \to M^G$ como

$$\eta_M(f) = f(1)$$

a) η_M es un morfismo de grupos abelianos, pues

$$\eta_M(f + g) = (f + g)(1) = f(1) + g(1) = \eta_M(f) + \eta_M(g).$$

b) η_M es inyectiva: si $f \in \mathit{Ker}(\eta_M)$, entonces $f(1) = \eta_M(f) = 0$, se sigue que

$$f(m) = f(m1) = mf(1) = 0$$

y así $f = 0$.

c) η_M es suprayectiva: si $a \in M^G$, la función $f_a : \mathbb{Z} \to M$ dada por $f_a(m) = ma$ es un morfismo de grupos abelianos. Además, si $x \in G$ y $m \in \mathbb{Z}$, entonces

$$f_a(x \cdot m) = f_a(m) = ma = m(x \cdot a) = x \cdot (ma) = x \cdot f_a(m)$$

de modo que f_a resulta ser un G-morfismo, y $\eta_M(f_a) = f_a(1) = 1a = a$.

d) Es natural, es decir, si $\varphi : M \to N$ es un G-morfismo, entonces el siguiente diagrama conmuta.

$$\begin{array}{ccc} \mathit{Hom}_G(\mathbb{Z}, M) & \xrightarrow{\eta_M} & M^G \\ \downarrow{\scriptstyle \varphi_*} & & \downarrow{\scriptstyle \varphi^G} \\ \mathit{Hom}_G(\mathbb{Z}, N) & \xrightarrow[\eta_N]{} & N^G \end{array}$$

En efecto,

$$\begin{aligned} \big(\varphi^G \circ \eta_M\big)(f) &= \varphi^G\big(\eta_M(f)\big) \\ &= \varphi^G\big(f(1)\big) \\ &= \varphi\big(f(1)\big) \\ &= \big(\varphi \circ f\big)(1) \\ &= \eta_N(\varphi \circ f) \\ &= \eta_N\big(\varphi_*(f)\big) \\ &= \big(\eta_N \circ \varphi_*\big)(f) \end{aligned}$$

□

La Proposición anterior nos muestra otra manera de definir a los grupos de cohomología $H^n(G, M)$, a saber, como los funtores derivados derechos del funtor Fix^G. Para concluir con esta pequeña sección enunciamos el siguiente Corolario.

Corolario 2.2.2. *Sean G un grupo y M un G-módulo. Entonces*

$$H^0(G, M) \simeq M^G$$

En particular, si M es un G-módulo trivial, entonces $H^0(G, M) \simeq M$.

2.3. Cohomología de grupos cíclicos finitos

En este apartado diremos con exactitud quienes son cada uno de los grupos $H^m(G, M)$, en el caso de que el grupo G sea cíclico y finito; si G no es el grupo trivial veremos que para $m \geq 1$ esencialmento solo podemos tener a lo más dos posibilidades y estas dependen de la paridad de m. La manera en la que calcularemos estos grupos será construyendo una resolución libre (y por lo tanto proyectiva) $\mathcal{P}$ del G-módulo trivial $\mathbb{Z}$, para después calcular la correspondiente homología del complejo $Hom_{\mathbb{Z}G}(\mathcal{P}_{\mathbb{Z}}, M)$. Iniciamos presentando a la susodicha resolución.

Proposición 2.3.1. *Sea $G = \langle x \rangle$ un grupo cíclico finito de orden n. Consideremos los siguientes dos elementos en $\mathbb{Z}G$:*

$$D := x - 1 \qquad y \qquad N := 1 + x + x^2 + \cdots + x^{n-1},$$

entonces la sucesión

$$\mathcal{P} : \cdots \longrightarrow \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

donde ε es el morfismo de aumento y D, N denotan multiplicaciones por D y N respectivamente, es una G-resolución libre de $\mathbb{Z}$.

Demostración. Abusaremos de la notación al denotar por D y N a los morfismos multiplicación respectivamente. Ya que G es abeliano (pues G es cíclico), el anillo $\mathbb{Z}G$ es conmutativo y por lo tanto las multiplicaciones por D y N resultan ser G-morfismos.

La sucesión es un complejo ya que:

a) $D \circ N = DN = (x - 1)(1 + x + \cdots + x^{n-1}) = x^n - 1 = 0$, pues $x^n = 1$.

b) $N \circ D = ND = DN = 0$.

c) $\varepsilon \circ D = 0$, ya que si $\alpha \in \mathbb{Z}G$, entonces

$$\big(\varepsilon \circ D\big)(\alpha) = \varepsilon\big(D(\alpha)\big) = \varepsilon(D\alpha) = \varepsilon\big((x-1)\alpha\big) = \varepsilon(x-1)\varepsilon(\alpha) = 0.$$

La penúltima igualdad se tiene porque ε es un morfismo de anillos.

Ahora veamos que la sucesión es exacta.

d) *Ker*$(\varepsilon) = I_G \subseteq$ *Im*(D), en efecto, si $\alpha \in I_G$ por la Proposición 1.3.3

$$\alpha = r_1(x-1) + r_2(x^2-1) + \cdots + r_{n-1}(x^{n-1}-1)$$

con $r_i \in \mathbb{Z}$. Entonces

$$\begin{aligned}\alpha &= r_1(x-1) + r_2(x^2-1) + \cdots + r_{n-1}(x^{n-1}-1)\\ &= r_1(x-1) + r_2(x-1)(x+1) + \cdots + r_{n-1}(x-1)(x^{n-2}+x^{n-3}+\cdots+1)\\ &= (x-1)\Big(r_1 + r_2(x+1) + \cdots + r_{n-1}(x^{n-2}+x^{n-3}+\cdots+1)\Big)\\ &= D\Big(r_1 + r_2(x+1) + \cdots + r_{n-1}(x^{n-2}+x^{n-3}+\cdots+1)\Big)\end{aligned}$$

Por lo tanto $\alpha \in$ *Im*(D).

e) *Ker*$(D) \subseteq$ *Im*(N), ya que si $u = \sum_{k=0}^{n-1} r_k x^k \in$ *Ker*(D), entonces

$$\begin{aligned}0 &= D(u)\\ &= Du\\ &= (x-1)(r_0 + r_1x + \cdots + r_{n-1}x^{n-1})\\ &= r_0x + r_1x^2 + \cdots + r_{n-1}x^n - r_0 - r_1x - \cdots - r_{n-1}x^{n-1}\\ &= r_0x + r_1x^2 + \cdots + r_{n-1}\cdot 1_G - r_0 - r_1x - \cdots - r_{n-1}x^{n-1}\\ &= (r_{n-1}-r_0)\cdot 1_G + (r_0-r_1)x + \cdots + (r_{n-2}-r_{n-1})x^{n-1}\end{aligned}$$

Se sigue que $r_0 - r_1 = \cdots = r_{n-2} - r_{n-1} = r_{n-1} - r_0 = 0$. Por lo tanto

$$r_0 = r_1 = \cdots = r_{n-1},$$

y así $u = r_0\left(\sum_{k=0}^{n-1} x^k\right) = r_0N = Nr_0 = N(r_0) \in$ *Im*(N).

f) *Ker*$(N) \subseteq$ *Im*(D). Si $u = \sum_{k=0}^{n-1} r_k x^k \in$ *Ker*(N), entonces

$$0 = \varepsilon\big(N(u)\big) = \varepsilon(Nu) = \varepsilon(N)\varepsilon(u) = n\varepsilon(u)$$

por lo tanto $\varepsilon(u) = \sum_{k=0}^{n-1} r_k = 0$. Realizando unos cuantos cálculos obtenemos la si-

guiente igualdad: Para $k \geq 1$, sea $s_k = \sum_{i=0}^{k} r_i$, entonces

$$\begin{aligned} -D\Big(r_0 + s_1x + \cdots + s_{n-2}x^{n-2}\Big) &= (1-x)\Big(r_0 + s_1x + \cdots + s_{n-2}x^{n-2}\Big) \\ &= r_0 + s_1x + \cdots + s_{n-2}x^{n-2} \\ &\quad - r_0x - s_1x^2 - \cdots - s_{n-2}x^{n-1} \\ &= r_0 + (s_1 - r_0)x + \cdots \\ &\quad + (s_{n-2} - s_{n-3})x^{n-2} - s_{n-2}x^{n-1} \\ &= r_0 + r_1x + \cdots + r_{n-2}x^{n-2} + r_{n-1}x^{n-1} \\ &= u \end{aligned}$$

La penúltima igualdad se tiene porque $s_{n-2} + r_{n-1} = \varepsilon(u) = 0$. Por lo tanto $u \in \mathit{Im}(D)$.

□

En lo sucesivo, si $G = \langle x \rangle$ es un grupo cíclico de orden n, las letras D y N representarán a los elementos $x-1$ y $1+x+x^2+\cdots+x^{n-1}$ respectivamente. Además, para un G-módulo M, denotaremos por I_GM al subgrupo de M generado por los elementos de la forma $y \cdot a - a$ con $y \in G$ y $a \in M$, por ${}_NM = \big\{a \in M : Na = 0\big\}$ y por ${}_nM = \big\{a \in M : na = 0\big\}$.

Lema 2.3.2. *Sea $G = \langle x \rangle$ un grupo cíclico finito de orden n. Si M es un G-módulo, entonces:*

a) $M^G = {}_DM = \{a \in M : (x-1)a = Da = 0\}$

b) $DM = I_GM$

c) Si M es un G-módulo trivial, entonces $NM = nM$, ${}_NM = {}_nM$ y $DM = 0$.

Demostración.

a) Si $b \in M^G$, entonces $x \cdot b = b$, es decir, $Db = (x-1)b = x \cdot b - b = 0$. Por lo tanto $b \in \{a \in M : Da = 0\}$. Recíprocamente, si $b \in \{a \in M : Da = 0\}$, entonces $x \cdot b - b = (x-1)b = Db = 0$. Por lo tanto $x \cdot b = b$. Por inducción obtenemos que $x^k \cdot b = x$ para $k \geq 1$ y como el grupo G es cíclico se tiene el resultado.

b) Sea $a \in M$, entonces $Da = (x-1)a = x \cdot a - a \in I_GM$, por lo tanto $DM \subseteq I_GM$. Recíprocamente, si $y \in G$ y $a \in M$, entonces $y = x^k$ para algún $k \geq 1$. Luego

$$y \cdot a - a = x^k \cdot a - a = \big(x^k - 1\big)a = (x-1)\big(x^{k-1} + x^{k-2} + \cdots + x + 1\big)a$$

Por lo tanto $y \cdot a - a \in DM$, se sigue que $I_GM \subseteq DM$.

c) Las dos primeras igualdades se siguen de que para todo $a \in M$

$$\begin{aligned} Na &= \big(1 + x + x^2 + \cdots + x^{n-1}\big)a \\ &= a + x \cdot a + x^2 \cdot a + \cdots + x^{n-1} \cdot a \\ &= a + a + \cdots + a \\ &= na \end{aligned}$$

Para la tercera igualdad. Si $a \in M$, entonces $Da = (x-1)a = x \cdot a - a = a - a = 0$.

□

Ahora estamos listos para enunciar y demostrar lo que prometimos al inicio de esta sección.

Teorema 2.3.3. *Sea $G = \langle x \rangle$ un grupo cíclico finito de orden n. Si M es un G-módulo, entonces para todo $k \geq 1$*

$$\begin{aligned} H^0(G, M) &\simeq M^G \\ H^{2k-1}(G, M) &\simeq {}_NM/DM = {}_NM/I_GM \\ H^{2k}(G, M) &\simeq {}_DM/NM = M^G/NM \end{aligned}$$

Demostración. Por el Corolario 2.2.2 tenemos que $H^0(G, M) \simeq M^G$. Para calcular los grupos restantes procedemos de la siguiente manera: aplicando el funtor $Hom_{\mathbb{Z}G}(\_, M)$ al complejo $\mathcal{P}_{\mathbb{Z}}$ de la Proposición 2.3.1 se obtiene el complejo

$$\begin{aligned} 0 \longrightarrow Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{D^*} Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{N^*} Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{D^*} \\ Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{N^*} Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \xrightarrow{D^*} Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \longrightarrow \cdots \end{aligned}$$

Este complejo es isomorfo al complejo

$$0 \longrightarrow M \xrightarrow{\varphi_D} M \xrightarrow{\varphi_N} M \xrightarrow{\varphi_D} M \xrightarrow{\varphi_N} M \longrightarrow \cdots,$$

donde los morfismos $\varphi_D : M \to M$ y $\varphi_N : M \to M$ están dados por

$$\begin{aligned} \varphi_D(a) &= Da \\ \varphi_N(a) &= Na, \end{aligned}$$

dicho isomorfismo de complejos se debe a que el morfismo $\psi : Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \to M$ definido como

$$\psi(f) = f(1)$$

hace conmutar el diagrama

$$\begin{array}{ccccc} Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) & \xrightarrow{D^*} & Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) & \xrightarrow{N^*} & Hom_{\mathbb{Z}G}(\mathbb{Z}G, M) \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} \\ M & \xrightarrow{\varphi_D} & M & \xrightarrow{\varphi_N} & M \end{array}$$

En efecto,

$$\begin{aligned}(\psi \circ D^*)(f) &= \psi\big(D^*(f)\big)\\ &= \psi(f \circ D)\\ &= (f \circ D)(1)\\ &= f\big(D(1)\big)\\ &= f(D \cdot 1)\\ &= Df(1)\\ &= \varphi_D\big(f(1)\big)\\ &= \varphi_D\big(\psi(f)\big)\\ &= \big(\varphi_D \circ \psi\big)(f)\end{aligned}$$

y

$$\begin{aligned}(\psi \circ N^*)(f) &= \psi\big(N^*(f)\big)\\ &= \psi(f \circ N)\\ &= (f \circ N)(1)\\ &= f\big(N(1)\big)\\ &= f(N \cdot 1)\\ &= Nf(1)\\ &= \varphi_N\big(f(1)\big)\\ &= \varphi_N\big(\psi(f)\big)\\ &= (\varphi_N \circ \psi)(f)\end{aligned}$$

Además, se verifica facilmente que ψ es un isomorfismo. Por lo tanto

$$Ker(N^*)/Im(D^*) \simeq Ker(\varphi_N)/Im(\varphi_D) \quad \text{y} \quad Ker(D^*)/Im(N^*) \simeq Ker(\varphi_D)/Im(\varphi_N).$$

Por otro lado, los morfismos en el complejo $\mathcal{P}_{\mathbb{Z}}$ están dados por: $d_{2n-1} = D$ y $d_{2n} = N$ para $n \geq 1$. Entonces

$$\begin{aligned}H^{2k-1}(G, M) &= Ext_{\mathbb{Z}G}^{2k-1}(\mathbb{Z}, M)\\ &= Ker(d_{2k}^*)/Im(d_{2k-1}^*)\\ &= Ker(N^*)/Im(D^*)\\ &\simeq Ker(\varphi_N)/Im(\varphi_D)\\ &= {}_NM/DM\\ &= {}_NM/I_GM\end{aligned}$$

donde la ultima igualdad se tiene por el inciso *b)* del Lema 2.3.2.

$$\begin{aligned} H^{2k}(G,M) &= \mathit{Ext}^{2k}_{\mathbb{Z}G}(\mathbb{Z},M) \\ &= \mathit{Ker}(d^*_{2k+1})/\mathit{Im}(d^*_{2k}) \\ &= \mathit{Ker}(D^*)/\mathit{Im}(N^*) \\ &\simeq \mathit{Ker}(\varphi_D)/\mathit{Im}(\varphi_N) \\ &= \{a \in M : Da = 0\}/NM \\ &= M^G/NM \end{aligned}$$

y la última igualdad se tiene por el inciso *a)* del Lema 2.3.2. □

Ejemplo 2.3.4. Sea $G = \langle x \rangle$ un grupo cíclico finito de orden n, entonces

$$H^k(G, \mathbb{Z}G) = 0$$

para todo $k \geq 1$.

Demostración. Recordemos que la resolución

$$\mathcal{P} : \cdots \longrightarrow \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

dada en 2.3.1 es exacta. Por el Teorema 2.3.3 tenemos que si k es impar,

$$\begin{aligned} H^k(G, \mathbb{Z}G) &\simeq {}_N\mathbb{Z}G/D\mathbb{Z}G \\ &= \big\{\alpha \in \mathbb{Z}G : N\alpha = 0\big\}/\big\{D\alpha : \alpha \in \mathbb{Z}G\big\} \\ &= \mathit{Ker}(N)/\mathit{Im}(D) \\ &= 0 \end{aligned}$$

Análogamente, si k es par, entonces

$$\begin{aligned} H^k(G, \mathbb{Z}G) &\simeq {}_D\mathbb{Z}G/N\mathbb{Z}G \\ &= \big\{\alpha \in \mathbb{Z}G : D\alpha = 0\big\}/\big\{N\alpha : \alpha \in \mathbb{Z}G\big\} \\ &= \mathit{Ker}(D)/\mathit{Im}(N) \\ &= 0 \end{aligned}$$

□

Corolario 2.3.5. *Si $G = \{1\}$, entonces $H^n(G, M) = \{0\}$ para todo $n \geq 1$ y para todo G-módulo M.*

Demostración. Ya que $G = \{1\}$ es un grupo cíclico generado por $x = 1$, se tiene que $N = 1$ y $D = 0$. Por lo tanto

$${}_NM = \big\{a \in M : Na = 0\big\} = \{0\} = \big\{Da : a \in M\big\} = DM$$

y

$$M^G = \big\{a \in M : y \cdot a = a \text{ para todo } y \in G\big\} = M = \big\{Na : a \in M\big\} = NM.$$

De estas igualdades y del Teorema 2.3.3 se sigue el resultado. □

Corolario 2.3.6. *Si G es un grupo cíclico de orden n y M es un G-módulo trivial, entonces para todo $k \geq 1$*

$$\begin{aligned} H^0(G, M) &\simeq M \\ H^{2k-1}(G, M) &\simeq {}_nM = \{a \in M : na = 0\} \\ H^{2k}(G, M) &\simeq M/nM \end{aligned}$$

En particular, si M es el G-módulo trivial $\mathbb{Z}$, entonces

$$\begin{aligned} H^0(G, \mathbb{Z}) &\simeq \mathbb{Z} \\ H^{2k-1}(G, \mathbb{Z}) &\simeq 0 \\ H^{2k}(G, \mathbb{Z}) &\simeq \mathbb{Z}_n \end{aligned}$$

Demostración. Como M es un G-módulo trivial, $M^G = M$. Por el inciso *c)* del Lema 2.3.2 ${}_NM = {}_nM$, $NM = nM$ y $DM = 0$. Finalmente, por el Teorema 2.3.3, se tiene que

$$\begin{aligned} H^0(G, M) &\simeq M^G = M \\ H^{2k-1}(G, M) &\simeq {}_NM/DM = {}_nM \\ H^{2k}(G, M) &\simeq M^G/NM = M/nM \end{aligned}$$

y para el caso en el que M es el G-módulo trivial $\mathbb{Z}$,

$$\begin{aligned} H^0(G, \mathbb{Z}) &\simeq \mathbb{Z} \\ H^{2k-1}(G, \mathbb{Z}) &\simeq {}_n\mathbb{Z} = \{a \in \mathbb{Z} : na = 0\} = \{0\} \\ H^{2k}(G, \mathbb{Z}) &\simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n. \end{aligned}$$

□

2.4. Resolución homogénea y resolución barra

Dar una descripción precisa de la cohomología de los grupos cíclicos finitos fue, en cierta forma, sencillo, esto se debió a la existencia de una resolución proyectiva del G-módulo trivial $\mathbb{Z}$ que simplificó en gran medida las expresiones que se obtenían. Nuestra tarea en esta sección será mostrar, a manera de ejemplo, algunas resoluciones proyectivas del G-módulo trivial $\mathbb{Z}$ para un grupo arbitrario G; éstas resoluciones son usadas en el *Capítulo 3* y en el *Capítulo 4* para obtener algunos resultados.

Para un grupo arbitrario G, sea P_n el $\mathbb{Z}$-módulo libre con base el conjunto G^{n+1}, es decir,

$$P_n = \left\{ p = \sum_{(y_0,\ldots,y_n) \in G^{n+1}} r_{(y_0,\ldots,y_n)}(y_0, \ldots, y_n) : r_{(y_0,\ldots,y_n)} \in \mathbb{Z} \text{ son casi todos ceros} \right\}$$

y definimos la acción de G sobre P_n en los generadores, mediante traslaciones, i.e., para cada $x \in G$

$$x \cdot (y_0, \ldots, y_n) = (xy_0, \ldots, xy_n)$$

de modo que los P_n son, en efecto, G-módulos. Estos G-módulos serán los proyectivos de nuestra resolución, puesto que resultan ser $\mathbb{Z}G$-módulos libres tal y como se demuestra en el siguiente Lema.

Lema 2.4.1. *Para cada $n \in \mathbb{N}$, P_n es un $\mathbb{Z}G$-módulo libre, que tiene a*

$$X = \Big\{(1_G, x_1, \ldots, x_n) : x_i \in G\Big\}$$

como base.

Demostración. Sea $p \in P_n$, entonces

$$\begin{aligned} p &= \sum_{(y_0,\ldots,y_n)\in G^{n+1}} r_{(y_0,\ldots,y_n)}(y_0, \ldots, y_n) \\ &= \sum_{(y_0,\ldots,y_n)\in G^{n+1}} r_{(y_0,\ldots,y_n)}\big(y_0 \cdot (1_G, y_0^{-1}y_1, \ldots, y_0^{-1}y_n)\big) \\ &= \sum_{(y_1,\ldots,y_n)\in G^{n}} \left(\sum_{y_0\in G} r_{(y_0,y_1,\ldots,y_n)} y_0 \left(1_G, y_0^{-1}y_1, \ldots, y_0^{-1}y_n\right)\right) \\ &= \sum_{(y_1,\ldots,y_n)\in G^{n}} \alpha_{(y_1,\ldots,y_n)} \left(1_G, y_0^{-1}y_1, \ldots, y_0^{-1}y_n\right) \end{aligned}$$

donde $\alpha_{(y_1,\ldots,y_n)} = \sum_{y_0\in G} r_{(y_0,y_1,\ldots,y_n)} y_0 \in \mathbb{Z}G$ y así p es una $\mathbb{Z}G$-combinación lineal de elementos de X. Ahora veamos que X es un conjunto linealmente independiente: Si

$$0 = \sum_{(x_1,\ldots,x_n)\in G^n} \alpha_{(x_1,\ldots,x_n)}(1_G, x_1, \ldots, x_n)$$

es una suma finita con $\alpha_{(x_1,\ldots,x_n)} \in \mathbb{Z}G$, entonces $\alpha_{(x_1,\ldots,x_n)} = \sum_{x_0\in G} r_{(x_0,x_1,\ldots,x_n)} x_0$ donde $r_{(x_0,x_1,\ldots,x_n)} \in \mathbb{Z}$. Por lo tanto

$$\begin{aligned} 0 &= \sum_{(x_1,\ldots,x_n)\in G^n} \alpha_{(x_1,\ldots,x_n)}(1_G, x_1, \ldots, x_n) \\ &= \sum_{(x_1,\ldots,x_n)\in G^n} \left(\sum_{x_0\in G} r_{(x_0,x_1,\ldots,x_n)} x_0 (1_G, x_1, \ldots, x_n)\right) \\ &= \sum_{(x_1,\ldots,x_n)\in G^n} \left(\sum_{x_0\in G} r_{(x_0,x_1,\ldots,x_n)} (x_0, x_0x_1, \ldots, x_0x_n)\right) \\ &= \sum_{(x_0,\ldots,x_n)\in G^{n+1}} r_{(x_0,\ldots,x_n)} (x_0, x_0x_1, \ldots, x_0x_n) \end{aligned}$$

puesto que P_n, como $\mathbb{Z}$-módulo, es libre sobre G^{n+1}, podemos concluir que $r_{(x_0,\ldots,x_n)} = 0$ para todo $(x_0, \ldots, x_n) \in G^{n+1}$, y así $\alpha_{(x_1,\ldots,x_n)} = \sum_{x_0\in G} r_{(x_0,x_1,\ldots,x_n)} x_0 = 0$. □

Para $n \geq 1$, los morfismos $\partial_n : P_n \to P_{n-1}$ se definen, también en los generadores, mediante la fórmula

$$\partial_n(x_0, x_1, \ldots, x_n) = \sum_{j=0}^{n} (-1)^j (x_0, \ldots, \widehat{x}_j, \ldots, x_n)$$

donde el símbolo $\widehat{x}_j$ indica que el elemento correspondiente ha sido omitido, en particular

$$\partial_1(x_0, x_1) = x_1 - x_0.$$

Por ultimo, el morfismo $\varepsilon : P_0 \to \mathbb{Z}$ se define enviando cada generador $x \in G$ a $\varepsilon(x) = 1$, y así

$$\varepsilon\left(\sum_{x \in G} r_x x\right) = \sum_{x \in G} r_x,$$

i.e., ε es el morfismo de aumento.

Que esta sucesión es exacta, es lo que se afirma a continuación.

Proposición 2.4.2. *Sea G un grupo. La sucesión de $\mathbb{Z}G$-módulos libres*

$$\boldsymbol{P}(G) : \cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

es exacta.

Demostración. Primero veamos que $\mathbf{P}(G)$ es un complejo.

a) $\varepsilon \circ \partial_1 = 0$, ya que para todo generador $(x_0, x_1) \in P_1$ se tiene que

$$(\varepsilon \circ \partial_1)(x_0, x_1) = \varepsilon\big(\partial_1(x_0, x_1)\big) = \varepsilon(x_1 - x_0) = 1 - 1 = 0$$

b) $\partial_{n-1} \circ \partial_n = 0$ para todo $n \geq 1$. En efecto, si $(x_0, \ldots, x_n) \in P_n$, entonces

$$\begin{aligned}
(\partial_{n-1} \circ \partial_n)(x_0, \ldots, x_n) &= \partial_{n-1}\big(\partial_n(x_0, \ldots, x_n)\big) \\
&= \partial_{n-1}\left(\sum_{j=0}^{n} (-1)^j \big(x_0, \ldots, \widehat{x}_j, \ldots, x_n\big)\right) \\
&= \sum_{j=0}^{n} (-1)^j \partial_{n-1}\big(x_0, \ldots, \widehat{x}_j, \ldots, x_n\big) \\
&= \sum_{j=0}^{n} (-1)^j \left(\sum_{i=0}^{j-1} (-1)^i \big(x_0, \ldots, \widehat{x}_i, \ldots, \widehat{x}_j, \ldots, x_n\big)\right. \\
&\quad \left. + \sum_{i=j+1}^{n} (-1)^{i-1} \big(x_0, \ldots, \widehat{x}_j, \ldots, \widehat{x}_i, \ldots, x_n\big)\right) \\
&= 0
\end{aligned}$$

ya que la primera suma tiene el signo $(-1)^{i+j}$ y la segunda suma el signo $(-1)^{i+j-1}$ y por lo tanto se cancelan.

Para terminar de probar la exactitud de $\mathbf{P}(G)$, basta ver que $1_{\mathbf{P}(G)}$ es nulhomotópico, es decir, que en el siguiente diagrama

$$\begin{array}{ccccccccccccccc}
P_{n+1} & \xrightarrow{\partial_{n+1}} & P_n & \xrightarrow{\partial_n} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_1 & \xrightarrow{\partial_1} & P_0 & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\
{\scriptstyle 1_{P_{n+1}}}\downarrow & \swarrow_{s_n} & \downarrow{\scriptstyle 1_{P_n}} & \swarrow_{s_{n-1}} & \downarrow{\scriptstyle 1_{P_{n-1}}} & & {\scriptstyle 1_{P_1}}\downarrow & \swarrow_{s_0} & \downarrow{\scriptstyle 1_{P_0}} & \swarrow_{s_{-1}} & \downarrow{\scriptstyle 1_{\mathbb{Z}}} & & \\
P_{n+1} & \xrightarrow[\partial_{n+1}]{} & P_n & \xrightarrow[\partial_n]{} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_1 & \xrightarrow[\partial_1]{} & P_0 & \xrightarrow[\varepsilon]{} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

existen morfismos $s_n : P_n \to P_{n+1}$ tales que

$$\begin{aligned}
\partial_{n+1} \circ s_n + s_{n-1} \circ \partial_n &= 1_{P_n} \\
\partial_1 \circ s_0 + s_{-1} \circ \varepsilon &= 1_{P_0} \\
\varepsilon \circ s_{-1} &= 1_{\mathbb{Z}}
\end{aligned}$$

Estos morfismos se definen de la siguiente manera: $s_{-1} : \mathbb{Z} \to P_0$ está dado por $s_{-1}(1) = 1_G$ (el neutro de G) y para $n \geq 0$, $s_n : P_n \to P_{n+1}$ se define como

$$s_n(x_0, \ldots, x_n) = (1_G, x_0, \ldots, x_n).$$

Para $(x_0, \ldots, x_n) \in P_n$ y $x \in G$:

- $$\begin{aligned}
(\partial_{n+1} \circ s_n + s_{n-1} \circ \partial_n)(x_0, \ldots, x_n) &= (\partial_{n+1} \circ s_n)(x_0, \ldots, x_n) + (s_{n-1} \circ \partial_n)(x_0, \ldots, x_n) \\
&= \partial_{n+1}\big(s_n(x_0, \ldots, x_n)\big) + s_{n-1}\big(\partial_n(x_0, \ldots, x_n)\big) \\
&= \partial_{n+1}(1_G, x_0, \ldots, x_n) \\
&\quad + s_{n-1}\left(\sum_{j=0}^{n}(-1)^j(x_0, \ldots, \widehat{x}_j, \ldots, x_n)\right) \\
&= (x_0, \ldots, x_n) + \sum_{j=0}^{n}(-1)^{j-1}\big(1_G, x_0, \ldots, \widehat{x}_j, \ldots, x_n\big) \\
&\quad + \sum_{j=0}^{n}(-1)^j s_{n-1}\big(x_0, \ldots, \widehat{x}_j, \ldots, x_n\big) \\
&= (x_0, \ldots, x_n) + \sum_{j=0}^{n}(-1)^{j-1}\big(1_G, x_0, \ldots, \widehat{x}_j, \ldots, x_n\big) \\
&\quad + \sum_{j=0}^{n}(-1)^j\big(1_G, x_0, \ldots, \widehat{x}_j, \ldots, x_n\big) \\
&= (x_0, \ldots, x_n)
\end{aligned}$$

- $(\partial_1 \circ s_0 + s_{-1} \circ \varepsilon)(x) = \partial_1\big(s_0(x)\big) + s_{-1}\big(\varepsilon(x)\big) = \partial_1(1_G, x) + s_{-1}(1) = x - 1_G + 1_G = x$
- $(\varepsilon \circ s_{-1})(1) = \varepsilon\big(s_{-1}(1)\big) = \varepsilon(1) = 1$

□

A la sucesión

$$\mathbf{P}(G) : \cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

se le llama la ***resolución homogénea*** o ***estándar*** de $\mathbb{Z}$.

Ahora es el turno de presentar a nuestra segunda resolución proyectiva de $\mathbb{Z}$. Empezamos como sigue.

Sea G un grupo arbitrario, y sea B_0 el $\mathbb{Z}G$-módulo libre generado por un solo símbolo denotado por $[\ ]$, por lo tanto $B_0 \simeq \mathbb{Z}G$. Para $n \geq 1$, definimos a B_n como el $\mathbb{Z}G$-módulo libre con base G^n (de este modo cada B_n es proyectivo). Denotaremos a los elementos de G^n por $[x_1 \mid \ldots \mid x_n]$ en vez de $(x_1, \ldots, x_n)$. Para $n \geq 1$, los morfismos $d_n : B_n \to B_{n-1}$ están dados por

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

En particular,

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

Finalmente, $\varepsilon : B_0 \to \mathbb{Z}$ es el morfismo de aumento.

El siguiente Lema tiene como objetivo demostrar que esta sucesión es un complejo y que además es isomorfo al complejo $\mathbf{P}(G)$.

Lema 2.4.3. *Para todo $n \geq 0$, existe un isomorfismo de módulos $\tau_n : B_n \to P_n$ tal que*

$$\tau_{n-1} \circ d_n = \partial_n \circ \tau_n,$$

es decir, el siguiente diagrama conmuta.

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

Demostración. Definimos $\tau_n : B_n \to P_n$ como

$$\tau_n[x_1 \mid \ldots \mid x_n] = (1_G, x_1, x_1x_2, \ldots, x_1x_2 \cdots x_n)$$

cuya inversa $\sigma_n : P_n \to B_n$ está dada por

$$\sigma_n(1_G, x_1, \ldots, x_n) = \left[x_1 \mid x_1^{-1}x_2 \mid \ldots \mid x_{n-1}^{-1}x_n\right].$$

En efecto,

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

y

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

Para verificar la conmutatividad mostraremos que $d_n = \tau_{n-1}^{-1} \circ \partial_n \circ \tau_n = \sigma_{n-1} \circ \partial_n \circ \tau_n$.

$$\begin{aligned}(\sigma_{n-1} \circ \partial_n \circ \tau_n)[x_1 \mid \ldots \mid x_n] &= \sigma_{n-1}\Big(\partial_n\big(\tau_n[x_1 \mid \ldots \mid x_n]\big)\Big)\\ &= \sigma_{n-1}\big(\partial_n(1_G, x_1, x_1x_2, \ldots, x_1x_2\cdots x_n)\big)\\ &= \sigma_{n-1}\Bigg((x_1, x_1x_2, \ldots, x_1x_2\cdots x_n)\\ &\quad + \sum_{j=1}^{n-1}(-1)^j(1_G, x_1, \ldots, \widehat{x_1\cdots x_j}, \ldots, x_1x_2\cdots x_n)\\ &\quad + (-1)^n(1_G, x_1, x_1x_2, \ldots, x_1x_2\cdots x_{n-1})\Bigg)\\ &= \sigma_{n-1}(x_1, x_1x_2, \ldots, x_1x_2\cdots x_n)\\ &\quad + \sum_{j=1}^{n-1}(-1)^j\sigma_{n-1}(1_G, x_1, \ldots, \widehat{x_1\cdots x_j}, \ldots, x_1x_2\cdots x_n)\\ &\quad + (-1)^n\sigma_{n-1}(1_G, x_1, x_1x_2, \ldots, x_1x_2\cdots x_{n-1})\\ &= x_1\sigma_{n-1}(1_G, x_2, \ldots, x_2\cdots x_n)\\ &\quad + \sum_{j=1}^{n-1}(-1)^j\big[x_1 \mid \ldots \mid (x_1\cdots x_{j-1})^{-1}(x_1\cdots x_{j+1}) \mid \ldots \mid\\ &\qquad\qquad (x_1\cdots x_{n-1})^{-1}(x_1\cdots x_n)\big]\\ &\quad + (-1)^n[x_1 \mid x_2 \mid \ldots \mid x_{n-1}]\end{aligned}$$

$$\begin{aligned}
&= x_1[x_2 \mid x_3 \mid \ldots \mid x_n] \\
&\quad + \sum_{j=1}^{n-1} (-1)^j [x_1 \mid \ldots \mid x_j x_{j+1} \mid \ldots \mid x_n] \\
&\quad + (-1)^n [x_1 \mid x_2 \mid \ldots \mid x_{n-1}] \\
&= d_n[x_1 \mid x_2 \mid \ldots \mid x_n]
\end{aligned}$$

Por lo tanto, $\tau_{n-1} \circ d_n = \partial_n \circ \tau_n$. □

Proposición 2.4.4. *Sea G un grupo. La sucesión de $\mathbb{Z}G$-módulos libres*

$$\boldsymbol{B}(G) : \cdots \longrightarrow B_n \xrightarrow{d_n} B_{n-1} \longrightarrow \cdots \longrightarrow B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

es exacta.

Demostración. $\mathbf{B}(G)$ es un complejo ya que

a) $\varepsilon \circ d_1[x] = \varepsilon\big(x[\,] - [\,]\big) = x\varepsilon[\,] - \varepsilon[\,] = \varepsilon[\,] - \varepsilon[\,] = 0$

b) Si $n \geq 1$, por el Lema 2.4.3,

$$\begin{aligned}
d_n \circ d_{n+1} &= \big(\tau_{n-1}^{-1} \circ \partial_n \circ \tau_n\big) \circ \big(\tau_n^{-1} \circ \partial_{n+1} \circ \tau_{n+1}\big) \\
&= \tau_{n-1}^{-1} \circ \partial_n \circ \big(\tau_n \circ \tau_n^{-1}\big) \circ \partial_{n+1} \circ \tau_{n+1} \\
&= \tau_{n-1}^{-1} \circ \partial_n \circ 1_{B_n} \circ \partial_{n+1} \circ \tau_{n+1} \\
&= \tau_{n-1}^{-1} \circ \big(\partial_n \circ \partial_{n+1}\big) \circ \tau_{n+1} \\
&= 0
\end{aligned}$$

Finalmente, como los cuadrados del Lema 2.4.3 conmutan, la familia

$$\tau = (\tau_n) : \mathbf{B}(G) \to \mathbf{P}(G)$$

es un isomorfismo de complejos, y por lo tanto induce isomorfismos en la cohomología de los complejos $\mathbf{B}(G)$ y $\mathbf{P}(G)$, pero $\mathbf{P}(G)$ es exacto, entonces para todo $n \geq 0$

$$H^n(\mathbf{B}(G)) \simeq H^n(\mathbf{P}(G)) = 0,$$

es decir, $\mathbf{B}(G)$ es una sucesión exacta. □

A la sucesión

$$\mathbf{B}(G) : \cdots \longrightarrow B_n \xrightarrow{d_n} B_{n-1} \longrightarrow \cdots \longrightarrow B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

se le llama la ***resolución barra*** de $\mathbb{Z}$.

2.5. Resolución barra normalizada

A continuación construimos la *resolución barra normalizada* de $\mathbb{Z}$, la cual usaremos en el *Capítulo* 4 para interpretar al segundo grupo de cohomología $H^2(G, M)$.

Sea G un grupo, para todo entero $n \geq 1$, sea

$$Y_n = \Big\{ [x_1 \mid \ldots \mid x_n] \in G^n : \textit{ al menos un } x_i = 1_G \Big\}$$

Definimos a U_0 como el submódulo cero de B_0 y para $n \geq 1$ sea U_n el $\mathbb{Z}G$-módulo generado por Y_n. Claramente U_n es un submódulo de B_n y además $d_n(U_n) \subseteq U_{n-1}$ para todo $n \geq 1$, para verificar esto último, basta ver que $d_n(Y_n) \subseteq U_{n-1}$.

Ya que $d_1[1_G] = 1_G \cdot [\ ] - [\ ] = 0$, entonces

$$d_1(Y_1) = \{0\} = U_0.$$

Si $n \geq 1$ y $[x_1 \mid \ldots \mid x_n] \in Y_n$, podemos considerar los siguientes dos casos.

Caso 1. Al menos dos entradas son iguales a 1_G, entonces

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

tiene al menos una entrada igual a 1_G en cada sumando.

Caso 2. Una sola entrada es igual a 1_G. Si $x_1 = 1_G$, entonces

$$\begin{aligned} d_n[1_G \mid x_2 \mid \ldots \mid x_n] &= [x_2 \mid \ldots \mid x_n] - [x_2 \mid \ldots \mid x_n] \\ &\quad + \sum_{i=2}^{n-1} (-1)^i [1_G \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n] \\ &\quad + (-1)^n [1_G \mid \ldots \mid x_{n-1}] \\ &= \sum_{i=2}^{n-1} (-1)^i [1_G \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n] \\ &\quad + (-1)^n [1_G \mid \ldots \mid x_{n-1}] \end{aligned}$$

el cual tiene exactamente una entrada igual a 1_G en cada sumando. Si $x_n = 1_G$,

entonces

$$\begin{aligned} d_n[x_1 \mid x_2 \mid \ldots \mid 1_G] &= x_1[x_2 \mid \ldots \mid 1_G] \\ &\quad + \sum_{i=1}^{n-2}(-1)^i[x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid 1_G] \\ &\quad + (-1)^{n-1}[x_1 \mid \ldots \mid x_{n-1}] + (-1)^n[x_1 \mid \ldots \mid x_{n-1}] \\ &= x_1[x_2 \mid \ldots \mid 1_G] \\ &\quad + \sum_{i=1}^{n-2}(-1)^i[x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid 1_G] \end{aligned}$$

el cual también tiene una entrada igual a 1_G en cada sumando. Finalmente, si $x_j = 1_G$ para $1 < j < n$, entonces los términos que no tienen ninguna entrada igual a 1_G son exactamente dos, a saber,

$$(-1)^{j-1}[x_1 \mid \ldots \mid x_{j-1}x_j \mid \ldots \mid x_n] = (-1)^{j-1}[x_1 \mid \ldots \mid x_{j-1} \mid \ldots \mid x_n]$$

y

$$(-1)^{j}[x_1 \mid \ldots \mid x_j x_{j+1} \mid \ldots \mid x_n] = (-1)^{j}[x_1 \mid \ldots \mid x_{j+1} \mid \ldots \mid x_n]$$

los cuales se cancelan.

Se tiene entonces que la sucesión

$$\mathbf{U}(G) : \cdots \longrightarrow U_n \xrightarrow{s_n} U_{n-1} \longrightarrow \cdots \longrightarrow U_1 \xrightarrow{s_1} U_0 \longrightarrow 0$$

donde $s_n = d_n|_{U_n}$ es un subcomplejo de $\mathbf{B}(G)$, por lo que podemos considerar el complejo cociente $\mathbf{B}(G)/\mathbf{U}(G)$.

Definición 2.5.1. Sea G un grupo. La ***resolución barra normalizada*** de $\mathbb{Z}$ es la sucesión

$$\mathbf{B}^*(G) : \cdots \longrightarrow B_n/U_n \xrightarrow{r_n} B_{n-1}/U_{n-1} \longrightarrow \cdots \longrightarrow B_1/U_1 \xrightarrow{r_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

donde los morfismos $r_n : B_n/U_n \to B_{n-1}/U_{n-1}$ están dados por

$$r_n(x + U_n) = d_n(x) + U_{n-1}$$

para todo $x \in B_n$. En particular,

$$r_n\big([x_1 \mid x_2 \mid \ldots \mid x_n] + U_n\big) = d_n[x_1 \mid x_2 \mid \ldots \mid x_n] + U_{n-1}$$

Proposición 2.5.2. *Para cada $n \geq 1$, B_n/U_n es un $\mathbb{Z}G$-módulo libre con base el conjunto*

$$X_n = \Big\{[x_1 \mid \ldots \mid x_n] + U_n \in B_n/U_n : x_i \in G \setminus \{1_G\} \text{ para todo } i\Big\}.$$

Demostración. Primero veamos que el conjunto es linealmente independiente. Para $i = 1, \dots, m$ sean $\alpha_i \in \mathbb{Z}G$ y $[x_{i_1} \mid \dots \mid x_{i_n}] + U_n \in X_n$ tales que

$$\begin{aligned} 0 &= \sum_{i=1}^{m} \big(\alpha_i [x_{i_1} \mid \dots \mid x_{i_n}] + U_n\big) \\ &= \left(\sum_{i=1}^{m} \alpha_i [x_{i_1} \mid \dots \mid x_{i_n}]\right) + U_n \end{aligned}$$

entonces $\sum_{i=1}^{m} \alpha_i [x_{i_1} \mid \dots \mid x_{i_n}] \in U_n = \langle Y_n \rangle$ y así $\sum_{i=1}^{m} \alpha_i [x_{i_1} \mid \dots \mid x_{i_n}] = \sum_{j=1}^{k} \beta_j [y_{j_1} \mid \dots \mid y_{j_n}]$ con $\beta_j \in \mathbb{Z}G$ y $[y_{j_1} \mid \dots \mid y_{j_n}] \in Y_n$. Luego

$$\sum_{i=1}^{m} \alpha_i [x_{i_1} \mid \dots \mid x_{i_n}] - \sum_{j=1}^{k} \beta_j [y_{j_1} \mid \dots \mid y_{j_n}] = 0$$

y como B_n es libre sobre G^n se tiene que $\alpha_i = 0$ para todo i. Finalmente, si $\sum_{G^n} \alpha_{(x_1,\dots,x_n)} [x_1 \mid x_2 \mid \dots \mid x_n] \in B_n$, entonces

$$\begin{aligned} \left(\sum_{G^n} \alpha_{(x_1,\dots,x_n)} [x_1 \mid x_2 \mid \dots \mid x_n]\right) + U_n &= \sum_{G^n} \Big(\alpha_{(x_1,\dots,x_n)} [x_1 \mid x_2 \mid \dots \mid x_n] + U_n\Big) \\ &= \sum_{(G^\times)^n} \Big(\alpha_{(x_1,\dots,x_n)} [x_1 \mid x_2 \mid \dots \mid x_n] + U_n\Big) \end{aligned}$$

donde $G^\times = G \setminus \{1_G\}$, y esto último se tiene porque $[x_1 \mid x_2 \mid \dots \mid x_n] + U_n = 0$ si $x_i = 1_G$ para algún i. Por lo tanto X_n genera a B_n/U_n. □

Lema 2.5.3. *Para cada $n \geq 1$, B_n/U_n es un $\mathbb{Z}$-módulo libre con base el conjunto*

$$Z_n = \Big\{ x[x_1 \mid \dots \mid x_n] + U_n \in B_n/U_n : x \in G, x_i \in G \setminus \{1_G\} \text{ para todo } i \Big\}.$$

Demostración. Primero veremos que Z_n genera a B_n/U_n como grupo abeliano. Un elemento $p \in B_n$ es de la forma

$$p = \sum_{G^n} \alpha_{(x_1,\dots,x_n)} [x_1 \mid \dots \mid x_n]$$

donde $\alpha_{(x_1,\dots,x_n)} \in \mathbb{Z}G$ son casi todos ceros. Por otro lado, para cada $(x_1, \dots, x_n) \in G^n$

$$\alpha_{(x_1,\dots,x_n)} = \sum_{x \in G} r_x^{(x_1,\dots,x_n)} x$$

con $r_x^{(x_1,\ldots,x_n)} \in \mathbb{Z}$. Por lo tanto

$$\begin{aligned} p + U_n &= \left(\sum_{G^n} \alpha_{(x_1,\ldots,x_n)}[x_1 \mid \ldots \mid x_n]\right) + U_n \\ &= \sum_{G^n} \big(\alpha_{(x_1,\ldots,x_n)}[x_1 \mid \ldots \mid x_n] + U_n\big) \\ &= \sum_{G^n} \left(\left(\sum_{G} r_x^{(x_1,\ldots,x_n)} x\right)[x_1 \mid \ldots \mid x_n] + U_n\right) \\ &= \sum_{\substack{x\in G \\ (x_1,\ldots,x_n)\in G^n}} r_x^{(x_1,\ldots,x_n)} \big(x[x_1 \mid \ldots \mid x_n] + U_n\big) \\ &= \sum_{\substack{x\in G \\ (x_1,\ldots,x_n)\in (G^\times)^n}} r_x^{(x_1,\ldots,x_n)} \big(x[x_1 \mid \ldots \mid x_n] + U_n\big) \end{aligned}$$

donde $G^\times = G \setminus \{1_G\}$, esto ultimo se tiene pues $[x_1 \mid \ldots \mid x_n] + U_n = 0$ si $x_i = 1_G$ para algun i. Se sigue que $p + U_n \in \langle Z_n \rangle$. Ahora veremos que el conjunto es linealmente independiente. Para $i = 1, \ldots, m$ sean $r_i \in \mathbb{Z}$, $y_i \in G$ y $[x_{i_1} \mid \ldots \mid x_{i_n}] \in G^n$ tal que $x_{i_j} \neq 1_G$ para todo i, j. Si

$$\begin{aligned} 0 &= \sum_{i=1}^{m} r_i \big(y_i[x_{i_1} \mid \ldots \mid x_{i_n}] + U_n\big) \\ &= \sum_{i=1}^{m} \big(r_i y_i[x_{i_1} \mid \ldots \mid x_{i_n}] + U_n\big) \\ &= \left(\sum_{i=1}^{m} r_i y_i[x_{i_1} \mid \ldots \mid x_{i_n}]\right) + U_n \end{aligned}$$

entonces $\sum_{i=1}^{m} r_i y_i[x_{i_1} \mid \ldots \mid x_{i_n}] \in U_n = \langle Y_n \rangle$, luego
$\sum_{i=1}^{m} r_i y_i[x_{i_1} \mid \ldots \mid x_{i_n}] = \sum_{j=1}^{k} \beta_j[z_{j_1} \mid \ldots \mid z_{j_n}]$ y así

$$\sum_{i=1}^{m} r_i y_i[x_{i_1} \mid \ldots \mid x_{i_n}] - \sum_{j=1}^{k} \beta_j[z_{j_1} \mid \ldots \mid z_{j_n}] = 0$$

Se sigue que $r_i y_i = 0$ para todo i, pues B_n es un $\mathbb{Z}G$-módulo libre sobre G^n y por lo tanto $r_i = 0$ para cada i. □

Lema 2.5.4. *Si*

$$(C_\bullet, d_\bullet) : \cdots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots$$

es un complejo de R-módulos y $\{s_n : C_n \to C_{n+1}\}_{n\in\mathbb{Z}}$ es una familia de $\mathbb{Z}$-morfismos que satisfacen

$$d_{n+1}s_n + s_{n-1}d_n = 1_{C_n}$$

para todo $n \in \mathbb{Z}$, entonces $(C_\bullet, d_\bullet)$ es una sucesión exacta.

Demostración. Ya que $(C_\bullet, d_\bullet)$ es un complejo, $d_n d_{n+1} = 0$ y así $Im(d_{n+1}) \subseteq Ker(d_n)$. Recíprocamente, si $a \in Ker(d_n)$ entonces

$$\begin{aligned} a &= \big(d_{n+1}s_n + s_{n-1}d_n\big)(a) \\ &= d_{n+1}\big(s_n(a)\big) + s_{n-1}\big(d_n(a)\big) \\ &= d_{n+1}\big(s_n(a)\big) + s_{n-1}\big(0\big) \\ &= d_{n+1}\big(s_n(a)\big) + 0 \\ &= d_{n+1}\big(s_n(a)\big) \end{aligned}$$

por lo tanto $a = d_{n+1}\big(s_n(a)\big) \in Im(d_{n+1})$. □

Proposición 2.5.5. *Sea G un grupo. La resolución barra normalizada*

$$\boldsymbol{B}^*(G) : \cdots \longrightarrow B_n/U_n \xrightarrow{r_n} B_{n-1}/U_{n-1} \longrightarrow \cdots \longrightarrow B_1/U_1 \xrightarrow{r_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

es una $\mathbb{Z}G$-resolución libre de $\mathbb{Z}$.

Demostración. Por la Proposición 2.5.2 cada uno de los $\mathbb{Z}G$-módulos B_n/U_n es $\mathbb{Z}G$-libre. Para probar la exactitud de $\mathbf{B}^*(G)$, por el Lema 2.5.4, basta construir una familia $\{s_n : B_n/U_n \to B_{n+1}/U_{n+1}\}_{n\geq -1}$ de $\mathbb{Z}$-morfismos que satisfagan

$$\begin{aligned} \varepsilon s_{-1} &= 1_{\mathbb{Z}} \\ r_1 s_0 + s_{-1}\varepsilon &= 1_{B_0} \\ r_{n+1}s_n + s_{n-1}r_n &= 1_{B_n/U_n} \end{aligned}$$

Estos morfismos se definen en la base de la siguiente manera: $s_{-1} : \mathbb{Z} \to B_0$ como

$$s_{-1}(1) = [\ ],$$

$s_0 : B_0 \to B_1/U_1$ como

$$s_0\big(x[\ ]\big) = [x] + U_1$$

y para $n \geq 1$, $s_n : B_n/U_n \to B_{n+1}/U_{n+1}$ como

$$s_n : \big(x[x_1 \mid \ldots \mid x_n] + U_n\big) = [x \mid x_1 \mid \ldots \mid x_n] + U_{n+1}$$

Para facilitar la notación denotaremos por $[x_1 \mid \ldots \mid x_n]^* = [x_1 \mid \ldots \mid x_n] + U_n$. Entonces

- $$\begin{aligned}(r_{n+1}s_n + s_{n-1}r_n)\big(x[x_1 \mid \ldots \mid x_n]^*\big) &= r_{n+1}s_n\big(x[x_1 \mid \ldots \mid x_n]^*\big) \\ &\quad + s_{n-1}r_n\big(x[x_1 \mid \ldots \mid x_n]^*\big) \\ &= r_{n+1}[x \mid x_1 \mid \ldots \mid x_n]^* + s_{n-1}\big(xr_n[x_1 \mid \ldots \mid x_n]^*\big) \\ &= x[x_1 \mid \ldots \mid x_n]^* - [xx_1 \mid x_2 \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{i+1}\sum_{i=1}^{n-1}[x \mid \ldots \mid x_ix_{i+1} \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{n+1}[x \mid x_1 \mid \ldots \mid x_{n-1}]^* \\ &\quad + s_{n-1}\Bigg(xx_1[x_2 \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{i}\sum_{i=1}^{n-1}x[x_1 \mid \ldots \mid x_ix_{i+1} \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{n}x[x_1 \mid \ldots \mid x_{n-1}]^*\Bigg) \\ &= x[x_1 \mid \ldots \mid x_n]^* - [xx_1 \mid x_2 \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{i+1}\sum_{i=1}^{n-1}[x \mid \ldots \mid x_ix_{i+1} \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{n+1}[x \mid x_1 \mid \ldots \mid x_{n-1}]^* \\ &\quad + s_{n-1}\Big(xx_1[x_2 \mid \ldots \mid x_n]^*\Big) \\ &\quad + (-1)^{i}\sum_{i=1}^{n-1}s_{n-1}\Big(x[x_1 \mid \ldots \mid x_ix_{i+1} \mid \ldots \mid x_n]^*\Big) \\ &\quad + (-1)^{n}s_n\Big(x[x_1 \mid \ldots \mid x_{n-1}]^*\Big) \\ &= x[x_1 \mid \ldots \mid x_n]^* - [xx_1 \mid x_2 \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{i+1}\sum_{i=1}^{n-1}[x \mid x_1 \mid \ldots \mid x_ix_{i+1} \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{n+1}[x \mid x_1 \mid \ldots \mid x_{n-1}]^* \\ &\quad + [xx_1 \mid x_2 \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{i}\sum_{i=1}^{n-1}[x \mid x_1 \mid \ldots \mid x_ix_{i+1} \mid \ldots \mid x_n]^* \\ &\quad + (-1)^{n}[x \mid x_1 \mid \ldots \mid x_{n-1}]^* \\ &= x[x_1 \mid \ldots \mid x_n]^*\end{aligned}$$

- $$\begin{aligned}(r_1 s_0 + s_{-1}\varepsilon)\big(x[\ ]\big) &= r_1 s_0\big(x[\ ]\big) + s_{-1}\varepsilon\big(x[\ ]\big)\\ &= r_1[x]^* + s_{-1}(1)\\ &= \big(x[\ ] - [\ ]\big) + [\ ]\\ &= x[\ ]\end{aligned}$$

- $$\begin{aligned}(\varepsilon s_{-1})(1) &= \varepsilon s_{-1}(1)\\ &= \varepsilon[\ ]\\ &= 1\end{aligned}$$

□

Capítulo 3

Extensiones de grupos y $H^2(G, M)$

Describir a cada uno de los grupos $H^n(G, M)$ cuando G no es cíclico, en términos de grupos más simples, se vuelve una tarea muy complicada. En algunos casos, por ejemplo, para $H^2(G, M)$ se pueden dar interpretaciones relativamente sencillas y este será el objetivo de este capítulo. Empezaremos por desarrollar los conceptos y resultados necesarios que nos permitirán dar una interpretación del segundo grupo de cohomología $H^2(G, M)$, en términos de clases de extensiones de M por G que preservan la acción. Para ello comenzamos explicando de manera muy breve en que consiste el "*problema de la extensión*".

3.1. Extensiones de grupos

Dada una pareja de grupos (M, G), el *problema de la extensión* consiste en encontrar a todos los grupos E que contengan un subgrupo normal M_1 isomorfo a M de tal modo que el grupo G sea isomorfo al grupo cociente E/M_1, es decir, lo que queremos es que E esté en una sucesión exacta de la forma:

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1.$$

Lo anterior da origen a la siguiente definición.

Definición 3.1.1. Si M y G son grupos, entonces una ***extensión*** de M por G es una sucesión exacta corta

$$1 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1.$$

En el problema de la extensión no asumimos que el grupo M sea abeliano, sin embargo para nuestros fines M siempre será considerado un grupo abeliano y estará escrito aditivamente. Los grupos E y G no necesariamente son abelianos y ambos se escribirán multiplicativamente. Una característica especial de considerar a M abeliano es que una extensión

$$0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$$

induce una acción de G sobre M, haciendo de M un G-módulo. Empezaremos con los conceptos necesarios para demostrar esta última afirmación.

Definición 3.1.2. Sea $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión. Una ***sección*** es una función $s : G \to E$, no necesariamente un morfismo, tal que $p \circ s = 1_G$ y $s(1) = 1$.

Ya que $p : E \to G$ es suprayectiva, el axioma de elección garantiza la existencia de una inversa derecha, es decir, de una función $r : G \to E$ tal que $p \circ r = 1_G$. Si $r(1) = 1$, entonces r es una sección. Si $r(1) \neq 1$, entonces podemos definir $s : G \to E$ como

$$s(x) = \begin{cases} r(x) & \textit{si } x \neq 1 \\ 1 & \textit{si } x = 1 \end{cases}$$

y claramente $p \circ s = 1_G$. Por lo tanto, siempre es posible hallar una sección.

Proposición 3.1.3. *Sean $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión y $s : G \to E$ una sección. Si $M' = Im(i)$, entonces $s(G)$ es un sistema completo de representantes de clases laterales derechas de M' en E.*

Demostración. Sea $e \in E$, entonces $x = p(e) \in G$ y

$$p\big(s(x)e^{-1}\big) = ps(x)p(e)^{-1} = xx^{-1} = 1,$$

se sigue que $s(x)e^{-1} \in Ker(p) = Im(i) = M'$ y por lo tanto $M's(x) = M'e$, esto es, toda clase lateral derecha tiene un representante en $s(G)$. Ahora mostraremos que $s(G)$ no tiene dos elementos de la misma clase. Si $M's(x) = M's(y)$, entonces existe $a \in M'$ tal que $s(x) = as(y)$, así

$$x = ps(x) = p\big(as(y)\big) = p(a)p\big(s(y)\big) = ps(y) = y$$

donde la penúltima igualdad se tiene porque $a \in M' = Im(i) = Ker(p)$, por lo tanto $s(x) = s(y)$. □

Si $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ es una extensión de un grupo M por un grupo G, entonces $Im(i) = Ker(p) \lhd E$, por lo tanto, si $s : G \to E$ es una sección tenemos que para cada $x \in G$ y $a \in M$ $s(x)i(a)s(x)^{-1} \in Im(i)$, luego existe un único $b_x \in M$ tal que $i(b_x) = s(x)i(a)s(x)^{-1}$. Denotaremos por $\theta_x(a) = b_x$.

Proposición 3.1.4. *Sea $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión de un grupo M por un grupo G. Si $s : G \to E$ es una sección, entonces:*

a) Para todo $x \in G$, la función $\theta_x : M \to M$, donde $\theta_x(a)$ es el único elemento en M tal que

$$i\big(\theta_x(a)\big) = s(x)i(a)s(x)^{-1},$$

es independiente de la elección de la sección s en x.

b) Para todo $x \in G$, $\theta_x : M \to M$ es un isomorfismo de grupos.

c) La función $\theta : G \to \mathbf{Aut}(M)$, definida por $\theta(x) = \theta_x$, es un morfismo de grupos.

d) M *es un* G*-módulo izquierdo con la acción dada por*

$$x \cdot a = \theta_x(a).$$

Demostración.

a) Sea r otra sección y sea $a \in M$. Ya que

$$p\big(s(x)^{-1}r(x)\big) = ps(x)^{-1}pr(x) = x^{-1}x = 1,$$

$s(x)^{-1}r(x) \in \mathit{Ker}(p) = \mathit{Im}(i)$, por lo tanto existe $c \in M$ tal que $s(x)^{-1}r(x) = i(c)$. Se sigue que $r(x) = s(x)i(c)$. Luego,

$$r(x)i(a)r(x)^{-1} = s(x)i(c)i(a)i(c)^{-1}s(x)^{-1} = s(x)i(c+a-c)s(x)^{-1} = s(x)i(a)s(x)^{-1}$$

donde la última igualdad se tiene porque a, c conmutan en el grupo abeliano M.

b) Sean $a, b \in M$ y $x \in G$. Tenemos que

$$\begin{aligned} i\big(\theta_x(a) + \theta_x(b)\big) &= i\big(\theta_x(a)\big)i\big(\theta_x(b)\big) \\ &= s(x)i(a)s(x)^{-1}s(x)i(b)s(x)^{-1} \\ &= s(x)i(a)i(b)s(x)^{-1} \\ &= s(x)i(a+b)s(x)^{-1} \\ &= i\big(\theta_x(a+b)\big) \end{aligned}$$

y por lo tanto $\theta_x(a+b) = \theta_x(a) + \theta_x(b)$.

c) Sean $x, y \in G$ y $a \in M$, ya que

$$p\big(s(y)^{-1}s(x)^{-1}s(xy)\big) = ps(y)^{-1}ps(x)^{-1}ps(xy) = y^{-1}x^{-1}xy = 1,$$

$s(y)^{-1}s(x)^{-1}s(xy) \in \mathit{Ker}(p) = \mathit{Im}(i)$, así $s(y)^{-1}s(x)^{-1}s(xy) = i(c)$ para algún $c \in M$. Por lo tanto $s(xy) = s(x)s(y)i(c)$. Finalmente,

$$\begin{aligned} i\big(\theta_{xy}(a)\big) &= s(xy)i(a)s(xy)^{-1} \\ &= s(x)s(y)i(c)i(a)i(c)^{-1}s(y)^{-1}s(x)^{-1} \\ &= s(x)s(y)i(c+a-c)s(y)^{-1}s(x)^{-1} \\ &= s(x)s(y)i(a)s(y)^{-1}s(x)^{-1} \\ &= s(x)i\big(\theta_y(a)\big)s(x)^{-1} \\ &= i\Big(\theta_x\big(\theta_y(a)\big)\Big) \\ &= i\big(\theta_x\theta_y(a)\big) \end{aligned}$$

se sigue que $\theta(xy) = \theta_{xy} = \theta_x\theta_y = \theta(x)\theta(y)$.

d) Se sigue del inciso *c)* y de la Proposición 2.1.2.

□

Sean G un grupo y M un G-módulo. Ya que tanto M como G son grupos podemos hablar de las extensiones de M por G y como un ejemplo de dicha extensión podemos considerar el producto directo de M por G, esto es, el conjunto de parejas ordenadas $(a, x) \in M \times G$ en donde la operación está dada por

$$(a, x)(b, y) = (a + b, xy).$$

Este grupo tiene como neutro a $(0, 1)$ y como inverso de (a, x) a $(-a, x^{-1})$. El monomorfismo $i : M \to M \times G$ definido por $i(a) = (a, 1)$ y el epimorfismo $p : M \times G \to G$ definido por $p(a, x) = x$ satisfacen que la $Im(i) = Ker(p)$ y por lo tanto la sucesión

$$0 \longrightarrow M \xrightarrow{i} M \times G \xrightarrow{p} G \longrightarrow 1$$

es, en efecto, una extensión de M por G. Por el inciso *d)* de la Proposición 3.1.4 esta extensión induce una acción $* : G \times M \to M$, haciendo de M un G-módulo, y es natural preguntarnos si esta acción coincide con la que M tenía en un principio. Para responder a esta pregunta consideremos la sección $s : G \to M \times G$ definida por $s(x) = (0, x)$. Realizando los siguientes calculos, tenemos que para todo $x \in G$ y $a \in M$

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

y podemos concluir que $x * a = a$, es decir, M con esta nueva acción es un G-módulo trivial y es de esperarse que en general no coincida con la que M tenía. Nosotros nos centraremos únicamente en aquellas extensiones cuyas dos acciones coincidan, por lo que conviene dar un nombre a este tipo de extensiones.

Definición 3.1.5. Sea M un G-módulo. Una extensión $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ preserva la acción si, para todo $x \in G$ y $a \in M$

$$i(x \cdot a) = s(x)i(a)s(x)^{-1},$$

donde $s : G \to E$ es una sección.

Para que esta definición realmente tenga sentido será necesario demostrar la existencia de este tipo de extensiones. El estudio del producto semidirecto de un G-módulo M nos dará un primer ejemplo de estas extensiones, para ello empezamos recordando lo que esto significa.

3.2. Productos Semidirectos

El concepto de producto semidirecto es una generalización del producto directo, al igual que en este último, los productos semidirectos describen una forma muy particular en la que un grupo está compuesto por dos grupos.

Definición 3.2.1. Una extensión $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ se ***escinde*** si existe un morfismo $s : G \to E$ tal que $p \circ s = 1_G$.

Entonces una extensión se escinde si y sólo si existe una sección, digamos s, que también es un morfismo. Por ejemplo, la extensión

$$0 \longrightarrow M \xrightarrow{i} M \times G \xrightarrow{p} G \longrightarrow 1$$

se escinde, ya que la sección $s : G \to M \times G$ dada por $s(x) = (0, x)$ es un morfismo.

Proposición 3.2.2. *Las siguientes condiciones son equivalentes.*

a) La extensión $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ *se escinde.*

b) Existe un subgrupo $Q \subseteq E$ *tal que* $Q \simeq G$, $i(M) \cap Q = 1$ *y* $i(M)Q = E$.

c) Existe un subgrupo $Q \subseteq E$ *tal que todo elemento* $e \in E$ *se expresa de manera única como* $e = i(a)x$ *con* $a \in M$ *y* $x \in Q$.

Demostración.

a) $\Rightarrow$ *b)* Por hipótesis existe un morfismo $s : G \to E$ tal que $ps = 1_G$, lo que implica que s es inyectiva y así $Q := Im(s) \simeq G$. Si $e \in E$, entonces $y = p(e) \in G$ y $ps(y) = y = p(e)$ por lo tanto $es(y)^{-1} \in Ker(p) = i(M)$, luego $e = i(a)s(y)$ para algún $a \in M$, es decir, $e \in i(M)Q$. Finalmente, si $e \in i(M) \cap Q$, entonces $e = i(a)$ para algún $a \in M$ y $e = s(x)$ para algún $x \in G$ pues $e \in Q = Im(s)$. Por otro lado, $x = ps(x) = p(e) = pi(a) = 1$, se sigue que $e = s(x) = s(1) = 1$.

b) $\Rightarrow$ *c)* Supongamos que tenemos dos expresiones de e, digamos

$$i(a)x = e = i(b)y$$

con $a, b \in M$ y $x, y \in Q$, entonces $i(-b+a) = i(b)^{-1}i(a) = yx^{-1} \in i(M) \cap Q = \{1\}$. Por lo tanto $a = b$ y $x = y$.

c) $\Rightarrow$ *a)* Veamos que $p\,|_Q \colon Q \to G$ es un isomorfismo. Sean $x, y \in Q$ tales que $p(x) = p(y)$, entonces $xy^{-1} \in Ker(p) = i(M)$ y así $xy^{-1} = i(a)$ para algún $a \in M$. Tenemos las siguientes dos expresiones de $x \in E$ como

$$i(0)x = 1x = x = \left(xy^{-1}\right)y = i(a)y$$

de la unicidad se sigue que $x = y$ y por lo tanto $p|_Q$ es un monomorfismo. Por otro lado, si $z \in G$, existe $e \in E$ tal que $p(e) = z$, pues p es un epimorfismo. Por hipótesis $e = i(a)x$ con $a \in M$ y $x \in Q$, se sigue que

$$z = p(e) = p\big(i(a)x\big) = pi(a)p(x) = 1p(x) = p(x),$$

es decir, $p\,|_Q$ es suprayectiva. Si $s : G \to Q \subseteq E$ es el inverso de $p\,|_Q$ entonces $p \circ s = 1_G$ y así la sucesión se escinde.

□

Definición 3.2.3. Diremos que un grupo E es ***producto semidirecto*** de M por G si se satisface alguna de las condiciones de la Proposición 3.2.2.

De la definición anterior tenemos que si M y G son grupos, entonces el producto directo $M \times G$ es un producto semidirecto. A continuación mostraremos otra manera de construir un producto semidirecto de M por G si M es un G-módulo.

Definición 3.2.4. Sean G un grupo y M un G-módulo. Definimos el producto semidirecto de M por G denotado $M \rtimes G$ como el conjunto cuyos elementos son parejas ordenadas $(a, x) \in M \times G$, junto con la siguiente operación

$$(a, x)(b, y) = (a + x \cdot b, xy)$$

Desde luego, este conjunto con esta operación resulta ser un grupo.

Proposición 3.2.5. *Sean G un grupo y M un G-módulo, entonces $M \rtimes G$ es un grupo.*

Demostración. Sean (a, x), (b, y) y $(c, z) \in M \rtimes G$.
La operación es asociativa

$$\begin{aligned}
\big((a, x)(b, y)\big)(c, z) &= (a + x \cdot b, xy)(c, z) \\
&= \big(a + x \cdot b + (xy) \cdot c, (xy)z\big) \\
&= \big(a + x \cdot b + x \cdot (y \cdot c), x(yz)\big) \\
&= \big(a + x \cdot (b + y \cdot c), x(yz)\big) \\
&= (a, x)(b + y \cdot c, yz) \\
&= (a, x)\big((b, y)(c, z)\big)
\end{aligned}$$

El elemento $(0, 1) \in M \rtimes G$ es el neutro de la operación

$$\begin{aligned}
(a, x)(0, 1) &= (a + x \cdot 0, x1) \\
&= (a, x)
\end{aligned}$$

y

$$\begin{aligned}
(0, 1)(a, x) &= (0 + 1 \cdot a, 1x) \\
&= (a, x)
\end{aligned}$$

El inverso de (a, x) es $\big(-(x^{-1} \cdot a), x^{-1}\big)$

$$\begin{aligned}(a, x)\big(-(x^{-1} \cdot a), x^{-1}\big) &= \big(a - x \cdot (x^{-1} \cdot a), xx^{-1}\big)\\ &= (a - 1 \cdot a, 1)\\ &= (0, 1)\end{aligned}$$

y

$$\begin{aligned}\big(-(x^{-1} \cdot a), x^{-1}\big)(a, x) &= \big(-(x^{-1} \cdot a) + x^{-1} \cdot a, x^{-1}x\big)\\ &= (0, 1)\end{aligned}$$

□

Los morfismos canónicos $j : M \to M \rtimes G$ y $\pi : M \rtimes G \to G$ que se definen como $j(a) = (a, 1)$ y $\pi(a, x) = x$ resultan ser monomorfismo y epimorfismo respectivamente. Además, la $Im(j) = \big\{(a, 1) : a \in M\big\} = Ker(\pi)$ de modo que la sucesión

$$\varepsilon : 0 \longrightarrow M \xrightarrow{j} M \rtimes G \xrightarrow{\pi} G \longrightarrow 1$$

resulta ser una extensión de M por G. Esta extensión, al igual que en el producto directo, se escinde y además tiene la propiedad adicional de preservar la acción. La siguiente Proposición demuestra lo dicho anteriormente y resuelve la incógnita acerca de la existencia de extensiones que preservan la acción.

Proposición 3.2.6. *Sean G un grupo y M un G-módulo. La extensión*

$$\varepsilon : 0 \longrightarrow M \xrightarrow{j} M \rtimes G \xrightarrow{\pi} G \longrightarrow 1$$

se escinde y preserva la acción.

Demostración. Primero veamos que la sucesión se escinde. Definimos $s : G \to M \rtimes G$ como

$$s(x) = (0, x).$$

Si $x, y \in G$, entonces

$$s(x)s(y) = (0, x)(0, y) = (0 + x \cdot 0, xy) = (0, xy) = s(xy),$$

es decir, s es un morfismo. Además $(\pi \circ s)(x) = \pi\big(s(x)\big) = \pi(0, x) = x$, por lo tanto $\pi \circ s = 1_G$ y la extensión se escinde.

Ahora veamos que la extensión preserva la acción, para ello obsérvese que toda sección $r : G \to M \rtimes G$ es de la forma $r(x) = (c, x)$ para algun $c \in M$. Entonces

$$\begin{aligned}r(x)j(a)r(x)^{-1} &= (c, x)(a, 1)\big(-(x^{-1} \cdot c), x^{-1}\big)\\ &= (c + x \cdot a, x)\big(-(x^{-1} \cdot c), x^{-1}\big)\\ &= \big(c + x \cdot a - x \cdot (x^{-1} \cdot c), xx^{-1}\big)\\ &= (c + x \cdot a - c, 1)\\ &= (x \cdot a, 1)\\ &= j(x \cdot a)\end{aligned}$$

□

Nótese que en el caso de que M sea un G-módulo trivial, su producto semidirecto $M \rtimes G$ coincide con el producto directo $M \times G$, ya que

$$(a, x)(b, y) = (a + x \cdot b, xy) = (a + b, xy),$$

que es la operación definida en el producto directo.

Recordemos que si E es un grupo, entonces el centro de E, denotado por $Z(E)$, es el conjunto (que resulta ser un subgrupo de E) de elementos del grupo que conmutan con todos los elementos del mismo, es decir,

$$Z(E) := \big\{e \in E : ee' = e'e \text{ para todo } e' \in E\big\}.$$

Proposición 3.2.7. *Sean M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión que preserva la acción. Entonces M es un G-módulo trivial si y solo si $i(M) \subseteq Z(E)$.*

Demostración. Sean $a \in M$ y $x \in G$, ya que M es un G-módulo trivial, $x \cdot a = a$. Por otro lado, $i(a) = i(x \cdot a) = s(x)i(a)s(x)^{-1}$ pues la extensión preserva la acción, se sigue que $s(x)i(a) = i(a)s(x)$, es decir, $i(a)$ conmuta con todos los elementos de $s(G)$. En general, un elemento $e \in E$ es de la forma $e = i(c)s(x)$ para algun $c \in M$ y $x \in G$. Entonces

$$\begin{aligned} i(a)e &= i(a)i(c)s(x) \\ &= i(a + c)s(x) \\ &= i(c + a)s(x) \\ &= i(c)i(a)s(x) \\ &= i(c)s(x)i(a) \\ &= ei(a) \end{aligned}$$

y por lo tanto $i(a) \in Z(E)$.

Recíprocamente, si $a \in M$ y $x \in G$, entonces $i(a)e = ei(a)$ para todo $e \in E$, en particular conmuta con los elementos de $s(G)$. Así $i(x \cdot a) = s(x)i(a)s(x)^{-1} = i(a)$, por lo tanto $x \cdot a = a$, es decir, M es un G-módulo trivial. □

A una extensión de grupos $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ tal que $i(M) \subseteq Z(E)$ se le llama una ***extensión central*** *de G.*

Entre los objetivos a resolver en el problema de la extensión está el de encontrar una manera de clasificar dichas extensiones. Antes de intentar hacer esto, es conveniente definir cuando dos extensiones son en esencia muy "parecidas". Por ejemplo, podríamos decir que dos extensiones

$$\varepsilon : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1 \qquad \text{y} \qquad \varepsilon' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$$

son equivalentes si existe un isomorfismo $\varphi : E \to E'$. Sin embargo, nosotros pediremos una condición más fuerte pero antes de hacerlo demostraremos el siguiente Lema.

Proposición 3.2.8 (Lema del 3). *Consideremos el siguiente diagrama conmutativo (de grupos) con renglones exactos.*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 1 & \longrightarrow & H' & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q' & \longrightarrow & 1 \end{array}$$

Si dos de los tres morfismos f, g, h son isomorfismos. Entonces el tercero también es un isomorfismo.

Demostración. Supongamos que f y h son isomorfismos. Veamos que g es un isomorfismo: Sea $x \in \mathit{Ker}(g)$; entonces

$$hp(x) = p'g(x) = p'(1) = 1$$

Ya que h es un isomorfismo se tiene que $p(x) = 1$, es decir, $x \in \mathit{Ker}(p) = \mathit{Im}(i)$ y así $x = i(y)$ para algún $y \in H$. Luego,

$$i'f(y) = gi(y) = g(x) = 1$$

Puesto que $i'f$ es un monomorfismo, se tiene que $y = 1$ y por lo tanto $x = i(y) = i(1) = 1$. Ahora veamos que g es un epimorfismo: Sea $x' \in G'$. Ya que h es un isomorfismo, existe $z \in Q$ tal que $h(z) = p'(x')$. Como p también es un epimorfismo, existe $x \in G$ tal que $p(x) = z$. Luego,

$$p'\big(g(x)\big) = hp(x) = h(z) = p'(x')$$

el cual equivale a que $g(x)^{-1}x' \in \mathit{Ker}(p') = \mathit{Im}(i')$ y así $g(x)^{-1}x' = i'(y')$ para algún $y' \in H'$. Como f es un isomorfismo, existe $y \in H$ tal que $f(y) = y'$. Se sigue que

$$g\big(i(y)\big) = i'f(y) = i'(y') = g(x)^{-1}x'.$$

Por lo tanto, $g\big(xi(y)\big) = g(x)g\big(i(y)\big) = x'$. Los otros dos casos posibles se demuestran de manera similar. □

Definición 3.2.9. Sean G un grupo y M un G-módulo. Si

$$\xi : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1 \qquad y \qquad \xi' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$$

son extensiones de M por G que preservan la acción, diremos que la extensión ξ es equivalente a la extensión ξ' si existe un morfismo de grupos $\varphi : E \to E'$ que hace conmutar el siguiente diagrama.

$$\begin{array}{ccccccccc} \xi : 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ \xi' : 0 & \longrightarrow & M & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

Obsérvese que por el Lema 3.2.8 los grupos E y E' son isomorfos, de manera que aún seguimos conservando parte de la idea de que estas extensiones son muy "parecidas". La siguiente Proposición muestra que esta relación es de equivalencia y esto nos permite agrupar en conjuntos ajenos a todas aquellas extensiones que son equivalentes.

Proposición 3.2.10. *La relación de la definición 3.2.9 es una relación de equivalencia.*

Demostración. Sea $\xi : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión, claramente el morfismo identidad $1_E : E \to E$ hace conmutar el diagrama

$$\begin{array}{ccccccccc} \xi : 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle 1_E} & & \downarrow{\scriptstyle 1_G} & & \\ \xi : 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

y así la relación es reflexiva.

Si la extensión $\xi : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ es equivalente a la extensión $\xi' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$, entonces existe un morfismo $\varphi : E \to E'$ tal que $\varphi i = i'$ y $p'\varphi = p$, es decir, el diagrama

$$\begin{array}{ccccccccc} \xi : 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ \xi' : 0 & \longrightarrow & M & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

conmuta. Por el Lema 3.2.8 tenemos que φ es un isomorfismo y así podemos considerar a $\psi : E' \to E$ el inverso de φ. Veamos que el diagrama

$$\begin{array}{ccccccccc} \xi' : 0 & \longrightarrow & M & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle 1_G} & & \\ \xi : 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

conmuta. En efecto,

$$\psi i' = \psi(\varphi i) = (\psi\varphi)i = 1_E i = i$$
$$p\psi = (p'\varphi)\psi = p'(\varphi\psi) = p'1_{E'} = p'$$

Por lo tanto ξ' es equivalente a ξ, es decir, la relación es simétrica.

Finalmente, si la extensión $\xi : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ es equivalente a la extensión $\xi' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$ y $\xi' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$ es equivalente a la extensión $\xi'' : 0 \longrightarrow M \xrightarrow{i''} E'' \xrightarrow{p''} G \longrightarrow 1$, entonces existen morfismos $\varphi : E \to E'$ y $\varphi' : E' \to E''$ tales que $\varphi i = i'$, $p'\varphi = p$ y $\varphi' i' = i''$, $p''\varphi' = p'$, es decir, cada cuadrado del diagrama

$$\begin{array}{ccccccccc} \xi : 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ \xi' : 0 & \longrightarrow & M & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle 1_G} & & \\ \xi'' : 0 & \longrightarrow & M & \xrightarrow{i''} & E'' & \xrightarrow{p''} & G & \longrightarrow & 1 \end{array}$$

conmuta. Si consideramos la composición $\varphi'\varphi$, entonces

$$(\varphi'\varphi)i = \varphi'(\varphi i) = \varphi' i' = i''$$
$$p''(\varphi'\varphi) = (p''\varphi')\varphi = p'\varphi = p$$

y así el diagrama

$$\begin{array}{ccccccccc} \xi: 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi'\varphi} & & \downarrow{\scriptstyle 1_G} & & \\ \xi'': 0 & \longrightarrow & M & \xrightarrow{i''} & E'' & \xrightarrow{p''} & G & \longrightarrow & 1 \end{array}$$

también conmuta, lo que demuestra que ξ es equivalente a ξ'' y por lo tanto la relación es transitiva. □

Sean G un grupo y M un G-módulo. Denotaremos por $\boldsymbol{e}(G, M)$ al conjunto de clases de equivalencia de extensiones de M por G que preservan la acción.

Para poder clasificar a estas extensiones salvo equivalencia, empezaremos por encontrar representantes adecuados de cada una de las clases de equivalencia. La siguiente Proposición nos da un candidato a considerar en la clase de extensiones que se escinden.

Proposición 3.2.11. *Sean G un grupo y M un G-módulo. Si la extensión*

$$0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$$

se escinde y preserva la acción, entonces existe un morfismo $\varphi : E \to M \rtimes G$ que hace conmutar el siguiente diagrama.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{j} & M \rtimes G & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

Demostración. Ya que la extensión se escinde, por la Proposición 3.2.2, existe un subgrupo $Q \subseteq E$ tal que todo elemento $e \in E$ se escribe de manera única como $e = i(a)z$ con $a \in M$ y $z \in Q$. Veamos que $p|_Q$ es un isomorfismo.

Sean $z, w \in Q$ tales que $p(z) = p(w)$, entonces $zw^{-1} \in Ker(p) = i(M)$ y así $zw^{-1} = i(c)$ para algún $c \in M$. Tenemos las siguientes expresiones para $z \in Q \subseteq E$

$$i(0)z = 1z = z = \big(zw^{-1}\big)w = i(c)w,$$

se sigue de la unicidad, que $z = w$ y por lo tanto $p|_Q$ es un monomorfismo. Por otro lado, si $x \in G$, existe $e \in E$ tal que $p(e) = x$, ya que p es un epimorfismo. Por hipótesis $e = i(a)z$ con $a \in M$ y $z \in Q$, luego

$$x = p(e) = p\big(i(a)z\big) = pi(a)p(z) = 1p(z) = p(z),$$

es decir, $p|_Q$ es suprayectiva. Si $s : G \to Q$ es el inverso de $p|_Q$, entonces s resulta ser una sección y por la Proposición 3.1.4 la estructura de G-módulo sobre M está dada como sigue: Para todo $x \in G$ y $a \in M$

$$i(xa) = s(x)i(a)s(x)^{-1}$$

es decir $xa = \theta_x(a)$. Ahora definimos $\varphi : E \to M \rtimes G$ de la siguiente manera: Si $e \in E$, $e = i(a)z$ con $a \in M$ y $z \in Q$

$$\varphi(e) = \varphi\big(i(a)z\big) = \big(a, p(z)\big)$$

φ está bien definido pues a, z son únicos y $p\,|_Q$ es un isomorfismo. Veamos que φ es un morfismo. Sean $e = i(a)z$ y $f = i(b)w$ con $a, b \in M$ y $z, w \in Q$

$$\begin{aligned}
\varphi(e \cdot f) &= \varphi\big(i(a)z \cdot i(b)w\big) \\
&= \varphi\big(i(a)sp(z) \cdot i(b)w\big) \\
&= \varphi\Big(i(a)s\big(p(z)\big)i(b)s\big(p(z)\big)^{-1}s\big(p(z)\big)w\Big) \\
&= \varphi\Big(i(a)i\big(p(z)b\big)zw\Big) \\
&= \varphi\Big(i\big(a + p(z)b\big)zw\Big) \\
&= \big(a + p(z)b, p(zw)\big) \\
&= \big(a + p(z)b, p(z)p(w)\big) \\
&= \big(a, p(z)\big)\big(b, p(w)\big) \\
&= \varphi\big(i(a)z\big)\varphi\big(i(b), w\big) \\
&= \varphi(e)\varphi(f)
\end{aligned}$$

Si $(a, x) \in M \rtimes G$, entonces $\varphi\big(i(a)s(x)\big) = \big(a, ps(x)\big) = (a, x)$ y así φ es suprayectiva. Finalmente, si $e = i(a)z \in E$ y

$$(0, 1) = \varphi\big(i(a)z\big) = \big(a, p(z)\big)$$

entonces $a = 0$ y $p\,|_Q\ (z) = p(z) = 1$, esto último implica que $z = 1$ pues $p\,|_Q$ es un isomorfismo. Por lo tanto $e = i(a)z = i(0)1 = 1 \cdot 1 = 1$, es decir, el *Ker*$(\varphi) = 1$. Por lo tanto φ es inyectiva. Por último,

$$\varphi i(a) = \varphi\big(i(a)1\big) = \big(a, p(1)\big) = (a, 1) = j(a)$$

y

$$\pi\varphi(e) = \pi\varphi\big(i(a)z\big) = \pi\big(a, p(z)\big) = p(z) = 1p(z) = pi(a)p(z) = p\big(i(a)z\big) = p(e),$$

es decir, $\varphi i = j$ y $\pi\varphi = p$. □

3.3. Conjuntos factores

Para encontrar al resto de los representantes de las respectivas clases de equivalencia (en el caso de que existan más clases), el primer paso que realizaremos será introducir funciones que nos permitan comparar que tanto difieren estas extensiones respecto de las que se escinden, para ello recordemos que si $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ es una extensión y $s : G \to E$ es una sección, entonces para cada $x, y \in G$

$$p\big(s(x)s(y)\big) = ps(x)ps(y) = xy = ps(xy),$$

es decir, $s(x)s(y)s(xy)^{-1} \in \textit{Ker}(p) = \textit{Im}(i)$ y por lo tanto existe un único elemento $a \in M$ (que depende de x y y) tal que $s(x)s(y) = i(a)s(xy)$.

Definición 3.3.1. Sean $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión que preserva la acción y $s : G \to E$ una sección. Un ***conjunto factor*** es una función $f : G \times G \to M$ tal que

$$s(x)s(y) = if(x, y)s(xy).$$

Como se mencionó anteriormente estos conjuntos factores de alguna forma miden lo que le falta a la sección s para ser un morfismo y por lo tanto para que la extensión se escinda. Obsérvese que en el caso de que la sucesión se escinda, existe una sección que es un morfismo, cuyo correspondiente conjunto factor es identicamente la función cero. Los siguientes Teoremas caracterizan a estos conjuntos factores.

Teorema 3.3.2. *Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión que preserva la acción. Si $s : G \to E$ es una sección y $f : G \times G \to M$ su correspondiente conjunto factor, entonces:*

a) Para todo $x, y \in G$

$$f(x, 1) = 0 = f(1, y)$$

b) Se satisface la identidad del cociclo: para todo $x, y, z \in G$, se cumple que

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

Demostración.

a) Por hipótesis tenemos que $s(x)s(y) = if(x, y)s(xy)$. Tomando $y = 1$ y usando el hecho de que $s(1) = 1$ (ya que s es una sección) se tiene que

$$s(x) = s(x)s(1) = if(x, 1)s(x \cdot 1) = if(x, 1)s(x)$$

lo que implica que $if(x, 1) = 1$, es decir, $f(x, 1) \in \textit{Ker}(i) = \{0\}$ y por lo tanto $f(x, 1) = 0$. Análogamente, haciendo $x = 1$ obtenemos que $f(1, y) = 0$.

b) La identidad del cociclo se obtiene de la asociatividad en E y en G. Para todo x, y, $z \in G$, se tiene que

$$\begin{aligned}\big(s(x)s(y)\big)s(z) &= if(x,y)s(xy)s(z)\\ &= if(x,y)if(xy,z)s(xyz)\\ &= i\big(f(x,y)+f(xy,z)\big)s(xyz)\end{aligned}$$

Por otro lado,

$$\begin{aligned}s(x)\big(s(y)s(z)\big) &= s(x)if(y,z)s(yz)\\ &= s(x)if(y,z)s(x)^{-1}s(x)s(yz)\\ &= i\big(xf(y,z)\big)if(x,yz)s(xyz)\\ &= i\big(xf(y,z)+f(x,yz)\big)s(xyz)\end{aligned}$$

Se sigue que $i\big(f(x,y)+f(xy,z)\big) = i\big(xf(y,z)+f(x,yz)\big)$ y como i es inyectiva

$$f(x,y)+f(xy,z) = xf(y,z)+f(x,yz).$$

□

En la demostración del siguiente Teorema se generaliza la construcción del producto semidirecto de un G-módulo M.

Teorema 3.3.3. *Sean G un grupo, M un G-módulo y $f : G \times G \to M$ una función que satisface:*

a) Para todo $x, y \in G$

$$f(x,1) = 0 = f(1,y).$$

b) Para todo $x, y, z \in G$

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

Entonces existe una extensión $\varepsilon_f : 0 \longrightarrow M \xrightarrow{j_f} E_f \xrightarrow{\pi_f} G \longrightarrow 1$ que preserva la acción y existe una sección s cuyo correspondiente conjunto factor es f.

Demostración. Definimos $M \rtimes_f G$ como el conjunto de parejas ordenadas $(a, x) \in M \times G$ junto con la siguiente operación

$$(a,x)(b,y) = \big(a + x\cdot b + f(x,y), xy\big)$$

Veamos que $M \rtimes_f G$ es un grupo con esta operación.

La operación es asociativa

$$\begin{aligned}\big((a,x)(b,y)\big)(c,z) &= \big(a+xb+f(x,y),xy\big)(c,z)\\ &= \big(a+xb+f(x,y)+(xy)c+f(xy,z),(xy)z\big)\\ &= \big(a+xb+(xy)c+f(x,y)+f(xy,z),xyz\big)\end{aligned}$$

Por otro lado,

$$\begin{aligned}(a,x)\big((b,y)(c,z)\big) &= (a,x)\big(b+yc+f(y,z),yz\big)\\ &= \Big(a+x\big(b+yc+f(y,z)\big)+f(x,yz),x(yz)\Big)\\ &= \big(a+xb+x(yc)+xf(y,z)+f(x,yz),xyz\big)\end{aligned}$$

Finalmente, la igualdad se sigue de que $f(x,y)+f(xy,z) = xf(y,z)+f(x,yz)$.

El elemento $(0,1)$ es el neutro de la operación

$$\begin{aligned}(a,x)(0,1) &= \big(a+x\cdot 0+f(x,1),x\cdot 1\big)\\ &= (a+0+0,x)\\ &= (a,x)\end{aligned}$$

y

$$\begin{aligned}(0,1)(a,x) &= \big(0+1\cdot a+f(1,x),1\cdot x\big)\\ &= (a+0,x)\\ &= (a,x)\end{aligned}$$

En lo que sigue, las expresiones de la forma $-xa$ con $x\in G$ y $a\in M$ se entienden como $-(xa)$, por ejemplo, $-x^{-1}a = -(x^{-1}a)$ y $-x^{-1}f(x,x^{-1}) = -\big(x^{-1}f(x,x^{-1})\big)$. Habiendo dicho lo anterior, el inverso de (a,x) es $\big(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1}\big)$, para verificar esto último, observemos que de la identidad del cociclo

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

y de las sustituciones $y=x^{-1}$ y $z=x$, se obtiene lo siguiente:

$$\begin{aligned}0 &= xf(x^{-1},x)-f(xx^{-1},x)+f(x,x^{-1}x)-f(x,x^{-1})\\ &= xf(x^{-1},x)-f(1,x)+f(x,1)-f(x,x^{-1})\\ &= xf(x^{-1},x)-0+0-f(x,x^{-1})\\ &= xf(x^{-1},x)-f(x,x^{-1})\end{aligned}$$

Multiplicando está última igualdad por x^{-1} obtenemos que $f(x^{-1},x)-x^{-1}f(x,x^{-1})=0$. Luego,

$$\begin{aligned}(a,x)\big(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1}\big) &= \Big(a+x\big(-x^{-1}a-x^{-1}f(x,x^{-1})\big)+f(x,x^{-1}),xx^{-1}\Big)\\ &= \Big(a-x(x^{-1}a)-x\big(x^{-1}f(x,x^{-1})\big)+f(x,x^{-1}),1\Big)\\ &= \big(a-a-f(x,x^{-1})+f(x,x^{-1}),1\big)\\ &= (0,1)\end{aligned}$$

y

$$\begin{aligned}\big(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1}\big)(a,x) &= \big(-x^{-1}a-x^{-1}f(x,x^{-1})+x^{-1}a+f(x^{-1},x),x^{-1}x\big)\\ &= \big(f(x^{-1},x)-x^{-1}f(x,x^{-1}),1\big)\\ &= (0,1)\end{aligned}$$

Por lo tanto $M \rtimes_f G$ es un grupo.

Desde luego, las funciones $j_f : M \to M \rtimes_f G$ y $\pi_f : M \rtimes_f G \to G$ definidas como $j_f(a) = (a, 1)$ y $\pi_f(a, x) = x$ resultan ser morfismos. Claramente j_f es un monomorfismo, π_f un epimorfismo y $Im(j_f) = \{(a, 1) : a \in M\} = Ker(\pi_f)$. Por lo tanto la sucesión

$$\varepsilon_f : 0 \longrightarrow M \xrightarrow{j_f} M \rtimes_f G \xrightarrow{\pi_f} G \longrightarrow 1$$

es una extensión de M por G. Solo resta ver que la extensión construida preserva la acción, para ello elegimos una sección $r : G \to M \rtimes_f G$, dicha sección es de la forma $r(x) = (c, x)$ para algún $c \in M$, entonces

$$\begin{aligned}
r(x)j_f(a)r(x)^{-1} &= (c, x)(a, 1)(c, x)^{-1} \\
&= \big(c + xa + f(x, 1), x \cdot 1\big)\big(-x^{-1}c - x^{-1}f(x, x^{-1}), x^{-1}\big) \\
&= (c + xa, x)\left(-x^{-1}c - x^{-1}f(x, x^{-1}), x^{-1}\right) \\
&= \Big(c + xa + x\big(-x^{-1}c - x^{-1}f(x, x^{-1})\big) + f(x, x^{-1}), x \cdot x^{-1}\Big) \\
&= \Big(c + xa - x(x^{-1}c) - x\big(x^{-1}f(x, x^{-1})\big) + f(x, x^{-1}), 1\Big) \\
&= \big(c + xa - c - f(x, x^{-1}) + f(x, x^{-1}), 1\big) \\
&= (xa, 1) \\
&= j_f(xa)
\end{aligned}$$

Por último, la función $s : G \to M \rtimes_f G$, donde $s : x \mapsto (0, x)$, es una sección cuyo correspondiente conjunto factor es f. En efecto,

$$\begin{aligned}
s(x)s(y)s(xy)^{-1} &= (0, x)(0, y)(0, xy)^{-1} \\
&= \big(0 + x \cdot 0 + f(x, y), xy\big)\Big(-(xy)^{-1} \cdot 0 - (xy)^{-1}f\big(xy, (xy)^{-1}\big), (xy)^{-1}\Big) \\
&= \big(f(x, y), xy\big)\Big(-(xy)^{-1}f\big(xy, (xy)^{-1}\big), (xy)^{-1}\Big) \\
&= \Big(f(x, y) + xy\Big(-(xy)^{-1}f\big(xy, (xy)^{-1}\big)\Big) + f\big(xy, (xy)^{-1}\big), (xy)(xy)^{-1}\Big) \\
&= \Big(f(x, y) - f\big(xy, (xy)^{-1}\big) + f\big(xy, (xy)^{-1}\big), 1\Big) \\
&= \big(f(x, y), 1\big) \\
&= j_f f(x, y),
\end{aligned}$$

es decir, $s(x)s(y) = j_f f(x, y)s(xy)$. □

El siguiente Corolario es consecuencia de las dos Proposiciones anteriores.

Corolario 3.3.4. *Sean G un grupo y M un G-módulo. Una función $f : G \times G \to M$ es un conjunto factor si y sólo si satisface la identidad del cociclo: para todo $x, y, z \in G$*

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

y para todo $x, y \in G$

$$f(x, 1) = 0 = f(1, y).$$

El Corolario 3.3.4 nos da la ventaja de poder caracterizar a los conjuntos factores prescindiendo de la extensión y de la sección usadas en su definición. Por otro lado, podemos considerar la función en la que a cada conjunto factor f se le asigna la clase $[\varepsilon_f]$ y es natural preguntarnos si esta función es inyectiva, suprayectiva o biyectiva.

Teorema 3.3.5. *Sean G un grupo, M un G-módulo y*

$$0 \longrightarrow M \xrightarrow{\ i\ } E \xrightarrow{\ p\ } G \longrightarrow 1$$

una extensión que preserva la acción. Entonces existe un conjunto factor f y un morfismo $\varphi : E \to M \rtimes_f G$ que hace conmutar el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\ i\ } & E & \xrightarrow{\ p\ } & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{\ j_f\ } & M \rtimes_f G & \xrightarrow{\ \pi_f\ } & G & \longrightarrow & 1 \end{array}$$

Demostración. Sea $s : G \to E$ una sección y sea f su correspondiente conjunto factor, es decir, $s(x)s(y) = if(x, y)s(xy)$. Por la Proposición 3.1.3 tenemos que $s(G)$ es un sistema completo de representantes de clases laterales derechas de $M' := Im(i)$ en E. Por lo tanto, si $e \in E$ entonces $M'e = M's(x)$ para un único $x \in G$, así $e = i(a)s(x)$ y además esta expresión es única. Definimos $\varphi : E \to M \rtimes_f G$ como

$$\varphi(e) = \varphi\big(i(a)s(x)\big) = (a, x),$$

ya que a, x son únicos φ es una función biyectiva. Ahora veamos que φ es un morfismo. Sean $e = i(a)s(x)$ y $f = i(b)s(y)$, entonces

$$\begin{aligned} \varphi(ef) &= \varphi\big(i(a)s(x)i(b)s(y)\big) \\ &= \varphi\big(i(a)s(x)i(b)s(x)^{-1}s(x)s(y)\big) \\ &= \varphi\big(i(a)i(xb)if(x, y)s(xy)\big) \\ &= \varphi\Big(i\big(a + xb + f(x, y)\big)s(xy)\Big) \\ &= \big(a + xb + f(x, y), xy\big) \\ &= (a, x)(b, y) \\ &= \varphi\big(i(a)s(x)\big)\varphi\big(i(b)s(y)\big) \\ &= \varphi(e)\varphi(f) \end{aligned}$$

Finalmente, el diagrama conmuta puesto que si $a \in M$ y $e = i(a)s(x) \in E$, entonces

$$(\varphi \circ i)(a) = \varphi\big(i(a)\big) = \varphi\big(i(a)s(1)\big) = (a, 1) = j_f(a)$$

y

$$(\pi_f \circ \varphi)(e) = \pi_f\Big(\varphi\big(i(a)s(x)\big)\Big) = \pi_f(a, x) = x = 1 \cdot x = pi(a)ps(x) = p\big(i(a)s(x)\big) = p(e),$$

es decir, $\varphi \circ i = j_f$ y $\pi_f \circ \varphi = p$. □

Lema 3.3.6. *Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión que preserva la acción. Si s y r son secciones con conjuntos factores f y g respectivamente, entonces existe una función $h : G \to M$ con $h(1) = 0$ tal que para todo $x, y \in G$*

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

Demostración. Para cada $x \in G$, $r(x)s(x)^{-1} \in Ker(p) = Im(i)$, podemos entonces definir a la función $h : G \to M$ donde $h(x)$ es el único elemento en M tal que $i\big(h(x)\big) = r(x)s(x)^{-1}$, es decir, $r(x) = i\big(h(x)\big)s(x)$ y así tenemos lo siguiente

$$i(0) = 1 = r(1) = i\big(h(1)\big)s(1) = i\big(h(1)\big) \cdot 1 = i\big(h(1)\big),$$

se sigue que $h(1) = 0$. Por otro lado,

$$\begin{aligned}
r(x)r(y) &= i\big(h(x)\big)s(x)i\big(h(y)\big)s(y) \\
&= i\big(h(x)\big)s(x)i\big(h(y)\big)s(x)^{-1}s(x)s(y) \\
&= i\big(h(x)\big)i\big(xh(y)\big)s(x)s(y) \\
&= i\big(h(x) + xh(y)\big)i\big(f(x, y)\big)s(xy) \\
&= i\big(h(x) + xh(y) + f(x, y)\big)i\big(h(xy)\big)^{-1}r(xy) \\
&= i\big(h(x) + xh(y) + f(x, y)\big)i\big(-h(xy)\big)\big(ig(x, y)\big)^{-1}r(x)r(y) \\
&= i\big(h(x) + xh(y) + f(x, y) - h(xy)\big)i\big(-g(x, y)\big)r(x)r(y) \\
&= i\big(h(x) + xh(y) + f(x, y) - h(xy) - g(x, y)\big)r(x)r(y)
\end{aligned}$$

Se sigue que $i\big(h(x) + xh(y) + f(x, y) - h(xy) - g(x, y)\big) = 1 = i(0)$, por lo tanto

$$h(x) + xh(y) + f(x, y) - h(xy) - g(x, y) = 0,$$

es decir, $g(x, y) - f(x, y) = xh(y) - h(xy) + h(x)$. □

Definición 3.3.7. Sean G un grupo y M un G-módulo. Una función $g : G \times G \to M$ es una ***cofrontera*** si existe una función $h : G \to M$ con $h(1) = 0$ tal que para todo $x, y \in G$,

$$g(x, y) = xh(y) - h(xy) + h(x).$$

Por lo tanto, el Lema 3.3.6 afirma que si s y r son secciones con conjuntos factores f y g respectivamente, entonces $f - g$ es una cofrontera.

Definición 3.3.8. Sean G un grupo y M un G-módulo. Definimos

$$Z^2(G, M) = \Big\{ f : G \times G \to M \mid f \text{ es un conjunto factor} \Big\}$$

y

$$B^2(G, M) = \Big\{ g : G \times G \to M \mid g \text{ es una cofrontera} \Big\}.$$

Enseguida veremos que estos dos conjuntos admiten estructura de grupo abeliano bajo la suma puntual de funciones y que además $B^2(G, M)$ resulta ser un subgrupo de $Z^2(G, M)$.

Proposición 3.3.9. *Si G es un grupo y M un G-módulo, entonces $Z^2(G, M)$ es un grupo abeliano bajo la suma puntual, es decir, si f, $f' \in Z^2(G, M)$*

$$f + f' : (x, y) \longmapsto f(x, y) + f'(x, y),$$

y $B^2(G, M)$ es un subgrupo de $Z^2(G, M)$.

Demostración. Si f y f' son conjuntos factores entonces para todo $x, y, z \in G$

$$\begin{aligned}\big(f + f'\big)(x, 1) &= f(x, 1) + f'(x, 1) = 0\\ \big(f + f'\big)(1, y) &= f(1, y) + f'(1, y) = 0\end{aligned}$$

y

$$\begin{aligned}&x\big(f + f'\big)(y, z) - \big(f + f'\big)(xy, z) + \big(f + f'\big)(x, yz) - \big(f + f'\big)(x, y)\\ &= xf(y, z) + xf'(y, z) - f(xy, z) - f'(xy, z) + f(x, yz)\\ &\quad + f'(x, yz) - f(x, y) - f'(x, y)\\ &= xf(y, z) - f(xy, z) + f(x, yz) - f(x, y)\\ &\quad + xf'(y, z) - f'(xy, z) + f'(x, yz) - f'(x, y)\\ &= 0\end{aligned}$$

Por lo tanto $f + f'$ también es un conjunto factor.

La asociatividad de la suma en $Z^2(G, M)$ se sigue de la asociatividad en M.

La funcion $f_0(x, y) = 0$ para todo $x, y \in G$ es un conjunto factor y es el neutro en $Z^2(G, M)$.

Si f es un conjunto factor, entonces $g(x, y) := -f(x, y)$ también es un conjunto factor pues para todo $x, y, z \in G$

$$\begin{aligned}g(x, 1) &= -f(x, 1) = -0 = 0\\ g(1, y) &= -f(1, y) = -0 = 0\end{aligned}$$

y

$$\begin{aligned}&xg(y, z) - g(xy, z) + g(x, yz) - g(x, y)\\ &= -xf(y, z) + f(xy, z) - f(x, yz) + f(x, y)\\ &= -\big(xf(y, z) - f(xy, z) + f(x, yz) - f(x, y)\big)\\ &= 0\end{aligned}$$

además $\big(f + g\big)(x, y) = f(x, y) + g(x, y) = f(x, y) + \big(-f(x, y)\big) = 0$. Finalmente, el grupo es abeliano ya que si f, $f' \in Z^2(G, M)$

$$\big(f + f'\big)(x, y) = f(x, y) + f'(x, y) = f'(x, y) + f(x, y) = \big(f' + f\big)(x, y)$$

es decir $f + f' = f' + f$.

Ahora veamos que $B^2(G, M)$ es un subgrupo de $Z^2(G, M)$. Para empezar $B^2(G, M)$ es un conjunto no vacío, ya que la función $f_0(x, y) = 0$ para todo $x, y \in G$ es una cofrontera.

Sea $g \in B^2(G, M)$, entonces existe una función $h : G \to M$ con $h(1) = 0$ tal que para todo $x, y \in G$

$$g(x, y) = xh(y) - h(xy) + h(x).$$

De lo anterior tenemos que:

$$\begin{aligned} g(x, 1) &= xh(1) - h(x) + h(x) = 0 \\ g(1, y) &= h(y) - h(y) + h(1) = 0 \end{aligned}$$

y

$$\begin{aligned} & xg(y, z) - g(xy, z) + g(x, yz) - g(x, y) \\ &= x\big(yh(z) - h(yz) + h(y)\big) - \big(xyh(z) - h(xyz) + h(xy)\big) \\ &\quad + \big(xh(yz) - h(xyz) + h(x)\big) - \big(xh(y) - h(xy) + h(x)\big) \\ &= xyh(z) - xh(yz) + xh(y) - xyh(z) + h(xyz) - h(xy) \\ &\quad + xh(yz) - h(xyz) + h(x) - xh(y) + h(xy) - h(x) \\ &= 0 \end{aligned}$$

Por lo tanto, g es un conjunto factor, es decir, $g \in Z^2(G, M)$ y así $B^2(G, M) \subseteq Z^2(G, M)$.

Por último, si $g, g' \in B^2(G, M)$, entonces existen funciones $h, h' : G \to M$ tales que $h(1) = 0 = h'(1)$ y para todo $x, y \in G$

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

definimos $h'' : G \to M$, $h'' : x \mapsto h(x) - h'(x)$, entonces $h''(1) = h(1) - h'(1) = 0 - 0 = 0$ y

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

es decir, $g - g'$ es una cofrontera. □

Posteriormente demostraremos que el segundo grupo de cohomología $H^2(G, M)$ es isomorfo al grupo $Z^2(G, M)/B^2(G, M)$.

Lema 3.3.10. *Sean G un grupo y M un G-módulo. Dos extensiones*

$$\xi : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1 \qquad y \qquad \xi' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$$

que preservan la acción son equivalentes si y sólo si existen conjuntos factores f de ξ y f' de ξ' tal que $f - f'$ es una cofrontera.

Demostración. Sean $s : G \to E$ y $s' : G \to E'$ secciones de las extensiones ξ y ξ' respectivamente.

Supongamos que las extensiones son equivalentes, es decir, existe un morfismo $\varphi : E \to E'$ tal que $\varphi i = i'$ y $p'\varphi = p$. Sea f el correspondiente conjunto factor de la sección s, esto es, para todo $x, y \in G$

$$s(x)s(y) = if(x, y)s(xy).$$

Definimos $r : G \to E'$ como $r := \varphi s$ y afirmamos que r es una sección de la extensión $\xi' : 0 \longrightarrow M \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$ que también tiene a f como conjunto factor. En efecto, para todo $x, y \in G$

$$p'r(x) = p'\varphi s(x) = ps(x) = x,$$

es decir, $p'r = 1_G$ y

$$\begin{aligned} r(x)r(y) &= \varphi s(x)\varphi s(y) \\ &= \varphi\big(s(x)s(y)\big) \\ &= \varphi\big(if(x, y)s(xy)\big) \\ &= (\varphi i)f(x, y)\varphi s(xy) \\ &= i'f(x, y)r(xy) \end{aligned}$$

Finalmente, por el Lema 3.3.6 $f - f'$ es una cofrontera.

Recíprocamente, supongamos que existen conjuntos factores f y f' de las extensiones ξ y ξ' respectivamente tal que $f - f'$ es una cofrontera, esto es, existe una función $h : G \to M$ con $h(1) = 0$ tal que para todo $x, y \in G$

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

o lo que es lo mismo,

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

Supongamos además que s y r son las secciones asociadas a los conjuntos factores f y f' respectivamente, así cada elemento $e \in E$ y $e' \in E'$ se expresan de manerá única como $e = i(a)s(x)$ y $e' = i'(c)r(z)$ con $a, c \in M$ y $x, z \in G$. Definimos $\varphi : E \to E'$ mediante

$$\varphi(e) = \varphi\big(i(a)s(x)\big) = i'\big(a + h(x)\big)r(x)$$

Primero veamos que φ es un morfismo. Sean $e = i(a)s(x)$ y $l = i(b)s(y) \in E$, entonces

$$\begin{aligned} \varphi(e \cdot l) &= \varphi\big(i(a)s(x)i(b)s(y)\big) \\ &= \varphi\Big(i(a)\big(s(x)i(b)s(x)^{-1}\big)s(x)s(y)\Big) \\ &= \varphi\big(i(a)i(xb)s(x)s(y)\big) \\ &= \varphi\big(i(a + xb)if(x, y)s(xy)\big) \\ &= \varphi\Big(i\big(a + xb + f(x, y)\big)s(xy)\Big) \\ &= i'\big(a + xb + f(x, y) + h(xy)\big)r(xy) \end{aligned}$$

$$\begin{aligned}
&= i'\big(a + xb + xh(y) + f'(x,y) + h(x)\big)r(xy)\\
&= i'\Big(a + h(x) + x\big(b + h(y)\big) + f'(x,y)\Big)r(xy)\\
&= i'\Big(a + h(x)\Big)i'\Big(x\big(b + h(y)\big)\Big)i'f'(x,y)r(xy)\\
&= i'\big(a + h(x)\big)i'\Big(x\big(b + h(y)\big)\Big)r(x)r(y)\\
&= i'\big(a + h(x)\big)\Big(r(x)i'\big(b + h(y)\big)r(x)^{-1}\Big)r(x)r(y)\\
&= i'\big(a + h(x)\big)r(x)i'\big(b + h(y)\big)r(y)\\
&= \varphi\big(i(a)s(x)\big)\varphi\big(i(b)s(y)\big)\\
&= \varphi(e)\varphi(l)
\end{aligned}$$

Finalmente, si $a \in M$ y $e = i(b)s(x) \in E$, entonces

$$\begin{aligned}
\varphi i(a) &= \varphi\big(i(a)s(1)\big)\\
&= i'\big(a + h(1)\big)r(1)\\
&= i'(a + 0)\cdot 1\\
&= i'(a)
\end{aligned}$$

y

$$\begin{aligned}
p'\varphi(e) &= p'\varphi\big(i(b)s(x)\big)\\
&= p'\Big(i'\big(b + h(x)\big)r(x)\Big)\\
&= p'i'\big(b + h(x)\big)p'r(x)\\
&= 1\cdot x\\
&= pi(b)\cdot ps(x)\\
&= p\big(i(b)s(x)\big)\\
&= p(e)
\end{aligned}$$

Por lo tanto, $\varphi i = i'$ y $p'\varphi = p$ y así las extensiones ξ y ξ' son equivalentes. □

Teorema 3.3.11 (Schreier). *Sean G un grupo y M un G-módulo. Existe una biyección*

$$\psi : Z^2(G,M)/B^2(G,M) \to \boldsymbol{e}(G,M)$$

tal que $\psi(0) = [\varepsilon]$ donde ε es la extensión

$$\varepsilon : 0 \longrightarrow M \xrightarrow{j} M \rtimes G \xrightarrow{\pi} G \longrightarrow 1.$$

Demostración. Definimos $\psi : Z^2(G,M)/B^2(G,M) \to \boldsymbol{e}(G,M)$ mediante

$$\psi\Big(f + B^2(G,M)\Big) = [\omega_f]$$

donde ω_f es la extensión

$$\omega_f : 0 \longrightarrow M \xrightarrow{j_f} M \rtimes_f G \xrightarrow{\pi_f} G \longrightarrow 1.$$

Esta función está bien definida, puesto que si $f + B^2(G, M) = f' + B^2(G, M)$, entonces $f - f' \in B^2(G, M)$ y por el Lema 3.3.10 las extensiones ω_f y $\omega_{f'}$ son equivalentes y así $[\omega_f] = [\omega_{f'}]$. Ahora veamos que ψ es inyectiva, para ello, supongamos que

$$\psi\Big(f + B^2(G, M)\Big) = [\omega_f] = [\omega_{f'}] = \psi\Big(f' + B^2(G, M)\Big).$$

La extensión ω_f tiene a f como conjunto factor y ya que ω_f es equivalente a $\omega_{f'}$, f también es un conjunto factor de la extensión $\omega_{f'}$ y por el Lema 3.3.6, $f - f' \in B^2(G, M)$, es decir, $f + B^2(G, M) = f' + B^2(G, M)$. La función ψ también es suprayectiva, ya que si $[\xi] \in \boldsymbol{e}(G, M)$, por el Teorema 3.3.5, existe un conjunto factor f tal que la extensión ξ es equivalente a ω_f y por lo tanto

$$\psi\Big(f + B^2(G, M)\Big) = [\omega_f] = [\xi].$$

Por último, si $f = 0$, entonces $M \rtimes_f G = M \rtimes G$ es el producto semidirecto de M por G y

$$\omega_f = \varepsilon : 0 \longrightarrow M \xrightarrow{j} M \rtimes G \xrightarrow{\pi} G \longrightarrow 1.$$

□

Capítulo 4

Derivaciones y $H^1(G, M)$

En este capítulo damos una descripción del primer grupo de cohomología $H^1(G, M)$ en términos de clases de equivalencia de derivaciones. Al final del capítulo usamos esta descripción y la teoría desarrollada en el Capítulo 3 para demostrar el *Teorema de Zassenhaus* el cual establece condiciones necesarias pero no suficientes para que un grupo finito G con $K \lhd G$ sea un producto semidirecto de K por G/K.

4.1. Automorfismos estabilizadores

Definición 4.1.1. Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión. Un automorfismo $\varphi : E \to E$ es un estabilizador de la extensión si el siguiente diagrama conmuta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

Si G es un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión, definimos el conjunto

$$\mathit{Stab}_E(G, M) = \Big\{\varphi : E \to E \mid \varphi \textit{ es un automorfismo estabilizador}\Big\},$$

esto es, el $\mathit{Stab}_E(G, M)$ es el conjunto de todos los automorfismos estabilizadores de la extensión. Posteriormente veremos que $\mathit{Stab}_E(G, M)$ es un grupo abeliano bajo la composición de funciones.

Lema 4.1.2. *Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión que preserva la acción. Entonces $\varphi : E \to E \in \mathit{Stab}_E(G, M)$ si y solo si existe una función $d : G \to M$ tal que:*

a) Para toda sección $s : G \to E$,

$$\varphi\big(i(a)s(x)\big) = i\big(a + d(x)\big)s(x)$$

.

b) Para todo $x, y \in G$ se tiene que $d(xy) = xd(y) + d(x)$.

Demostración.

a) Sea $s : G \to M$ una sección, por hipótesis $\varphi i = i$ y $p\varphi = p$, entonces para cada $x \in G$ se tiene que

$$\begin{aligned} p\Big(\varphi\big(s(x)\big)s(x)^{-1}\Big) &= p\varphi\big(s(x)\big)p\Big(s(x)^{-1}\Big) \\ &= ps(x)\big(ps(x)\big)^{-1} \\ &= xx^{-1} \\ &= 1, \end{aligned}$$

es decir, $\varphi\big(s(x)\big)s(x)^{-1} \in \mathit{Ker}(p) = \mathit{Im}(i)$, por lo que podemos definir a la función $d : G \to M$ donde $d(x)$ es el único elemento en M tal que

$$i\big(d(x)\big) = \varphi\big(s(x)\big)s(x)^{-1}.$$

Por lo tanto, $\varphi\big(s(x)\big) = i\big(d(x)\big)s(x)$. Si $e \in E$, entonces $e = i(a)s(x)$ y además esta expresión es única, así

$$\begin{aligned} \varphi(e) &= \varphi\big(i(a)s(x)\big) \\ &= \varphi\big(i(a)\big)\varphi\big(s(x)\big) \\ &= i(a)i\big(d(x)\big)s(x) \\ &= i\big(a + d(x)\big)s(x) \end{aligned}$$

Ahora veamos que $d : G \to M$ es independiente de la elección de la sección s. Para ello consideremos $r : G \to M$ otra sección, dicha sección induce una función $d' : G \to M$ donde $d'(x)$ es el único elemento en M tal que

$$i\big(d'(x)\big) = \varphi\big(r(x)\big)r(x)^{-1}.$$

Por otro lado, $s(x)^{-1}r(x) \in \mathit{Ker}(p) = \mathit{Im}(i)$, ya que s y r son secciones. Se sigue que $r(x) = s(x)i(a)$ para algún $a \in M$. Entonces,

$$\begin{aligned} i\big(d'(x)\big) &= \varphi\big(r(x)\big)r(x)^{-1} \\ &= \varphi\big(s(x)i(a)\big)i(a)^{-1}s(x)^{-1} \\ &= \varphi\big(s(x)\big)\varphi\big(i(a)\big)i(a)^{-1}s(x)^{-1} \\ &= \varphi\big(s(x)\big)i(a)i(a)^{-1}s(x)^{-1} \\ &= \varphi\big(s(x)\big)s(x)^{-1} \\ &= i\big(d(x)\big) \end{aligned}$$

de la inyectividad de i se sigue que $d'(x) = d(x)$.

b) Sean $x, y \in G$ y f el correspondiente conjunto factor asociado a la sección s, entonces

$$s(x)s(y) = if(x, y)s(xy)$$

Evaluaremos a φ de dos maneras. Por un lado tenemos que

$$\begin{aligned}
\varphi\big(s(x)s(y)\big) &= \varphi\big(s(x)\big)\varphi\big(s(y)\big) \\
&= i\big(d(x)\big)s(x)i\big(d(y)\big)s(y) \\
&= i\big(d(x)\big)\Big(s(x)i\big(d(y)\big)s(x)^{-1}\Big)s(x)s(y) \\
&= i\big(d(x)\big)i\big(xd(y)\big)if(x, y)s(xy) \\
&= i\big(d(x) + xd(y) + f(x, y)\big)s(xy)
\end{aligned}$$

Por otro lado,

$$\begin{aligned}
\varphi\big(s(x)s(y)\big) &= \varphi\big(if(x, y)s(xy)\big) \\
&= \varphi\big(if(x, y)\big)\varphi\big(s(xy)\big) \\
&= if(x, y)i\big(d(xy)\big)s(xy) \\
&= i\big(f(x, y) + d(xy)\big)s(xy)
\end{aligned}$$

se sigue que $i\big(d(x) + xd(y) + f(x, y)\big) = i\big(f(x, y) + d(xy)\big)$ y como i es inyectiva $d(x) + xd(y) + f(x, y) = f(x, y) + d(xy)$. Por lo tanto, $d(xy) = xd(y) + d(x)$.

Recíprocamente, si existe una función $d : G \to M$ que satisface los incisos *a)* y *b)* y $s : G \to E$ es una sección, entonces

$$d(1) = d(1 \cdot 1) = 1 \cdot d(1) + d(1) = d(1) + d(1)$$

por lo tanto $d(1) = 0$. Luego para cada $a \in M$ y $e = i(a')s(x) \in E$

$$\varphi i(a) = \varphi\big(i(a)s(1)\big) = i\big(a + d(1)\big)s(1) = i(a + 0) = i(a)$$

y

$$\begin{aligned}
p\varphi(e) &= p\Big(\varphi\big(i(a')s(x)\big)\Big) \\
&= p\Big(i\big(a' + d(x)\big)s(x)\Big) \\
&= pi\big(a' + d(x)\big)ps(x) \\
&= 1x \\
&= pi(a')ps(x) \\
&= p\big(i(a')s(x)\big) \\
&= p(e).
\end{aligned}$$

□

Daremos un nombre a aquellas funciones que satisfacen el inciso *b)*.

4.2. Derivaciones

Definición 4.2.1. Sean G un grupo y M un G-módulo. Una derivación (o homomorfismo cruzado) es una función $d : G \to M$ tal que para todo $x, y \in G$

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

Denotaremos por $Der(G, M)$ al conjunto de todas las derivaciones.

Ejemplo 4.2.2. Sean G un grupo, M un G-módulo y $a \in M$. La función $d_a : G \to M$ dada por

$$d_a(x) = xa - a$$

es una derivación, pues

$$\begin{aligned} xd_a(y) + d_a(x) &= x(ya - a) + xa - a \\ &= x(ya) - xa + xa - a \\ &= (xy)a - a \\ &= d_a(xy). \end{aligned}$$

Definición 4.2.3. Sean G un grupo y M un G-módulo. Decimos que $d : G \to M$ es una derivación principal si existe $a \in M$ tal que

$$d(x) = xa - a$$

para todo $x \in G$.

Denotaremos por $PDer(G, M)$ al conjunto de todas las derivaciones principales. A continuación enunciamos algunas de sus propiedades.

Proposición 4.2.4. *Sean G un grupo y M, N G-módulos. Entonces*

a) $Der(G, M)$ es un grupo abeliano bajo la suma puntual de funciones.

b) $PDer(G, M)$ es un subgrupo de $Der(G, M)$.

c) Si M es un G-módulo trivial, entonces

$$Der(G, M) = Hom(G, M).$$

d) Si $f : M \to N$ es un G-morfismo y $d \in Der(G, M)$, entonces $f \circ d \in Der(G, N)$.

Demostración.

a) Se verifica facilmente.

b) La función $d_0(x) = 0$ para todo $x \in G$, es una derivación ya que

$$xd_0(y) + d_0(x) = x \cdot 0 + 0 = 0 = d_0(xy)$$

por lo tanto *PDer*$(G, M) \neq \emptyset$ y además *PDer*$(G, M) \subseteq$ *Der*(G, M). Por último si d, $d' \in$ *PDer*(G, M) entonces existen a, $a' \in M$ tales que

$$d(x) = xa - a \qquad y \qquad d'(x) = xa' - a'$$

para todo $x \in G$. Así

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

Por lo tanto, $d - d' \in$ *PDer*(G, M).

c) Si $d \in$ *Der*(G, M), entonces

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

donde la segunda igualdad se tiene porque M es G-trivial. Por lo tanto, *Der*$(G, M) \subseteq$ *Hom*(G, M). De la misma manera se obtiene la otra contención.

d) Para todo $x, y \in G$

$$\begin{aligned}(f \circ d)(xy) &= f\big(d(xy)\big) \\ &= f\big(xd(y) + d(x)\big) \\ &= xf\big(d(y)\big) + f\big(d(x)\big) \\ &= x(f \circ d)(y) + (f \circ d)(x).\end{aligned}$$

□

Proposición 4.2.5. *Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión. Entonces*

a) Stab$_E(G, M)$ es un grupo bajo la composicion de funciones.

b) Existe un isomorfismo de grupos

$$\sigma : \textit{Stab}_E(G, M) \to \textit{Der}(G, M),$$

donde $\sigma(\varphi) = d$ si $\varphi\big(i(a)s(x)\big) = i\big(a + d(x)\big)s(x)$. En particular, Stab$_E(G, M)$ es un grupo abeliano.

Demostración.

a) Sean $\varphi, \varphi' : E \to E \in \mathit{Stab}_E(G, M)$, entonces los siguientes diagramas conmutan

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array} \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

es decir, $\varphi' i = i$, $p\varphi' = p$ y $\varphi i = i$, $p\varphi = p$. Por lo tanto,

$$(\varphi\varphi')i = \varphi(\varphi' i) = \varphi i = i$$

y

$$p(\varphi\varphi') = (p\varphi)\varphi' = p\varphi' = p$$

y así el siguiente diagrama conmuta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi\varphi'} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

Se tiene entonces que la composición de funciones es una operación cerrada en $\mathit{Stab}_E(G, M)$. La asociatividad se sigue de la asociatividad de la composición de funciones. La identidad $1_E : E \to E \in \mathit{Stab}_E(G, M)$ y es neutro para la operación. Por último, si $\varphi \in \mathit{Stab}_E(G, M)$, φ es un isomorfismo y podemos considerar a ψ la inversa de φ, es decir, $\varphi\psi = 1_E$ y $\psi\varphi = 1_E$. Entonces,

$$\psi i = \psi(\varphi i) = (\psi\varphi)i = 1_E i = i$$

y

$$p\psi = (p\varphi)\psi = p(\varphi\psi) = p1_E = p,$$

es decir, el siguiente diagrama conmuta.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

y así $\psi \in \mathit{Stab}_E(G, M)$.

b) Sea $s : G \to E$ una sección. Si $\varphi \in \mathit{Stab}_E(G, M)$ entonces por la Proposición 4.1.2 existe $d \in \mathit{Der}(G, M)$ tal que $\varphi(i(a)s(x)) = i\big(a + d(x)\big)s(x)$. Es fácil demostrar que dicha derivación es única, por lo que podemos definir $\sigma : \mathit{Stab}_E(G, M) \to \mathit{Der}(G, M)$ como $\sigma(\varphi) = d$. Veamos que σ es un morfismo de grupos.
Sean $\varphi, \varphi' \in \mathit{Stab}_E(G, M)$ y $d, d' \in \mathit{Der}(G, M)$ tales que

$$\varphi\big(i(a)s(x)\big) = i\big(a + d(x)\big)s(x)$$

y

$$\varphi'\big(i(a)s(x)\big) = i\big(a + d'(x)\big)s(x),$$

es decir, $\sigma(\varphi) = d$ y $\sigma(\varphi') = d'$. Se tiene lo siguiente

$$\begin{aligned}\big(\varphi\varphi'\big)\big(i(a)s(x)\big) &= \varphi\Big(\varphi'\big(i(a)s(x)\big)\Big)\\ &= \varphi\Big(i\big(a + d'(x)\big)s(x)\Big)\\ &= i\Big(\big(a + d'(x)\big) + d(x)\Big)s(x)\\ &= i\Big(a + \big(d + d'\big)(x)\Big)s(x)\end{aligned}$$

entonces $\sigma(\varphi\varphi') = d + d' = \sigma(\varphi) + \sigma(\varphi')$. Finalmente, para ver que σ es un isomorfismo exhibimos su inversa $\tau : \mathit{Der}(G, M) \to \mathit{Stab}_E(G, M)$ donde
$\tau(d) : E \to E$ está dada por

$$\tau(d)\big(e = i(a)s(x)\big) = i\big(a + d(x)\big)s(x)$$

obsérvese que por el Lema 4.1.2, $\tau(d) \in \mathit{Stab}_E(G, M)$. Claramente $\sigma\big(\tau(d)\big) = d$ para todo $d \in \mathit{Der}(G, M)$, es decir, $\sigma\tau = 1_{\mathit{Der}(G,M)}$. Sean $\varphi \in \mathit{Stab}_E(G, M)$ y $d \in \mathit{Der}(G, M)$ tales que $\varphi\big(i(a)s(x)\big) = i\big(a + d(x)\big)s(x)$, esto es, $\sigma(\varphi) = d$. Entonces,

$$\begin{aligned}(\tau\sigma)(\varphi)\big(i(a)s(x)\big) &= \tau\big(\sigma(\varphi)\big)\big(i(a)s(x)\big)\\ &= \tau(d)\big(i(a)s(x)\big)\\ &= i\big(a + d(x)\big)s(x)\\ &= \varphi\big(i(a)s(x)\big).\end{aligned}$$

Por lo tanto, $(\tau\sigma)(\varphi) = \varphi$ para todo $\varphi \in \mathit{Stab}_E(G, M)$, es decir, $\tau\sigma = 1_{\mathit{Stab}_E(G,M)}$.

□

No es obvio que $\mathit{Stab}_E(G, M)$ sea un grupo abeliano, ya que la operación está dada por la composición de funciones. Esto se concluye del inciso *b)* de la Proposición 4.2.5.

Corolario 4.2.6. *Sean G un grupo y M un G-módulo. Si*

$$0 \longrightarrow M \xrightarrow{\ i\ } E \xrightarrow{\ p\ } G \longrightarrow 1 \qquad y \qquad 0 \longrightarrow M \xrightarrow{\ j\ } E' \xrightarrow{\ q\ } G \longrightarrow 1$$

son dos extensiones de M por G, entonces $\mathit{Stab}_E(G, M) \simeq \mathit{Stab}_{E'}(G, M)$.

Demostración. Ambos grupos $\mathit{Stab}_E(G, M)$ y $\mathit{Stab}_{E'}(G, M)$ son isomorfos a $\mathit{Der}(G, M)$. □

Teorema 4.2.7. *Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{\ i\ } E \xrightarrow{\ p\ } G \longrightarrow 1$ una extensión que preserva la acción. Entonces*

$$\mathit{Stab}_E(G, M)/\big(\mathit{Inn}(E) \cap \mathit{Stab}_E(G, M)\big) \simeq \mathit{Der}(G, M)/\mathit{PDer}(G, M).$$

Demostración. Sea $s : G \to E$ una sección, por el inciso *b)* de la Proposición 4.2.5, existe un isomorfismo $\sigma : \mathit{Stab}_E(G, M) \to \mathit{Der}(G, M)$, donde

$$\sigma(\varphi) = d \qquad \textit{si } \varphi\big(i(a)s(x)\big) = i\big(a + d(x)\big)s(x).$$

Veamos que $\sigma\big(\mathit{Inn}(E) \cap \mathit{Stab}_E(G, M)\big) = \mathit{PDer}(G, M)$. Sea $\varphi \in \mathit{Inn}(E) \cap \mathit{Stab}_E(G, M)$, ya que $\varphi \in \mathit{Stab}(G, M)$ se tiene que $\varphi i = i$. Por otro lado, existe $c \in E$ tal que $\varphi(e) = cec^{-1}$ para todo $e \in E$, pues $\varphi \in \mathit{Inn}(E)$. Afirmamos que $c \in \mathit{Im}(i)$. En efecto, sea $a \in M$, $ci(a)c^{-1} \in \mathit{Im}(i)$ puesto que $\mathit{Im}(i) \trianglelefteq E$, así $ci(a)c^{-1} = i(b)$ para algún $b \in M$. Entonces

$$ci(a)c^{-1} = i(b) = \varphi\big(i(b)\big) = ci(b)c^{-1},$$

se sigue que $i(a) = i(b)$ y así $a = b$. Se tiene que $ci(a)c^{-1} = i(a)$ o equivalentemente que $ci(a) = i(a)c$ para todo $a \in M$, es decir, $c \in Z\big(\mathit{Im}(i)\big) = \mathit{Im}(i)$, ya que $\mathit{Im}(i)$ es abeliano.

Sea $a_0 \in M$ tal que $i(a_o) = c$ y sea $d \in \mathit{Der}(G, M)$ tal que $\varphi\big(i(a)s(x)\big) = i\big(a + d(x)\big)s(x)$. Tenemos lo siguiente

$$\begin{aligned} i\big(a + d(x)\big)s(x) &= \varphi\big(i(a)s(x)\big) \\ &= ci(a)s(x)c^{-1} \\ &= i(a_0)i(a)s(x)i(a_0)^{-1} \\ &= i(a_0)i(a)\big(s(x)i(-a_0)s(x)^{-1}\big)s(x) \\ &= i(a_0)i(a)i(-xa_0)s(x) \\ &= i(a_0 + a - xa_0)s(x) \end{aligned}$$

Se sigue que $d(x) = a_0 - xa_0$, es decir, $d \in \mathit{PDer}(G, M)$ y $\sigma(\varphi) = d$, por lo tanto $\sigma\big(\mathit{Inn}(E) \cap \mathit{Stab}_E(G, M)\big) \subseteq \mathit{PDer}(G, M)$. Recíprocamente, si $d \in \mathit{PDer}(G, M)$, existe $a_0 \in M$ tal que $d(x) = xa_0 - a_0$ para todo $x \in G$. Si definimos $\varphi : E \to E$ como

$$\varphi\big(e = i(a)s(x)\big) = i\big(a + d(x)\big)s(x),$$

entonces $\varphi \in \mathit{Stab}_E(G, M)$ y además

$$\begin{aligned} \varphi\big(e = i(a)s(x)\big) &= i\big(a + d(x)\big)s(x) \\ &= i(a + xa_0 - a_0)s(x) \\ &= i(-a_0 + a + xa_0)s(x) \\ &= i(-a_0)i(a)i(xa_0)s(x) \\ &= i(a_0)^{-1}i(a)\big(s(x)i(a_0)s(x)^{-1}\big)s(x) \\ &= i(a_0)^{-1}i(a)s(x)i(a_0) \\ &= i(a_0)^{-1}ei(a_0) \end{aligned}$$

es decir, φ es la conjugación por $i(a_0)^{-1}$. Por lo tanto $d = \sigma(\varphi) \in \sigma\big(\mathit{Inn}(E) \cap \mathit{Stab}_E(G, M)\big)$. □

Por el inciso *d)* de la Proposición 4.2.4 tenemos que: Si $f : M \to N$ es un G-morfismo y $d \in Der(G, M)$, entonces $f \circ d \in Der(G, N)$ y así podemos definir a la función $f_\star : Der(G, M) \to Der(G, N)$ como

$$f_\star(d) = f \circ d$$

Tenemos las siguientes propiedades.

Proposición 4.2.8. *Si $f : M \to N$ y $g : N \to L$ son G-morfismos. Entonces*

a) $f_\star : Der(G, M) \to Der(G, N)$ *es un morfismo de grupos abelianos.*

b) $(gf)_\star = g_\star f_\star$

c) Si $1_M : M \to M$ *es la identidad en* M*, entonces* $(1_M)_\star = 1_{Der(G,M)}$.

Demostración.

a) Sean $d, d' \in Der(G, M)$ y $a \in M$. Entonces,

$$\begin{aligned}
\big(f_\star(d + d')\big)(a) &= \big(f \circ (d + d')\big)(a) \\
&= f\big((d + d')(a)\big) \\
&= f\big(d(a) + d'(a)\big) \\
&= f\big(d(a)\big) + f\big(d'(a)\big) \\
&= (f \circ d)(a) + (f \circ d')(a) \\
&= (f \circ d + f \circ d')(a) \\
&= \big(f_\star(d) + f_\star(d')\big)(a)
\end{aligned}$$

Por lo tanto, $f_\star(d + d') = f_\star(d) + f_\star(d')$.

b) $(gf)_\star(d) = (gf)d = g(fd) = g_\star(fd) = g_\star(f_\star(d)) = (g_\star f_\star)(d)$.

c) $(1_M)_\star(d) = 1_M d = d$.

□

La Proposición anterior nos dice que si G es un grupo, entonces la asignación $Der(G, \_) : {}_{\mathbb{Z}G}\mathbf{Mod} \to \mathbf{Ab}$ definida por $Der(G, \_)(M) = Der(G, M)$ y $Der(G, \_)(f) = f_\star$ es un funtor covariante.

Proposición 4.2.9. *Sea G un grupo. Entonces, existe un isomorfismo natural*

$$\tau : Hom_{\mathbb{Z}G}(I_G, \_) \to Der(G, \_),$$

donde I_G es el ideal de aumento.

Demostración. Sean M un G-módulo y $\varphi : I_G \to M$ un G-morfismo, si definimos $\varphi' : G \to M$ como

$$\varphi'(x) = \varphi(x-1)$$

Entonces φ' resulta ser una derivación. En efecto,

$$\begin{aligned}\varphi'(xy) &= \varphi(xy-1)\\ &= \varphi\big(x(y-1)+(x-1)\big)\\ &= x\varphi(y-1)+\varphi(x-1)\\ &= x\varphi'(y)+\varphi'(x)\end{aligned}$$

Definimos $\tau_M : \mathit{Hom}_{\mathbb{Z}G}(I_G, M) \to \mathit{Der}(G, M)$ mediante $\tau_M(\varphi) = \varphi'$.

a) τ_M es un morfismo de grupos abelianos, ya que

$$\begin{aligned}\tau_M(\varphi+\psi)(x) &= (\varphi+\psi)'(x)\\ &= (\varphi+\psi)(x-1)\\ &= \varphi(x-1)+\psi(x-1)\\ &= \varphi'(x)+\psi'(x)\\ &= (\varphi'+\psi')(x)\\ &= \big(\tau_M(\varphi)+\tau_M(\psi)\big)(x)\end{aligned}$$

Por lo tanto, $\tau_M(\varphi+\psi) = \tau_M(\varphi)+\tau_M(\psi)$.

b) τ_M es suprayectiva. Por la Proposición 1.3.3 el ideal de aumento I_G es un grupo abeliano libre con base el conjunto

$$X = \big\{x-1 : x \in G \setminus \{1\}\big\}$$

Si $d \in \mathit{Der}(G, M)$, definimos $\widetilde{d} : X \to M$ mediante

$$\widetilde{d}(x-1) = d(x),$$

esto induce un único morfismo de grupos $\varphi : I_G \to M$ tal que $\varphi|_X = \widetilde{d}$. Para verificar que φ es un G-morfismo basta demostrar que $\varphi\big(x(y-1)\big) = x\varphi(y-1)$ para todo $x \in G$ y $y \in G \setminus \{1\}$. En efecto,

$$\begin{aligned}\varphi\big(x(y-1)\big) &= \varphi(xy-1-x+1)\\ &= \varphi\big(xy-1-(x-1)\big)\\ &= \varphi(xy-1)-\varphi(x-1)\\ &= \widetilde{d}(xy-1)-\widetilde{d}(x-1)\\ &= d(xy)-d(x)\\ &= xd(y)\\ &= x\widetilde{d}(y-1)\\ &= x\varphi(y-1)\end{aligned}$$

Finalmente,

$$\begin{aligned}\tau_M(\varphi)(x) &= \varphi'(x)\\ &= \varphi(x-1)\\ &= \widetilde{d}(x-1)\\ &= d(x)\end{aligned}$$

Por lo tanto, $\tau_M(\varphi) = d$.

c) τ_M es inyectiva ya que si $\varphi \in \mathit{Ker}(\tau_M)$, entonces para todo $x \in G \setminus \{1\}$

$$\varphi(x-1) = \varphi'(x) = \tau_M(\varphi)(x) = 0$$

Por lo tanto, $\varphi = 0$.

d) Para la naturalidad, si $\phi : M \to N$ es un G-morfismo, entonces el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathit{Hom}_{\mathbb{Z}G}(I_G, M) & \xrightarrow{\tau_M} & \mathit{Der}(G, M) \\ \downarrow{\scriptstyle \phi_*} & & \downarrow{\scriptstyle \phi_\star} \\ \mathit{Hom}_{\mathbb{Z}G}(I_G, N) & \xrightarrow[\tau_N]{} & \mathit{Der}(G, N) \end{array}$$

En efecto,

$$\begin{aligned}(\tau_N\phi_*)(\varphi) &= \tau_N\big(\phi_*(\varphi)\big)\\ &= \tau_N(\phi\varphi)\\ &= (\phi\varphi)'\\ &= \phi\varphi'\\ &= \phi_\star(\varphi')\\ &= \phi_\star\big(\tau_M(\varphi)\big)\\ &= (\phi_\star\tau_M)(\varphi)\end{aligned}$$

□

Teorema 4.2.10. *Sean G un grupo y M un G-módulo. Entonces*

$$H^1(G, M) \simeq \mathit{Der}(G, M)/\mathit{PDer}(G, M).$$

Demostración. Aplicando el funtor $\mathit{Hom}_{\mathbb{Z}G}(\_, M)$ a la resolución reducida de $\mathbf{B}(G)$ de la Proposición 2.4.4, obtenemos el complejo

$$0 \longrightarrow \mathit{Hom}_{\mathbb{Z}G}(B_0, M) \xrightarrow{d_1^*} \mathit{Hom}_{\mathbb{Z}G}(B_1, M) \xrightarrow{d_2^*} \mathit{Hom}_{\mathbb{Z}G}(B_2, M) \longrightarrow \cdots$$

Por definición $H^1(G, M) = \mathit{Ext}^1_{\mathbb{Z}G}(\mathbb{Z}, M) = \mathit{Ker}(d_2^*)/\mathit{Im}(d_1^*)$.

Sea $\delta : B_1 \to M \in \mathit{Ker}(d_2^*)$, entonces para todo $x, y \in G$

$$\begin{aligned} 0 &= d_2^*(\delta)[x \mid y] \\ &= \delta d_2[x \mid y] \\ &= \delta\big(x[y] - [xy] + [x]\big) \\ &= x\delta[y] - \delta[xy] + \delta[x]. \end{aligned}$$

Se sigue que $\delta[xy] = x\delta[y] + \delta[x]$ y por lo tanto $\delta|_G \in \mathit{Der}(G, M)$. Definimos $\psi : \mathit{Ker}(d_2^*) \to \mathit{Der}(G, M)$ como

$$\psi(\delta) = \delta|_G$$

Claramente ψ es un morfismo de grupos abelianos.

a) ψ es inyectiva ya que si $\delta : B_1 \to M \in \mathit{Ker}(\psi)$, entonces para todo $x \in G$

$$0 = \psi(\delta)[x] = \delta|_G\,[x].$$

Por lo tanto $\delta = 0$, ya que B_1 es libre sobre G.

b) ψ es suprayectiva. Sea $\rho \in \mathit{Der}(G, M)$, entonces existe un único $\mathbb{Z}G$-morfismo $\overline{\rho} : B_1 \to G$ tal que $\overline{\rho}\,|_G = \rho$ pues B_1 es un $\mathbb{Z}G$-módulo libre sobre G. Además, para todo $x, y \in G$

$$\begin{aligned} d_2^*(\overline{\rho})[x \mid y] &= \overline{\rho} d_2[x \mid y] \\ &= \overline{\rho}\big(x[y] - [xy] + [x]\big) \\ &= x\overline{\rho}[y] - \overline{\rho}[xy] + \overline{\rho}[x] \\ &= x\rho[y] - \rho[xy] + \rho[x] \\ &= 0 \end{aligned}$$

así $\overline{\rho} \in \mathit{Ker}(d_2^*)$ y $\psi(\overline{\rho}) = \overline{\rho}|_G = \rho$.

Por lo tanto, $\psi : \mathit{Ker}(d_2^*) \to \mathit{Der}(G, M)$ es un isomorfismo el cual induce un morfismo

$$\overline{\psi} : \mathit{Ker}(d_2^*)/\mathit{Im}(d_1^*) \to Der(G, M)/\psi\big(\mathit{Im}(d_1^*)\big)$$

el cual también es un isomorfismo. Solo resta verificar que $\psi\big(\mathit{Im}(d_1^*)\big) = \mathit{PDer}(G, M)$, para ello, sea $\varphi \in \mathit{Hom}_{\mathbb{Z}G}(B_0, M)$ y sea $a_0 = \varphi\big([\ ]\big) \in M$. Tenemos que

$$(\varphi d_1)|_G\,[x] = \varphi d_1[x] = \varphi\big(x[\ ] - [\ ]\big) = x\varphi[\ ] - \varphi[\ ] = xa_0 - a_0.$$

Se sigue que, $\psi\big(d_1^*(\varphi)\big) = \psi(\varphi d_1) = (\varphi d_1)\ |_G \in \mathit{PDer}(G, M)$. Por lo tanto, $\psi\big(\mathit{Im}(d_1^*)\big) \subseteq \mathit{PDer}(G, M)$. Recíprocamente, si $\rho \in \mathit{PDer}(G, M)$, entonces existe $a_0 \in M$ tal que $\rho(x) = xa_0 - a_0$ para todo $x \in G$. Definimos $\varphi : B_0 \to M$ como $\varphi\big([\ ]\big) = a_0$, entonces

$$(\varphi d_1)|_G\,[x] = \varphi d_1[x] = \varphi\big(x[\ ] - [\ ]\big) = x\varphi[\ ] - \varphi[\ ] = xa_0 - a_0 = \rho[x].$$

Por lo tanto, $\rho = (\varphi d_1)|_G = \psi(\varphi d_1) = \psi\big(d_1^*(\varphi)\big) \in \psi\big(\mathit{Im}(d_1^*)\big)$. □

Proposición 4.2.11. *Sean G un grupo, M un G-módulo y $0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ una extensión que preserva la acción y se escinde. Si $H^1(G, M) = 0$, entonces cualesquiera dos complementos C y Q de Im(i) en E son conjugados.*

Demostración. Ya que la extensión se escinde existen morfismos r y s tales que la *Im*$(r) = C$ y *Im*$(s) = Q$. Sean f y g los correspondientes conjuntos factores de r y s respectivamente. Por el Lema 3.3.6, $g - f$ es una cofrontera, i.e., existe una función $h : G \to M$ con $h(1) = 0$ tal que

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

además dicha h es tal que $i\big(h(x)\big) = s(x)r(x)^{-1}$. Por otro lado, ya que r y s son morfismos,

$$f(x, y) = 0 = g(x, y).$$

Se sigue que, $xh(y) - h(xy) + h(x) = 0$, es decir, $h \in$ *Der*(G, M). Por el Teorema 4.2.10

$$\textit{Der}(G, M)/\textit{PDer}(G, M) \simeq H^1(G, M) = 0,$$

entonces *Der*$(G, M) =$ *PDer*(G, M) y así $h(x) = xa_0 - a_0$ para algún $a_0 \in M$. Luego,

$$\begin{aligned} s(x)r(x)^{-1} &= i\big(h(x)\big) \\ &= i(xa_0 - a_0) \\ &= i(xa_0)i(a_0)^{-1} \\ &= s(x)i(a_0)s(x)^{-1}i(a_0)^{-1} \end{aligned}$$

Entonces, $r(x)^{-1} = i(a_0)s(x)^{-1}i(a_0)^{-1}$ o equivalentemente $r(x) = i(a_0)s(x)i(a_0)^{-1}$. Por lo tanto, $C =$ *Im*$(r) = i(a_0)$*Im*$(s)i(a_0)^{-1} = i(a_0)Qi(a_0)^{-1}$. □

Proposición 4.2.12. *Sean G un grupo y M un G-módulo. Entonces,*

$$H^2(G, M) \simeq Z^2(G, M)/B^2(G, M).$$

Demostración. Aplicando el funtor *Hom*$_{\mathbb{Z}G}(\_, M)$ a la resolución reducida de $\mathbf{B}^*(G)$ de la Proposición 2.5.5 obtenemos el complejo

$$0 \longrightarrow \textit{Hom}_{\mathbb{Z}G}(B_0, M) \xrightarrow{r_1^*} \textit{Hom}_{\mathbb{Z}G}(B_1/U_1, M) \xrightarrow{r_2^*} \textit{Hom}_{\mathbb{Z}G}(B_2/U_2, M) \xrightarrow{r_3^*} \cdots$$

Por definición, $H^2(G, M) =$ *Ext*$^2_{\mathbb{Z}G}(\mathbb{Z}, M) =$ *Ker*$(r_3^*)/$*Im*(r_2^*). Sean $\pi_1 : B_1 \to B_1/U_1$, $\pi_2 : B_2 \to B_2/U_2$ las proyecciones canónicas y $f : B_2/U_2 \to M \in$ *Ker*(r_3^*). Tenemos lo siguiente: Para todo $x, y, z \in G$

$$\begin{aligned} (f\pi_2)|_{G^2}\,[x \mid 1] &= f\big([x \mid 1] + U_2\big) \\ &= f(0) \\ &= 0 \end{aligned}$$

análogamente $(f\pi_2)|_{G^2}\ [1 \mid y] = 0$. Además,

$$\begin{aligned}
&x(f\pi_2)|_{G^2}\ [y \mid z] - (f\pi_2)|_{G^2}\ [xy \mid z] + (f\pi_2)|_{G^2}\ [x \mid yz] - (f\pi_2)|_{G^2}\ [x \mid y] \\
&\quad = xf\big([y \mid z] + U_2\big) - f\big([xy \mid z] + U_2\big) + f\big([x \mid yz] + U_2\big) - f\big([x \mid y] + U_2\big) \\
&\quad = f\Big(\big(x[y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y]\big) + U_2\Big) \\
&\quad = f\big(d_3[x \mid y \mid z] + U_2\big) \\
&\quad = fr_3\big([x \mid y \mid z] + U_3\big) \\
&\quad = r_3^*(f)\big([x \mid y \mid z] + U_3\big) \\
&\quad = 0,
\end{aligned}$$

es decir, $(f\pi_2)|_{G^2}$ es un conjunto factor. Definimos $\varphi : \mathit{Ker}(r_3^*) \to Z^2(G, M)$ como

$$\varphi(f) = (f\pi_2)|_{G^2}$$

La función φ es un morfismo de grupos, ya que si $f,\ f' \in \mathit{Ker}(r_3^*)$, entonces

$$\begin{aligned}
\varphi(f + f') &= \big((f + f')\pi_2\big)|_{G^2} \\
&= (f\pi_2 + f'\pi_2)|_{G^2} \\
&= (f\pi_2)|_{G^2} + (f'\pi_2)|_{G^2} \\
&= \varphi(f) + \varphi(f')
\end{aligned}$$

Además,

a) φ es inyectiva, ya que si $\varphi(f) = 0$, entonces para todo $x, y \in G \setminus \{1\}$ se tiene que

$$f\big([x \mid y] + U_2\big) = (f\pi_2)|_{G^2}\ [x \mid y] = \varphi(f)[x \mid y] = 0,$$

es decir, $f|_{X_2} = 0$ y por lo tanto $f = 0$ pues X_2 es base de B_2/U_2.

b) φ también es suprayectiva. Para verificar esto, sea $g \in Z^2(G, M)$. Ya que B_2 es un $\mathbb{Z}G$-módulo libre sobre G^2, existe un único $\mathbb{Z}G$-morfismo $\overline{g} : B_2 \to M$ tal que $\overline{g}|_{G^2} = g$. Además, $U_2 \subseteq \mathit{Ker}(\overline{g})$ pues U_2 está genereado por

$$\begin{aligned}
Y_2 &= \big\{[x_1 \mid x_2] \in G^2 :\ \textit{al menos un } x_i = 1\big\} \\
&= \big\{[x \mid 1], [1 \mid y] : x, y \in G\big\}
\end{aligned}$$

y para todo $x, y \in G$

$$\overline{g}[x \mid 1] = g[x \mid 1] = 0 = g[1 \mid y] = \overline{g}[1 \mid y].$$

Por lo tanto, existe un único $\mathbb{Z}G$-morfismo $f : B_2/U_2 \to M$ tal que $f\pi_2 = \overline{g}$. Veamos

que $f \in \mathit{Ker}(r_3^*)$, para ello notemos que para todo $x, y, z \in G \setminus \{1\}$

$$\begin{aligned} r_3^*(f)\big([x \mid y \mid z] + U_3\big) &= f r_3\big([x \mid y \mid z] + U_3\big) \\ &= f\big(d_3[x \mid y \mid z] + U_2\big) \\ &= f\Big(\pi_2\big(d_3[x \mid y \mid z]\big)\Big) \\ &= f\Big(\pi_2\big(x[y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y]\big)\Big) \\ &= xf\pi_2[y \mid z] - f\pi_2[xy \mid z] + f\pi_2[x \mid yz] - f\pi_2[x \mid y] \\ &= x\overline{g}[y \mid z] - \overline{g}[xy \mid z] + \overline{g}[x \mid yz] - \overline{g}[x \mid y] \\ &= xg[y \mid z] - g[xy \mid z] + g[x \mid yz] - g[x \mid y] \\ &= 0 \end{aligned}$$

y como $X_3 = \Big\{[x \mid y \mid z] + U_3 \in B_3/U_3 : x, y, z \in G \setminus \{1\}\Big\}$ es base de B_3/U_3 se tiene que $r_3^*(f) = 0$. Finalmente,

$$\varphi(f) = (f\pi_2)|_{G^2} = \overline{g}|_{G^2} = g.$$

Por lo tanto, $\varphi : \mathit{Ker}(r_3^*) \to Z^2(G, M)$ es un isomorfismo, el cual induce un isomorfismo

$$\overline{\varphi} : \mathit{Ker}(r_3^*)/\mathit{Im}(r_2^*) \to Z^2(G, M)/\varphi\big(\mathit{Im}(r_2^*)\big).$$

Para concluir con la demostración mostraremos que $\varphi\big(\mathit{Im}(r_2^*)\big) = B^2(G, M)$. Para ello, sea $h \in \mathit{Hom}_G(B_1/U_1, M)$. Definimos $h' : G \to M$ como

$$h' = (h\pi_1)|_G$$

entonces $h'[1] = (h\pi_1)|_G\,[1] = h\big([1] + U_1\big) = h(0) = 0$ y

$$\begin{aligned} (hr_2\pi_2)|_{G^2}\,[x \mid y] &= hr_2\big([x \mid y] + U_2\big) \\ &= h\big(d_2[x \mid y] + U_1\big) \\ &= h\Big(\pi_1\big(d_2[x \mid y]\big)\Big) \\ &= h\Big(\pi_1\big(x[y] - [xy] + [x]\big)\Big) \\ &= xh\pi_1[y] - h\pi_1[xy] + h\pi_1[x] \\ &= xh'[y] - h'[xy] + h'[x], \end{aligned}$$

es decir, $\varphi\big(r_2^*(h)\big) = \varphi(hr_2) = (hr_2\pi_2)|_{G^2} \in B^2(G, M)$. Recíprocamente, si $g \in B^2(G, M)$, entonces existe una función $h : G \to M$ con $h[1] = 0$ tal que

$$g[x \mid y] = xh[y] - h[xy] + h[x].$$

Ya que B_1 es un $\mathbb{Z}G$-módulo libre sobre G, existe un único $\mathbb{Z}G$-morfismo $\overline{h} : B_1 \to M$ tal que $\overline{h}\,|_G = h$. Además, $U_1 \subseteq \mathit{Ker}(\overline{h})$, por lo que $\overline{h}$ también induce un único $\mathbb{Z}G$-morfismo $f : B_1/U_1 \to M$ tal que $f\pi_1 = \overline{h}$. Finalmente,

$$\begin{aligned}
(fr_2\pi_2)|_{G^2}\,[x \mid y] &= fr_2\big([x \mid y] + U_2\big) \\
&= f\big(d_2[x \mid y] + U_1\big) \\
&= f\Big(\pi_1\big(d_2[x \mid y]\big)\Big) \\
&= f\Big(\pi_1\big(x[y] - [xy] + [x]\big)\Big) \\
&= xf\pi_1[y] - f\pi_1[xy] + f\pi_1[x] \\
&= x\overline{h}[y] - \overline{h}[xy] + \overline{h}[x] \\
&= xh[y] - h[xy] + h[x] \\
&= g[x \mid y]
\end{aligned}$$

Por lo tanto, $g = (fr_2\pi_2)|_{G^2} = \varphi(fr_2) = \varphi\big(r_2^*(f)\big) \in \varphi\big(\mathit{Im}(r_2^*)\big)$. □

Corolario 4.2.13. *Sean G un grupo y M un G-módulo. Existe una biyección*

$$\phi : H^2(G, M) \to \boldsymbol{e}(G, M)$$

tal que $\phi(0) = [\varepsilon]$, donde ε es la extensión

$$\varepsilon : 0 \longrightarrow M \xrightarrow{\ j\ } M \rtimes G \xrightarrow{\ \pi\ } G \longrightarrow 1.$$

Demostración. Por el Teorema 3.3.11 existe una biyección

$$\psi : Z^2(G, M)/B^2(G, M) \to \boldsymbol{e}(G, M)$$

tal que $\psi(0) = [\varepsilon]$, donde ε es la extensión

$$\varepsilon : 0 \longrightarrow M \xrightarrow{\ j\ } M \rtimes G \xrightarrow{\ \pi\ } G \longrightarrow 1$$

y por la Proposición 4.2.12, $H^2(G, M) \simeq Z^2(G, M)/B^2(G, M)$. □

Corolario 4.2.14. *Sean G un grupo y M un G-módulo. Si $H^2(G, M) = 0$, entonces toda extensión de M por G que preserva la acción se escinde. Es decir, si*

$$0 \longrightarrow M \xrightarrow{\ i\ } E \xrightarrow{\ p\ } G \longrightarrow 1$$

es una extensión que preserva la acción, entonces $E \simeq M \rtimes G$.

Demostración. Sea $\omega : 0 \longrightarrow M \xrightarrow{\ i\ } E \xrightarrow{\ p\ } G \longrightarrow 1$ una extensión que preserva la acción. Por el Corolario 4.2.13 tenemos que

$$[\omega] \in \boldsymbol{e}(G, M) = \mathit{Im}(\phi) = \big\{\phi(0)\big\} = \big\{[\varepsilon]\big\},$$

donde ε es la extensión

$$\varepsilon : 0 \longrightarrow M \xrightarrow{j} M \rtimes G \xrightarrow{\pi} G \longrightarrow 1.$$

Y así, $[\omega] = [\varepsilon]$ y por lo tanto las extensiones $\omega : 0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ y $\varepsilon : 0 \longrightarrow M \xrightarrow{j} M \rtimes G \xrightarrow{\pi} G \longrightarrow 1$ son equivalentes. En particular, $E \simeq M \rtimes G$. □

Teorema 4.2.15. *Sea G un grupo finito de orden m y sea M un G-módulo. Entonces,*

$$mH^n(G, M) = 0$$

para todo $n \geq 1$.

Demostración. Aplicando el funtor $Hom_{\mathbb{Z}G}(\_, M)$ a la resolución reducida de $\mathbf{B}(G)$ de la Proposición 2.4.4 se obtiene el complejo

$$0 \longrightarrow Hom_{\mathbb{Z}G}(B_0, M) \xrightarrow{d_1^*} Hom_{\mathbb{Z}G}(B_1, M) \longrightarrow \cdots$$
$$Hom_{\mathbb{Z}G}(B_{n-1}, M) \xrightarrow{d_n^*} Hom_{\mathbb{Z}G}(B_n, M) \xrightarrow{d_{n+1}^*} Hom_{\mathbb{Z}G}(B_{n+1}, M) \longrightarrow \cdots$$

Por definición, $H^n(G, M) = Ext^n_{\mathbb{Z}G}(\mathbb{Z}, M) = Ker(d_{n+1}^*)/Im(d_n^*)$.

Sea $f : B_n \to M \in Ker(d_{n+1}^*)$, definimos $\varphi : B_{n-1} \to M$ como

$$\varphi[x_1 \mid \ldots \mid x_{n-1}] = \sum_{x \in G} f[x_1 \mid \ldots \mid x_{n-1} \mid x].$$

El morfismo φ está bien definido pues G es finito. Por otro lado, para cada $x \in G$

$$\begin{aligned}
0 &= d_{n+1}^*(f)[x_1 \mid \ldots \mid x_n \mid x] = f d_{n+1}[x_1 \mid \ldots \mid x_n \mid x] \\
&= f\Bigg(x_1[x_2 \mid \ldots \mid x_n \mid x] + \sum_{i=1}^{n-1} (-1)^i [x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n \mid x] \\
&\quad + (-1)^n [x_1 \mid \ldots \mid x_{n-1} \mid x_n x] + (-1)^{n+1} [x_1 \mid \ldots \mid x_{n-1} \mid x_n] \Bigg) \\
&= x_1 f[x_2 \mid \ldots \mid x_n \mid x] + \sum_{i=1}^{n-1} (-1)^i f[x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n \mid x] \\
&\quad + (-1)^n f[x_1 \mid \ldots \mid x_{n-1} \mid x_n x] + (-1)^{n+1} f[x_1 \mid \ldots \mid x_{n-1} \mid x_n].
\end{aligned}$$

Realizando la suma sobre cada $x \in G$ tenemos que

$$\begin{aligned}
0 &= x_1 \sum_{x\in G} f[x_2 \mid \ldots \mid x_n \mid x] + \sum_{i=1}^{n-1}(-1)^i \sum_{x\in G} f[x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n \mid x] \\
&\quad + (-1)^n \sum_{x\in G} f[x_1 \mid \ldots \mid x_{n-1} \mid x_n x] + (-1)^{n+1} \sum_{x\in G} f[x_1 \mid \ldots \mid x_{n-1} \mid x_n] \\
&= x_1 \varphi[x_2 \mid \ldots \mid x_n] + \sum_{i=1}^{n-1}(-1)^i \varphi[x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n] \\
&\quad + (-1)^n \varphi[x_1 \mid \ldots \mid x_{n-1}] + (-1)^{n+1} m f[x_1 \mid \ldots \mid x_{n-1} \mid x_n] \\
&= \varphi\Bigg(x_1[x_2 \mid \ldots \mid x_n] + \sum_{i=1}^{n-1}(-1)^i [x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n] \\
&\quad + (-1)^n [x_1 \mid \ldots \mid x_{n-1}] \Bigg) + (-1)^{n+1} m f[x_1 \mid \ldots \mid x_{n-1} \mid x_n] \\
&= \varphi d_n[x_1 \mid \ldots \mid x_n] + (-1)^{n+1} m f[x_1 \mid \ldots \mid x_n] \\
&= \big(\varphi d_n + (-1)^{n+1} m f\big)[x_1 \mid \ldots \mid x_{n-1} \mid x_n]
\end{aligned}$$

Por lo tanto, $\varphi d_n + (-1)^{n+1} m f = 0$, así $mf = \pm \varphi d_n = d_n^*(\pm\varphi) \in \mathit{Im}(d_n^*)$. □

Lema 4.2.16. *Sea G un grupo finito y sea M un $\mathbb{Z}G$-módulo finitamente generado. Entonces, M como grupo abeliano es finitamente generado.*

Demostración. Sea $G = \{x_1, \ldots, x_n\}$ y sea $\{a_1, \ldots, a_m\} \subseteq M$ tal que $M = \langle a_1, \ldots, a_m \rangle$. Veamos que M como grupo abeliano está generado por el conjunto

$$\big\{x_i a_j : 1 \leq i \leq n, 1 \leq j \leq m\big\}.$$

En efecto, si $a \in M$, entonces $a = \gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_m a_m$ con $\gamma_j \in \mathbb{Z}G$. Además, para cada j se tiene que $\gamma_j = \sum_{i=1}^{n} r_{ji} x_i$ con $r_{ji} \in \mathbb{Z}$. Por lo tanto,

$$\begin{aligned}
a &= \gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_m a_m \\
&= \left(\sum_{i=1}^{n} r_{1i} x_i\right) a_1 + \left(\sum_{i=1}^{n} r_{2i} x_i\right) a_2 + \cdots + \left(\sum_{i=1}^{n} r_{1i} x_i\right) a_m \\
&= \sum_{i=1}^{n} r_{1i}\big(x_i a_1\big) + \sum_{i=1}^{n} r_{2i}\big(x_i a_2\big) + \cdots + \sum_{i=1}^{n} r_{mi}\big(x_i a_m\big) \\
&= \sum_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} r_{ji}\big(x_i a_j\big).
\end{aligned}$$

□

Lema 4.2.17. *Sean R un anillo y M un R-módulo finitamente generado. Si R es noetheriano izquierdo, entonces M es noetheriano.*

Demostración. Como M es finitamente generado existe un epimorfismo $\varphi : R^k \to M$. Ya que R es noetheriano, R^k es noetheriano y como φ es un epimorfismo M es noetheriano. □

Del Lema 4.2.17, eligiendo $R = \mathbb{Z}$, concluimos que todo subgrupo de un grupo abeliano finitamente generado es también finitamente generado.

Lema 4.2.18. *Sean R un anillo conmutativo y M, N R-módulos finitamente generados. Si R es noetheriano, entonces $Hom_R(M, N)$ es un R-módulo finitamente generado.*

Demostración. Como M es finitamente generado, existe un epimorfismo $\varphi : R^k \to M$. Ya que el funtor $Hom_R(\_, N)$ es exacto izquierdo,

$$\varphi^* : Hom_R(M, N) \to Hom_R(R^k, N)$$

es un monomorfismo. Por otro lado, $Hom_R(R^k, N) \simeq Hom_R(R, N)^k \simeq N^k$ el cual es también finitamente generado pues N lo es. Finalmente, como R es noetheriano y $Hom_R(R^k, N)$ es finitamente generado, del Lema 4.2.17, se sigue que $Hom_R(R^k, N)$ es noetheriano y por lo tanto, $Hom_R(M, N) \simeq Im(\varphi^*)$ es finitamente generado. □

Lema 4.2.19. *Sea M un grupo abeliano finitamente generado. Si M es un grupo de torsión, entonces M es finito.*

Demostración. Sea $\{a_1, \ldots, a_n\} \subseteq M$ tal que $M = \langle a_1, \ldots, a_n \rangle$. Ya que M es de torsión todos sus elementos son de orden finito. Sea $r_i = ord(a_i)$. Definimos

$$f : \bigoplus_{i=1}^{n} \langle a_i \rangle \to M$$

como $f(r_1 a_1, \ldots, r_n a_n) = r_1 a_1 + \cdots + r_n a_n$. Claramente f es suprayectiva y por lo tanto

$$|M| \leq \left| \bigoplus_{i=1}^{n} \langle a_i \rangle \right| = \prod_{i=1}^{n} |\langle a_i \rangle| = \prod_{i=1}^{n} r_i < \infty.$$

□

Corolario 4.2.20. *Sea G un grupo finito y sea M un $\mathbb{Z}G$-módulo finitamente generado. Entonces, $H^n(G, M)$ es finito para todo $n \geq 1$.*

Demostración. Los términos B_n en la resolución barra $\mathbf{B}(G)$ son $\mathbb{Z}G$-módulos finitamente generados, puesto que son libres sobre G^n. Del Lema 4.2.16, se sigue que, como grupos abelianos M y B_n son finitamente generados. Ya que $\mathbb{Z}$ es noetheriano, del Lema 4.2.18, $Hom_{\mathbb{Z}}(B_n, M)$ es un grupo abeliano finitamente generado. Puesto que $Ker(d_{n+1}^*)$ y

$Hom_{\mathbb{Z}G}(B_n, M)$ son subgrupos de $Hom_{\mathbb{Z}}(B_n, M)$, entonces $Hom_{\mathbb{Z}G}(B_n, M)$ y $Ker(d^*_{n+1})$ también son grupos abelianos finitamente generados y por lo tanto,

$$H^n(G, M) = Ext^n_{\mathbb{Z}G}(\mathbb{Z}, M) = Ker(d^*_{n+1})/Im(d^*_n)$$

es también un grupo abeliano finitamente generado. Finalmente, si $m = |G|$ entonces por el Teorema 4.2.15, $mH^n(G, M) = 0$. Se sigue que, $H^n(G, M)$ es un grupo de torsión, y por el Lema 4.2.19 concluimos que $H^n(G, M)$ es finito. □

Lema 4.2.21. *Sean $\varphi : R \to S$ un morfismo de anillos y M un S-módulo. Entonces,*

a) M admite estructura de R-módulo a través de φ.

b) Si M es un S-módulo finitamente generado y φ es un morfismo suprayectivo, entonces M como R-módulo también es finitamente generado.

Demostración.

a) Si $r \in R$ y $a \in M$, definimos

$$r \cdot a = \varphi(r)a.$$

Dicha acción hace de M un R-módulo. En efecto, para cualesquiera r, $r' \in R$ y a, $b \in M$

1) $(rr') \cdot a = \varphi(rr')a = \big(\varphi(r)\varphi(r')\big)a = \varphi(r)\big(\varphi(r')a\big) = \varphi(r)(r' \cdot a) = r \cdot (r' \cdot a)$

2) $(r + r') \cdot a = \varphi(r + r')a = \big(\varphi(r) + \varphi(r')\big)a = \varphi(r)a + \varphi(r')a = r \cdot a + r' \cdot a$

3) $r \cdot (a + b) = \varphi(r)(a + b) = \varphi(r)a + \varphi(r)b = r \cdot a + r \cdot b$

4) $1_R \cdot a = \varphi(1_R)a = 1_S a = a$

b) Sean $a_1, \ldots, a_n \in M$ tales que $M = \sum_{i=1}^{n} Sa_i$. Entonces,

$$\sum_{i=1}^{n} R \cdot a_i = \sum_{i=1}^{n} \varphi(R)a_i = \sum_{i=1}^{n} Sa_i = M,$$

es decir, M como R-módulo también está generado por $a_1, \ldots, a_n$.

□

Ejemplo 4.2.22. Consideremos el grupo cíclico $C_3 = \langle x \rangle = \{1, x, x^2\}$ de orden 3,

$$\mathbb{Z}C_3 = \Big\{\alpha = r_0 + r_1 x + r_2 x^2 : r_0, r_1, r_2 \in \mathbb{Z}\Big\}$$

su anillo de grupo y $\varepsilon : \mathbb{Z}C_3 \to \mathbb{Z}$ el morfismo de aumento. Ya que $\mathbb{Z}C_3$ es un $\mathbb{Z}$-módulo finitamente generado (pues es libre sobre C_3) y ε un morfismo suprayectivo, el Lema 4.2.21 nos garantiza que $\mathbb{Z}C_3$ es un $\mathbb{Z}C_3$-módulo (vía el morfismo ε) finitamente generado. Por el Corolario 4.2.20, $H^n(C_3, \mathbb{Z}C_3)$ es finito para todo $n \geq 1$. Para este caso en particular,

podemos verificar esta última afirmación usando algunos de los resultados obtenidos en el *Capítulo 2*. Para ello, observemos que $\mathbb{Z}C_3$ es un C_3-módulo trivial, pues

$$x \cdot \alpha = \varepsilon(x)\alpha = 1\alpha = \alpha.$$

Además, $\mathbb{Z}C_3 \simeq \mathbb{Z}^3$ como C_3-módulos triviales. Del Corolario 2.3.6, se sigue que para todo $k \geq 1$

- $H^0(C_3, \mathbb{Z}C_3) \simeq \mathbb{Z}C_3 \simeq \mathbb{Z}^3$
- $H^{2k-1}(C_3, \mathbb{Z}C_3) \simeq H^{2k-1}(C_3, \mathbb{Z}^3) \simeq H^{2k-1}(C_3, \mathbb{Z})^3 \simeq 0$
- $H^{2k}(C_3, \mathbb{Z}C_3) \simeq H^{2k}(C_3, \mathbb{Z}^3) \simeq H^{2k}(C_3, \mathbb{Z})^3 \simeq \mathbb{Z}_3^3$

4.3. El Teorema de Schur-Zassenhaus

Teorema 4.3.1 (Zassenhaus). *Sea G un grupo finito de orden nm con $(n, m) = 1$. Si M es un subgrupo normal abeliano de orden n, entonces G es un producto semidirecto de M por G/M, además cualesquiera dos complementos de M son conjugados.*

Demostración. Aún cuando M es un grupo abeliano, seguiremos utilizando notación multiplicativa. Sea $Q = G/M$, consideremos la sucesión exacta corta

$$\omega : 1 \longrightarrow M \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

donde i es la inclusión y p la proyección canónica. Sea $s : Q \to G$ una sección, por la Proposición 3.1.4, M admite estructura de Q-módulo, el cual está dada de la siguiente manera: Para todo $x \in Q$ y $a \in M$,

$$xa = s(x)as(x)^{-1}.$$

De este modo la extensión ω preserva la acción. Consideremos la función $\mu : M \to M$ definida como

$$\mu(a) = a^m$$

Afirmamos que μ es un Q-isomorfismo. Primero veamos que es un Q-morfismo. Sean a, $b \in M$ y $x \in Q$, entonces

$$\mu(ab) = (ab)^m = a^m b^m = \mu(a)\mu(b),$$

donde la penúltima igualdad se tiene porque M es abeliano, y

$$\mu(xa) = \mu\big(s(x)as(x)^{-1}\big) = \big(s(x)as(x)^{-1}\big)^m = s(x)a^m s(x)^{-1} = x\mu(a).$$

Ahora veamos que μ es un isomorfismo. Si $a \in Ker(\mu)$, entonces $1 = \mu(a) = a^m$ por lo que $ord(a)|m$, además $ord(a)|n$ ya que $a \in M$ y $\big|M\big| = n$, por lo tanto $ord(a)|(n, m) = 1$ y así $a = 1$. Ya que $\mu : M \to M$ es inyectiva y M es finito, μ también resulta ser suprayectiva.

Para cada entero $k \geq 0$, consideremos el funtor $T_k = \mathit{Hom}_{\mathbb{Z}G}(B_k, \_)$, donde B_k son los proyectivos que aparecen en la resolución de la Proposición 2.4.4, y sea

$$\mu_*^k = T_k(\mu) : \mathit{Hom}_{\mathbb{Z}G}(B_k, M) \to \mathit{Hom}_{\mathbb{Z}G}(B_k, M)$$

Ya que μ es un isomorfismo, entonces $\mu_*^k = T_k(\mu)$ también es un isomorfismo, el cual resulta ser la multiplicación por m. Esto último se verifica como sigue

$$\mu_*^k(f)(x) = (\mu f)(x) = \mu\big(f(x)\big) = f(x)^m = (mf)(x)$$

Por lo tanto, $\mu_*^k(f) = mf$. Además, se verifica facilmente que el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathit{Hom}_{\mathbb{Z}G}(B_k, M) & \xrightarrow{d_{k+1}^*} & \mathit{Hom}_{\mathbb{Z}G}(B_{k+1}, M) \\ \Big\downarrow{\scriptstyle \mu_*^k} & & \Big\downarrow{\scriptstyle \mu_*^{k+1}} \\ \mathit{Hom}_{\mathbb{Z}G}(B_k, M) & \xrightarrow[d_{k+1}^*]{} & \mathit{Hom}_{\mathbb{Z}G}(B_{k+1}, M) \end{array}$$

Se sigue que la familia $\mu = \Big\{\mu_*^k : \mathit{Hom}_{\mathbb{Z}G}(B_k, M) \to \mathit{Hom}_{\mathbb{Z}G}(B_k, M)\Big\}_{k\geq 0}$ es un isomorfismo de complejos el cual induce un isomorfismo, en la cohomología de los complejos,

$$\varphi_k : \mathit{Ker}(d_{k+1}^*)/\mathit{Im}(d_k^*) \to \mathit{Ker}(d_{k+1}^*)/\mathit{Im}(d_k^*)$$

el cual está dado por

$$\varphi_k\big(f + \mathit{Im}(d_k^*)\big) = \mu_*^k(f) + \mathit{Im}(d_k^*) = mf + \mathit{Im}(d_k^*) = m\big(f + \mathit{Im}(d_k^*)\big)$$

es decir, el isomorfismo

$$\varphi_k : H^k(Q, M) \to H^k(Q, M)$$

es también la multiplicación por m. Ya que $|Q| = |G| \,/\, |M| = mn/n = m$ el Teorema 4.2.15 nos garantiza que $mH^k(Q, M) = 0$. Por lo tanto, si $x \in H^k(Q, M)$ entonces existe $y \in H^k(Q, M)$ tal que

$$x = \varphi_k(y) = my = 0$$

y así $H^k(Q, M) = 0$. En particular, $H^2(Q, M) = 0 = H^1(Q, M)$ y del Corolario 4.2.14 la extensión

$$\omega : 1 \longrightarrow M \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

se escinde y por la Proposición 4.2.11 cualesquiera dos complementos de M son conjugados. □

Lema 4.3.2. *Sean G un grupo finito de orden nm con $(n, m) = 1$ y K un subgrupo normal de G de orden m. Si G contiene un subgrupo Q de orden n, entonces G es producto semidirecto de K por Q.*

Demostración. Sean Q un subgrupo de G de orden n y $d = |K \cap Q|$. Por el *Teorema de Lagrange* $d \,|\, n$ y $d \,|\, m$, se sigue que $d \,|\, (n, m) = 1$, entonces $K \cap Q = \{1\}$. Por otro lado, $K \lhd G$ implica que KQ es un subgrupo de G y $K \cap Q \lhd Q$, por el *Segundo Teorema de Isomorfismo*

$$Q/(K \cap Q) \simeq KQ/K$$

Luego,

$$|Q| \,/\, |K \cap Q| = [Q : K \cap Q] = |Q/K \cap Q| = |KQ/K| = [KQ : K] = |KQ| \,/\, |K| \,.$$

Ya que $|K \cap Q| = 1$, $|KQ| = |K|\,|Q| = nm$, por lo tanto $KQ = G$. □

Ejemplo 4.3.3. Sea A_4 el grupo formado por las permutaciones pares de S_4, es decir,

$$A_4 = \begin{Bmatrix} 1, (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,4,2), (1,4,3) \\ (2,3,4), (2,4,3), (3,4)(1,2), (2,4)(1,3), (2,3)(1,4) \end{Bmatrix}$$

y sea

$$V = \Big\{1, (3,4)(1,2), (2,4)(1,3), (2,3)(1,4)\Big\}$$

el 4-*grupo de Klein*. Veamos que $V \lhd A_4$, para ello observemos lo siguiente:

1) Para todo $\sigma \in V$, $\sigma^2 = 1$.

2) $V \setminus \{1\}$ son todos los elementos de A_4 de orden 2.

Sean $\tau \in A_4$ y $\sigma \in V$, entonces

$$\big(\tau\sigma\tau^{-1}\big)^2 = \big(\tau\sigma\tau^{-1}\big)\big(\tau\sigma\tau^{-1}\big) = \tau\sigma^2\tau^{-1} = \tau 1 \tau^{-1} = 1$$

se sigue que el orden de $\tau\sigma\tau^{-1}$ es 1 ó 2. Si el orden de $\tau\sigma\tau^{-1}$ es 1, entonces $\tau\sigma\tau^{-1} = 1 \in V$. Si el orden de $\tau\sigma\tau^{-1}$ es 2, entonces $\tau\sigma\tau^{-1} \in V \setminus \{1\} \subseteq V$. Por lo tanto $V \lhd A_4$. Sea $Q_1 = \langle (1,2,3) \rangle = \big\{1, (1,2,3), (1,3,2)\big\}$, entonces por el Lema 4.3.2 $A_4 = V \rtimes Q_1$.

Lema 4.3.4 (Argumento de Frattini). *Sean G un grupo finito y K un subgrupo normal de G. Si P es un p-subgrupo de Sylow de K para algún primo p, entonces*

$$G = KN_G(P).$$

En particular, si $P \lhd K$ entonces $P \lhd G$.

Demostración. Ya que $K \lhd G$, $KN_G(P)$ es un subgrupo de G. Recíprocamente, si $x \in G$, entonces $xPx^{-1} \leq xKx^{-1} = K$, pues $K \lhd G$. Por lo tanto xPx^{-1} también es un p-subgrupo de Sylow de K. Por el *Segundo Teorema de Sylow* P y xPx^{-1} son conjugados, es decir, existe $y \in K$ tal que

$$xPx^{-1} = yPy^{-1},$$

equivalentemente

$$\left(y^{-1}x\right)P\left(y^{-1}x\right)^{-1} = y^{-1}xPx^{-1}y = P,$$

es decir, $y^{-1}x \in N_G(P)$ y así $x = y\left(y^{-1}x\right) \in KN_G(P)$.

Si $P \lhd K$, entonces $yPy^{-1} = P$ para todo $y \in K$, esto es, $K \subseteq N_G(P)$. Se sigue que

$$G = KN_G(P) = N_G(P),$$

es decir, $P \lhd G$. □

Para dar por terminado este trabajo demostraremos el Teorema 4.3.1 para el caso en el que el subgrupo normal M del grupo G no es abeliano. Sin embargo, la demostración de que cualesquiera dos complementos de M son conjugados está fuera del alcance de este trabajo.

Teorema 4.3.5 (Schur-Zassenhaus). *Sean G un grupo finito y K un subgrupo normal de G tal que $\left(|K|, [G : K]\right) = 1$. Entonces G contiene un subgrupo de orden $[G : K]$.*

Demostración. Probaremos el Teorema por inducción sobre $|G|$. Si $|G| = 1$ claramente el Teorema se cumple. Supongamos que $|G| > 1$ y que la afirmación se cumple para cualquier grupo de orden menor a $|G|$.

Si K es el grupo trivial, el Teorema se cumple trivialmente, pues en este caso $|G| = [G : K]$. Podemos entonces suponer que K no es trivial. Sea p un primo tal que $p \big| |K|$ y sea P un p-subgrupo de Sylow de K. Por el Lema 4.3.4 y el *Segundo Teorema de Isomorfismo*

$$G/K = KN_G(P)/K \simeq N_G(P)/(N_G(P) \cap K) = N_G(P)/N_K(P),$$

se sigue que

$$[N_G(P) : N_K(P)] = |N_G(P)/N_K(P)| = |G/K| = [G : K].$$

Si P no es normal en G, entonces $N_G(P)$ es un subgrupo propio de G y

$$\left(|N_K(P)|, [N_G(P) : N_K(P)]\right) = 1,$$

pues $|N_K(P)| \, \big| |K|$. Por lo tanto $N_G(P)$ y su subgrupo normal $N_K(P)$ satisfacen la hipótesis de inducción, esto es, $N_G(P)$ contiene (y por lo tanto G también) un subgrupo de orden $[N_G(P) : N_K(P)] = [G : K]$.

Si $P \lhd G$, entonces $P \lhd K$ y $K/P \lhd G/P$. Por el *Tercer Teorema de Isomorfismo*

$$(G/P)\big/(K/P) \simeq G/K,$$

luego

$$[G/P : K/P] = \left|(G/P)\big/(K/P)\right| = |G/K| = [G : K].$$

De lo anterior y del hecho de que $|K/P| \, \big| |K|$ también podemos concluir que

$$\left(|K/P|, [G/P : K/P]\right) = 1$$

y como $|G/P| < |G|$, existe un subgrupo H/P de G/P tal que

$$|H/P| = [G/P : K/P] = [G : K].$$

Por otro lado, $Z(P)$ es no trivial, pues P es un p-grupo no trivial, además $P \lhd G$ implica que $Z(P) \lhd G$, en particular, $Z(P) \lhd P$ y $Z(P) \lhd H$. Usando nuevamente el *Tercer Teorema de Isomorfismo* obtenemos que

$$[H/Z(P)) : P/Z(P)] = [H : P] = |H/P| = [G : K],$$

luego

$$\left(|P/Z(P)|, [H/Z(P)) : P/Z(P)]\right) = 1$$

ya que $|P/Z(P)| \,||K|$. Como $|H/Z(P)| < |H| \leq |G|$, existe un subgrupo $T/Z(P)$ de $H/Z(P)$ tal que

$$|T/Z(P)| = [H/Z(P)) : P/Z(P)] = [G : K].$$

Tenemos que $Z(P) \lhd T$ y

$$[T : Z(P)] = |T/Z(P)| = [G : K], \tag{4.1}$$

ademas

$$\left(|Z(P)|, [T : Z(P)]\right) = 1$$

pues $|Z(P)| \,||K|$. Si $|T| < |G|$, podemos aplicar la hipótesis de inducción y concluir que T contiene (y por lo tanto G también) un subgrupo de orden $[T : Z(P)] = [G : K]$. Si $|T| = |G|$, entonces $T = G$ y de 4.1 podemos concluir que $K = Z(P)$ y por lo tanto K es abeliano. Puesto que

$$|G| = |K| \, [G : K]$$

y $\left(|K|, [G : K]\right) = 1$, se sigue del Teorema 4.3.1 que G es producto semidirecto de K por G/K y de la Proposición 3.2.2 tenemos que existe un subgrupo $Q \simeq G/K$ de G tal que $G = KQ$ y $K \cap Q = \{1\}$. Finalmente,

$$|Q| = |G/K| = [G : K].$$

□

Bibliografía

[1] Avella, D., Mendoza, O., Saenz, E. C., Souto, M. J., *Grupos II*. Prensas de Ciencias, 2015.

[2] Hilton, P. J., Stammbach, U., *A Course in Homological Algebra*, Springer-Verlag, 1971.

[3] Lluis, E. Álgebra Homológica, Cohomología de Grupos y K-Teoría algebraica clásica. Sociedad Matemática Mexicana, 2005.

[4] Milies, C. P., Sehgal, S. K., *An introduction to Group Rings*. Algebras and applications, Volume 1. Springer, 2002.

[5] Rotman, J. J., *An Introduction to Homological Algebra*, 2nd. Ed. Springer-Verlag, 2009.

[6] Rotman, J. J., *An Introduction to the Theory of Groups*, 4th ed., Springer-Verlag, 1995.

[7] Weibel, C. A., *An Introduction to Homological Algebra*, Cambridge University Press, 1994.

[8] Zaldívar, F., *Cohomología de Galois de Campos Locales*. Sociedad Matemática Mexicana, 2001.